Kvůli nesprávně nastaveným pravidlům pro výkon funkce pověřence v rámci GDPR může společnost přijít o statisíce korun. Jaká jsou základní pravidla pro fungování pověřence ve firmě?

GDPR: Pověřenec jako důvod pro uložení pokuty

Po účinnosti nařízení GDPR jsme se mohli setkat s názorem, že pro image společnosti je lepší, pokud jmenuje pověřence pro ochranu osobních údajů, a to i v případě, kdy jí tuto povinnost zákon neukládá. Tento pohled však v poslední době významným způsobem posunulo hned několik evropských úřadů pro ochranu osobních údajů, které se tématu nominace a reálného fungování pověřence věnovaly – a padaly i nemalé pokuty.

Prvním z dozorových úřadů, který se tématu jmenování pověřence věnoval, byl belgický úřad. Uložil pokutu ve výši 50 tisíc eur za to, že pověřencem byla jmenována nevhodná osoba, které byly navíc omezeny pravomoci. Pokutovaná společnost jmenovala pověřencem vedoucího oddělení interního auditu a compliance. S obdobným nastavením se často setkáváme v praxi i u nás. Jedním ze základních atributů pověřence je jeho nezávislost, která v tomto případě dle dozorového úřadu nebyla dodržena. Pokutovaná společnost totiž neimplementovala směrnici řešící konflikt zájmů mezi výkonem funkce pověřence a interního auditora. Pověřenec tedy nemohl jednat nestranně, pokud šlo o jeho vlastní oddělení interního auditu a compliance. Osoba vykonávající funkci pověřence zastávala tuto funkci vedle svého hlavního pracovního poměru a nebyla zahrnuta do řešení všech okolností zpracování osobních údajů. Například nebyla zapojena do vyšetřování bezpečnostních incidentů, což lze označit za jednou z hlavních odpovědností pověřence.

Podobným případem, řešícím konflikt zájmů, byl případ lucemburské společnosti, která jmenovala pověřencem vedoucího svého compliance oddělení, primárně zodpovědného za kontrolu protikorupčního jednání, AML, a kontroly dodavatelů.[1] Společnost již během kontroly jmenovala nového pověřence, nepodařilo se jí však odstranit konflikt zájmů, pouze jej přenést na jiné oddělení. Pokuta zde přesto uložena nebyla.

1 Luxembourg data protection authority (CNPD), případ č. 19FR/2021 ze dne 31. 5. 2021.

Foto: Shutterstock

Externí pověřenci

Lucemburský úřad pro ochranu osobních údajů řešil v minulém roce několik podobných případů. V červnu uložil pokutu 15 tisíc eur[2] za nedostatečnou dokumentaci postavení pověřence v organizační struktuře společnosti, chybějící plán kontrol a neuspokojivou dokumentaci zdrojů pověřence pro výkon jeho úkolů. Následně v říjnu uložil pokutu 18 tisíc eur orgánu veřejné správy za nedostatečnou dokumentaci procesů potvrzujících zahrnutí pověřence do všech záležitostí týkajících se ochrany osobních údajů a poskytnutí zdrojů nezbytných pro plnění úkolů pověřence. V daném případě orgán veřejné správy přijal model, kdy formálně jmenoval pověřenci své dva zaměstnance, ale jejich činnost outsourcoval na externí společnost. Ta řešila každodenní úkoly pověřenců, aniž by oba pověřenci zasahovali či jakkoliv koordinovali činnost externího dodavatele.[3] Daný model se vyskytuje i v České republice: s příchodem GDPR je pověřencem jmenovaný jeden zaměstnanec, který však práci nestíhá, tudíž začne úkoly zadávat externí společnosti. Časem již externí společnost řeší veškeré úkony sama, aniž by do její činnosti jmenovaný pověřenec zasahoval. Tudíž existují paralelně dva pověřenci, jeden formálně jmenovaný a druhý faktický, který řeší veškeré záležitosti. Lucemburský úřad pro ochranu osobních údajů v daném případě tuto dvoukolejnost vyhodnotil jako porušení článku 37 odst. 6 a 7 GDPR.

