24. 2. 2021

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

# Pokut za porušení GDPR přibývá, jak jim předejít?

Letos to budou tři roky od účinnosti nařízení GDPR a otázka možných sankcí je stále velice aktuální. Jak vyplývá z reportu DLA Piper[1] shrnujícího uplynulý rok, roste počet pokut i nahlášených případů v členských státech Evropské unie včetně České republiky.

Oproti loňskému roku evropské úřady zaznamenaly téměř o pětinu více porušení nařízení spojených s GDPR, rovněž byly uloženy i vyšší pokuty, a to i přes to, že velké množství pokut bylo nakonec sníženo úspěšnými odvoláními.

Doposud nejvyšší pokuta byla udělena francouzským úřadem CNIL v lednu 2019, která dosahovala 50 milionů EUR, následuje úřad v německém Hamburku, který v říjnu 2020 pokutoval nejmenovaný maloobchod za nedostatečný právní základ zpracování osobních údajů částkou 35 milionů EUR. Třetí je pak italský úřad Garante, který v lednu 2020 udělil pokutu telekomunikačnímu operátorovi za několik rozdílných prohřešků, zejména za neadekvátní technické a organizační opatření k ochraně osobních údajů, nedostatečný právní základ pro zpracování osobních údajů či nedostatečný *„privacy by design*" – tato pokuta pak dosáhla výše 27 milionů EUR.

**Jak se vyhnout pokutám?**

Z nedávno zveřejněné studie vyplývá několik hlavních oblastí, kde správci osobních údajů nejčastěji chybují a kde je nutno dávat zvláštní pozor:

1. Transparentnost – v praxi je nutné mít kompletní, přesné a přehledné oznámení o ochraně osobních údajů, ideálně se všemi potřebnými informacemi na jednom místě;
2. Právní základ – jak je zjevné z krátkého shrnutí pokut výše – je nutné se vždy opírat o vhodný titul ke zpracování osobních údajů a ten dodržet, tedy například, pokud se jedná o souhlas, tak je nutné ho platně získat, vše se musí opírat o správně provedený data mapping a poctivé vedení záznamů o činnostech zpracovávání;
3. Nedostatečná implementace zabezpečení – během posledních 12 měsíců bylo uloženo velké množství pokut právě pro to, že regulátoři došli k názoru, že nebylo dostatečně implementováno nutné zabezpečení, typicky:
    a. Monitoring administrátorských účtů;
    b. Monitoring přístupu do databází, které obsahují osobní údaje;
    c. Šifrování osobních údajů;
    d. Použití vícefaktorové autentizace k předejití neoprávněnému přístupu;
    e. Logování neúspěšných přihlášení;
    f. Manuální kontrola zdrojových kódů apod.
4. Porušení zásady minimalizace dat a principů ukládání dat – zpracovávání příliš velkého množství dat (z nichž může být část i zcela zbytečná) a jejich ukládání na příliš dlouhou dobu zvyšuje riziko úniku, a proto i tato oblast byla regulátory často pokutována;
5. Nedostatečné zajištění přenosu osobních údajů do zahraničí (třetích zemí) – ve velkém množství případů vůbec neprobíhá kontrola, mapping a zhodnocení, nakolik takový přenos představuje ohrožení pro subjekty přenášených osobních údajů. Je nutné rovněž správně implementovat standardní smluvní doložky.

**Co říkají statistiky**

Nejvyšší pokuty plynoucí z GDPR byly v evropských státech uděleny v následujících zemích: Itálie, Německo, Francie, Velká Británie, Španělsko a Švédsko. Ve vztahu k těmto zemím je možné hovořit o tom, že jejich regulátoři zaujali velice přísný postup. Na opačném pólu pak nalezneme Estonsko, Lichtenštejnsko, Island, Rakousko, Litvu a Lotyšsko, kde jsou pokuty nejnižší. V případě Estonska zatím v součtu pouhých 408 EUR. Zbylých šestnáct zemí, zahrnujících i Českou republiku, Slovensko či Polsko je pak přibližně uprostřed evropského žebříčku a regulátoři zde stále „testují", kam až je možné zajít.

Co se týče nahlašování, tak nejvíce porušení osobních údajů (*personal data breaches*) bylo od účinnosti GDPR nahlášeno v Německu (více než 77.000 porušení) a Nizozemsku, následováno Velkou Británií, Dánskem, Irskem, Polskem, Švédskem a Finskem. Nejméně naopak v Lichtenštejnsku (pouhých 50 porušení), na Kypru, v Chorvatsku, Litvě a Lotyšsku. Opět je Česká republika s 1.031 případy přibližně v polovině spektra. Situace se trošku změní při přepočtení počtu porušení na počet obyvatel (resp. při indikaci počtu porušení na 100.000 obyvatel) – v tu chvíli je nejvíc porušení hlášeno v Dánsku, následně v Nizozemsku, Irsku, Slovinsku, Finsku a na Islandu. Česká republika patří mezi pět nejméně nahlašujících.

**Závěr**

Z reportu mapujícího tuto problematiku za uplynulé období lze vypozorovat trend, kdy se národní regulátoři již nebojí udělovat  vysoké pokuty, a rovněž že nejpřísnější úřady jsou v západní Evropě. Česká republika se drží počtem a výší pokut přibližně uprostřed evropského žebříčku, nicméně i Úřad pro ochranu osobních údajů bude s nejvyšší pravděpodobností své sankce v příštích letech zvyšovat. Společnostem nakládajícím s osobními údaji doporučujeme nebrat otázku jejich ochrany na lehkou váhu a zvýšenou měrou se soustředit na oblasti vypsané výše, které byly v minulosti dle názoru regulátorů porušovány nejčastěji.

**JUDr. Jan Metelka, LL.M.,**
Associate

DLA Piper Prague LLP, organizační složka

Panská 854/2
110 00  Praha 1

Tel.:  +420 222 817 111

e-mail: prague@dlapiper.com

---

[1] Pro úplné informace prosím stáhněte plnou verzi reportu nk dispozici >>> zde.



## Další články:


- Vybrané otázky poskytování zdravotních služeb na dálku
- DEAL MONITOR
- „Za každou kauzou je živý příběh“
- Ombudsman na Maltě – základní parametry a role. A v čem bychom se mohli poučit i my v Česku?
- DEAL MONITOR
- DEAL MONITOR
- Rozhovor s JUDr. Veronikou Janoušek Rudolfovou, samostatnou advokátkou specializující se na sportovní právo
- DEAL MONITOR
- DEAL MONITOR
- DEAL MONITOR
- Fotbaloví agenti vs. FIFA ve světle stanoviska generálního advokáta Soudního dvora Evropské unie