

To nejzajímavější z výroční zprávy Úřadu pro ochranu osobních údajů (ÚOOÚ) a nové pokyny Evropského sboru

🕒 08.07.2022 / 07:17

Úřad pro ochranu osobních údajů (ÚOOÚ, Úřad) vydal výroční zprávu o své činnosti za rok 2021. Ta představuje nejdůležitější výsledky dozorové činnosti ÚOOÚ v oblasti zpracování osobních údajů, které jsou prezentovány na příkladech vybraných kontrol. Níže shrnujeme některé z nich.



Martin Lukáš

Weinhold Legal, v. o. s. advokátní kancelář



Tereza Hošková

Weinhold Legal, v. o. s. advokátní kancelář



Daša Aradská

Weinhold Legal, v.o.s. advokátní kancelář

Sdílet



Věrnostní programy obchodníků

ÚOOÚ provedl kontrolu věrnostních programů maloobchodních řetězců. Při kontrole neshledal žádná závažná provinění. Byl kontrolován rozsah shromažďovaných údajů (nejčastěji titul, jméno, příjmení, datum narození, adresa, platební údaje, e-mailová adresa, tel. číslo, číslo zákaznické karty), doba uchovávání osobních údajů a jejich zabezpečení. Další informace, které obchody uchovávaly, se týkaly nakoupeného zboží, domovské prodejny, využití promoakcí, množství bodů v rámci věrnostního programu a další údaje, které však Úřad shledal přiměřenými vzhledem k účelu jejich zpracování. **Pochybení, která ale kontrolovaným prodejcům vytkl, se týkala příliš dlouhého a neopodstatněného uchovávání osobních údajů – např. uchovávání údajů o nákupu potravinářského zboží po dobu 3 let shledal ÚOOÚ jako nepřiměřené. Úřad proto doporučil zkrátit tuto dobu v souladu s účelem uchovávání těchto údajů (např. dle doby, kdy je možné u zboží uplatnit reklamaci).**

Telemarketing a osobní údaje

Další z oblastí provedených kontrol se týkala telemarketingu, kde přibližně čtvrtinu podnětů přijatých Úřadem tvořily stížnosti ohledně zpracování osobních údajů pro marketingové účely. Jedna z kontrolovaných telemarketingových společností nereagovala na uplatnění práva subjektů údajů na přístup k osobním údajům dle čl. 15 obecného nařízení („GDPR“), případně uváděla jako zdroj osobních údajů pouze náhodné generování telefonního čísla. Na vznesení námítky proti zpracování osobních údajů dle čl. 21 GDPR, event. po uplatnění práva na výmaz dle čl. 17 GDPR, společnost buď vůbec nereagovala, anebo přislíbila ukončení zpracování osobních údajů pro účel marketingu, avšak i po uplynutí měsíční lhůty pro přijetí opatření (dle čl. 12 odst. 3 GDPR) byly subjekty údajů znovu v rámci telemarketingu kontaktovány.

V rámci kontroly telemarketingové společnosti dospěl Úřad ke zjištění, že vystupovala jako zpracovatel osobních údajů, nikoliv jako správce, když svou činnost prováděla dle pokynů správců, pro které zajišťovala službu telemarketingu. Dále bylo zjištěno, že společnost porušila povinnost stanovenou v čl. 15–21 GDPR,

když neposkytla subjektům údajů relevantní informace týkající se zpracování jejich osobních údajů. Konkrétně toto porušení spočívalo v tom, že při poskytování informací subjektům údajů odpovídala unifikovaným způsobem, aniž by zohlednila fakt, že byla v postavení zpracovatele. Společnost též ve svých odpovědích žadatelům neuvedla účel volání, tedy že telefonický hovor byl učiněn za účelem poskytnutí marketingové nabídky jiného subjektu (smluvního klienta); dále bylo ve většině odpovědí uvedeno, že zákonným titulem pro využití telefonního čísla byl oprávněný zájem kontrolované osoby jako správce osobních údajů, což však v tomto případě neplatilo.

Posouzení vlivu na ochranu osobních údajů

Posouzení vlivu na ochranu osobních údajů dle čl. 35 GDPR má provádět **každý správce, jehož záměr zpracování lze hodnotit jako vysoce rizikový** z hlediska zásahu do práv a svobod fyzických osob v souvislosti se zpracováním jejich osobních údajů. Úřad ve své zprávě upozorňuje na chyby, kterých se správci při tomto posuzování dopouštěli:

- balanční test je proveden tak, že z něj není možno ověřit potřebnost, vhodnost a přiměřenost zpracování osobních údajů;
- chybí nebo není dostatečně propracován popis zajištění práv subjektů údajů;
- popis přijatých technických a organizačních opatření bývá obecný a často není zřejmé, jak správce k jejich návrhu dospěl (není využita metodika zpracovaná ÚOOÚ a vlastní metodika správce zřejmá není); důsledkem je, že nelze ověřit, zda jsou přijatá opatření přiměřená a úplná.

Pokyny EDPB 05/2022

Předmětem veřejné konzultace jsou až do 27. června 2022 [Pokyny 05/2022](#) Evropského sboru pro ochranu osobních údajů („EDPB“) o **používání technologie pro rozpoznávání obličeje** v oblasti vymáhání práva ve smyslu Směrnice (EU) [2016/680](#) o vymáhání práva („Směrnice“). Pokyny vycházejí ze současné situace, kdy stále více orgánů činných v trestním řízení používá nebo má v úmyslu používat technologii rozpoznávání obličeje (např. k identifikaci nebo

ověření osoby). Pokyny obsahují také postoj EDPB k této problematice, který vychází ze společného stanoviska EDPB a Evropského inspektora pro ochranu osobních údajů 05/2021 k návrhu Nařízení o umělé inteligenci. Ve stanovisku tyto instituce společně vyzývají k zákazu použití technologie rozpoznávání obličeje k některým účelům (např. k biometrické identifikaci osob na dálku ve veřejném prostoru nebo posuzování emocí osoby).

EDPB uvádí, že technologie rozpoznávání obličeje zahrnující zpracování biometrických údajů představuje vážný zásah do práv na soukromí a též do ochrany osobních údajů. EDPB připomíná, že požadavky na ochranu osobních údajů upravené ve Směrnici musí být samozřejmě plně respektovány (jasný právní základ; konzultace s dozorovým úřadem pro ochranu osobních údajů; posouzení nezbytnosti a přiměřenosti; minimalizace údajů atd.). Rovněž doporučuje zveřejnit výsledky povinného posouzení vlivu na ochranu osobních údajů dle čl. 35 GDPR.

Pokyny EDPB 1/2021

EDPB přijal po veřejných konzultacích finální verzi Pokynů 1/2021 k příkladům týkajícím se **oznamování porušení zabezpečení osobních údajů**. Cílem pokynů je pomoci správcům osobních údajů při rozhodování o tom, jak zacházet s případy porušení ochrany osobních údajů a jaké faktory je třeba zvážit při hodnocení rizika. Přínosem těchto pokynů je, že při každém praktickém příkladu jsou popsána opatření, která přijal správce před vznikem protiprávního jednání, aby odvrátil riziko jeho vzniku, a opatření, která pomohou následně snížit riziko pro práva a svobody subjektů údajů. Dále se u každého příkladu nachází posouzení rizika, hodnocení kroků k odvrácení rizika a doporučená organizační a technická opatření k jeho minimalizaci.

Weinhold Legal