Podobně v říjnu 2021 řešil lucemburský úřad hned několik kontrol týkajících se výkonu činnosti pověřence a opět padaly pokuty: první se týkala porušení nahlášení porušení zabezpečení osobních údajů. Úřad v tomto případu mimo jiné poukazoval na nemožnost komunikovat s pověřencem společnosti, jehož kontaktní údaje nebyly u úřadu aktualizovány. Celková výše pokuty se následně vyšplhala na 135 tisíc eur.[4]

2 Luxembourg data protection authority (CNPD), případ č. 20FR/2021 ze dne 11. 6. 2021.
3 Luxembourg data protection authority (CNPD), případ č. 38FR/2021 ze dne 15. 10. 2021.
4 Luxembourg data protection authority (CNPD), případ č. 31FR/2021 ze dne 5. 8. 2021.

Vzápětí uložil jiné společnosti pokutu 15 tisíc eur[5] za nedostatečné doložení činnosti pověřence. Zajímavé je, že společnost doložila veškeré procesy a dokumenty dokazující compliance. Nedokázala však doložit podílení se svého pověřence na tvorbě nebo revizi těchto dokumentů. Mezi další pochybení patřila organizační struktura společnosti, kdy pověřenec reportoval vedení společnosti přes několik manažerů nad ním. Jednalo se tak o přímé porušení článku 38 odst. 3 GDPR, jenž vyžaduje přímý přístup pověřence k vedení společnosti – správce osobních údajů. Posledním z nejzávažnějších porušení byla neexistence plánu kontrol pověřence.

U jiné společnosti, kontrolované v listopadu 2021, Lucemburský úřad pro ochranu osobních údajů shledal, že pověřenec dostával úkoly, které jsou v přímém rozporu s čl. 38 odst. 3 GDPR. Ani v tomto případě pověřenec nepředložil kontrolní plán.[6] Celková pokuta byla uložena ve výši 18 700 eur. Na konci listopadu 2021 potom lucemburský úřad uložil zatím nejvyšší pokutu týkající se pověřence, a to 80 tisíc eur.[7] Společnost provozovala věrnostní systém, ve kterém zpracovávala velké množství osobních údajů, navíc konstantě monitorovala nákupy svých zákazníků. I přes tyto skutečnosti nesprávně vyhodnotila, že nemusí jmenovat pověřence dle čl. 37 odst. 1 GDPR.

Vodítka pro pověřence

V návaznosti na vydaná rozhodnutí a porušení lucemburský úřad poskytl vodítko ohledně výkonu úkolů pověřence, mezi které mimo jiné patří:

- provedení analýzy povinnosti jmenovat pověřence[8];
- oznámení kontaktních údajů pověřence dozorovému úřadu, včetně jejich včasné aktualizace, protože neaktuálnost kontaktních údajů je příčinou navýšení ukládané pokuty za porušení[9];
- zveřejnění kontaktních údajů pověřence na webových stránkách a v interních dokumentech;
- odborná způsobilost pověřence – proškolení, odpovídající vzdělání a zkušenosti;
- nastavení procesů společnosti tak, aby nedošlo ke konfliktu zájmů (případně lze řešit jmenováním externího pověřence a správným nastavením spolupráce s ním);
- přidělení dostatečných zdrojů pověřenci tak, aby mohl svoji funkci vykonávat efektivně;
- zahrnutí pověřence do veškerých záležitostí, týkajících se zpracování osobních údajů společnosti;
- pověření pověřence výkonem poradenství pro správce osobních údajů i jeho zaměstnance;
- zapojení pověřence do hodnocení rizik jakékoliv nové zpracovatelské činnosti.

Významná pozornost je v rámci kontrol věnována kvalifikaci pověřence. Určitým vodítkem v tuzemském kontextu může být text zveřejněný Úřadem pro ochranu osobních údajů nazvaný Postavení a úkoly pověřence, který se problematice věnuje. Případně, opět z vnějších zdrojů, významně detailnější popis vydaný irským úřadem pro ochranu osobních údajů, který např. mezi základní požadavky na znalosti pověřence řadí:

- detailní znalost národního a evropského práva týkajícího se ochrany osobních údajů;
- přehled o veškerých činnostech, při nichž dochází ke zpracování osobních údajů ve společnosti;
- znalost problematiky IT a zabezpečení údajů;
- znalost odvětví a konkrétní společnosti;
- schopnost propagace a zlepšování kultury ochrany osobních údajů ve společnosti.

Dobrovolné jmenování pověřence s sebou nese výhody, zejména lepší zajištění procesů a pravidel vyžadovaných GDPR a s tím se pojící větší důvěru ohledně nakládání osobními údaji správcem, jak dovnitř, tak i na venek. To potom vede nejen k omezení compliance rizik, ale též ke zvýšení prestiže a hodnoty společnosti správce. Z výše popsaných případů z poslední doby je ale zřejmé, že verze *„imidžového pověřence“* s sebou stejně tak nese významná rizika. Z evropské rozhodovací praxe totiž plyne, že nestačí pouze formálně jmenovat pověřence, ale že společnost jako správce osobních údajů musí být schopná prokázat, že vybrala tu správnou osobu, které zajistila opravdovou nezávislost výkonu funkce a přidělila odpovídající kompetence a prostředky. Dále musí být připravena kdykoli demonstrovat, že má nastavený funkční systém kontrol a dalšího zapojení pověřence do všech relevantních činností a v neposlední řadě nesmí opomenout jeho kontakty publikovat jak vůči veřejnosti, tak vůči dozorovému úřadu. Jinak se vystavuje riziku uložení pokuty.

Jitka S. Ivančíková
advokát,
FairData Professionals

Jaroslav Šuchman
vedoucí advokát,
Havel & Partners

5 Luxembourg data protection authority (CNPD), případ č. 40FR/2021 ze dne 27. 10. 2021.
6 Luxembourg data protection authority (CNPD), případ č. 41FR/2021 ze dne 27. 10. 2021.
7 Luxembourg data protection authority (CNPD), případ č. 42FR/2021 ze dne 27. 10. 2021.
8 Za nedostatečné vyhodnocení, zdali společnost má či nemá mít jmenovaného pověřence, ukládaly dozorové úřady pokuty již od začátku účinnosti GDPR. Z poslední doby můžeme uvést pokuty uložené řeckým dozorovým úřadem, HDPA, ze dne 29. 12. 2021 (případ č. 55/2021), ve kterém řecké Ministerstvo pro cestovní ruch dostalo pokutu za nejmenování pověřence. Nerespektování dané povinnosti představovalo jedno z hlavních porušení, pro něž ministerstvo dostalo pokutu 75 tisíc eur.
9 Z poslední doby můžeme uvést případy např. italského dozorového úřadu, Garante, který uložil 10. 3. 2022 pokutu správci za to, že údaje pověřence nahlášené úřadu již nebyly aktuální. Celková pokuta za více pochybení byla 6000 eur (rozhodnutí č. 98 z 10. 3. 2022, Caltanissetta Provincial Health Authority). Podobně rozhodnutí belgického dozorového úřadu ze 4. 4. 2022, které se týkalo měření tělesné teploty na belgickém letišti Charleroi, zahrnovalo porušení kontrolovaného subjektu ohledně nenahlášení správných údajů o pověřenci dozorovému úřadu. Celková pokuta v daném případě byla dokonce 100 tisíc eur (rozhodnutí č. DOS-2020-04002 proti Brussels South Charleroi Airport SA). Posledním z nedávných případů je případ polské pobočky bank Santander Bank Polska, S.A.: vedle dalších pochybení byla též za neaktuálnost kontaktních údajů pověřence na webových stránkách a v registru vedeném polským dozorovým úřadem uložena pokuta ve výši 545 748 PLN (cca 120 000 eur) (případ č. DKN.5131.33.2021 ze dne 22. 2. 2022).