TEXT MGR. LENKA GOMEZ TOMČALOVÁ, MGR. TOMÁŠ MATĚJKA, Z/C/H LEGAL V.O.S., ADVOKÁTNÍ KANCELÁŘ

Whistleblowing v kontextu ochrany osobních údajů

Dlouho očekávanou právní úpravu whistleblowingu, která se v České republice zhmotnila v podobě zákona o ochraně oznamovatelů a částečně již vstoupila do života českých zaměstnavatelů a zaměstnanců, může provázet poněkud rozpačité přijetí.

Kromě toho, že whistleblowing s sebou může nést pachuť „donašečství“, mohou jej někteří vnímat jako zavedení povinností, které by měly zůstat výhradně dobrovolné. Jiní v něm naopak spatřují cestu ke zlepšení firemní kultury a posílení ochrany zaměstnanců i zaměstnavatelů.

Správná implementace může být přínosem

Autoři článku se domnívají, že whistleblowingu rozhodně není nutné se obávat. Zkušenost ze zahraničí, jakož i zkušenost společností, které obdobné systémy již v České republice dobrovolně zavedly, ukazuje, že správná a efektivní implementace whistleblowingu má převážně pozitivní přínosy. Společnosti, které mají takový systém zaveden zpravidla řeší méně soudních sporů se zaměstnanci, mají nižší náklady na vypořádání se s nimi a bývá o nich rovněž méně negativních zmínek v médiích. Whistleblowing navíc přispívá k budování zdravé, bezpečné a odpovědné firemní kultury, stejně jako ke zlepšení podmínek na pracovišti.

Whistleblowing spočívá v možnosti oznámit protiprávní chování, ke kterému dochází v rámci společnosti, případně jiného subjektu. Důvodnost oznámení posuzuje tzv. příslušná osoba, která zaměstnavateli jako povinnému subjektu následně navrhuje přijetí opatření. Zaměstnavatel je povinen zajistit, aby oznamovatel v souvislosti s učiněním oznámení nebyl vystaven tzv. odvetnému opatření.

Práva a povinnosti přímo související s whistleblowingem dopadají i na veřejnoprávní subjekty. V článku se nicméně zaměříme výhradně na společnosti ze soukromoprávního sektoru.

Povinnosti zaměstnavatelů

U společností s více jak 250 zaměstnanci by již měly vnitřní systémy fungovat tak, aby naplňovaly požadavky zákona o ochraně oznamovatelů. Zaměstnavatelé s více než 50 a méně než 250 zaměstnanců mají čas připravit se na nové povinnosti až do 15. prosince 2023.

O základních povinnostech zaměstnavatelů – povinných subjektů již zaznělo mnoho. Proto tyto základní povinnosti níže jen stručně shrneme. Jde o:

- povinnost zajistit oznamovatelům možnost podat oznámení prostřednictvím vnitřního oznamovacího systému;
- povinnost určit příslušnou osobu;
- povinnost uveřejnit stanovené informace způsobem umožňujícím dálkový přístup;
- zákaz bránit v podání oznámení;
- zákaz použití tzv. odvetných opatření proti oznamovateli.

Již méně diskutovaným tématem je vztah whistleblowingu a ochrany osobních údajů. V rámci podávání a vyhodnocování oznámení, stejně jako navrhování ochranných opatření, nevyhnutelně dochází ke zpracovávání a uchovávání informací, které mají charakter osobních údajů. Právní úprava whistleblowingu tedy naráží na právní úpravu obsaženou v rámci GDPR a v zákoně o zpracování osobních údajů, a to v různých ohledech.

Dodržování ochrany soukromí

Předně se samotné oznámení může týkat porušení pravidel na ochranu soukromí. Příslušná osoba tedy musí být schopna posoudit, zda je oznámení relevantní a zda skutečně došlo či dochází k porušování pravidel na ochranu soukromí. Typicky může jít o situace, kdy byly osobní údaje zpracovány protiprávním způsobem nebo došlo k jejich neoprávněnému využití či nedostatečnému zabezpečení jejich ochrany.

Povinné subjekty musí zajistit dodržování pravidel na ochranu soukromí při zpracování osobních údajů v rámci vnitřního oznamovacího systému. Jelikož je vnitřní oznamovací systém veden povinným subjektem, stává se povinný subjekt nevyhnutelně správcem osobních údajů ve smyslu GDPR. Příslušná osoba, která osobní údaje fakticky zpracovává, je tak v postavení zpracovatele osobních údajů.

Příslušná osoba bude v souvislosti s oznámením zpravidla zpracovávat osobní údaje oznamovatele, osoby, proti které oznámení směřuje, „poškozené osoby“ a případných svědků. Ke zpracovávání osobních údajů by mělo docházet v poměrně omezeném rozsahu, a to vždy pouze pro účely konkrétního oznámení. Je třeba identifikovat jen ty osobní údaje, které je v souvislosti s oznámením nutné zpracovávat. Ostatní osobní údaje nad tento rámec by zpracovávány být neměly.

Jelikož zákon o ochraně oznamovatelů vyžaduje identifikaci oznamovatele, vyplývají pro něj z případného úniku osobních údajů zásadní rizika. Není těžké si představit, že v důsledku úniku může být oznamovatel vystaven diskriminaci, dehonestaci nebo přímo odvetným opatřením ve smyslu zákona o ochraně oznamovatelů. Obdobně to platí o jakýchkoliv dalších osobách, které v rámci oznámení figurují.

Zabránit úniku osobních údajů

Je tedy nutné, aby vnitřní oznamovací systém v maximální možné míře úniku informací zabraňoval. Zejména je třeba zajistit, aby k osobním údajům měla přístup výhradně jen příslušná osoba, která oznámení zpracovává. Zároveň je nutné zvolit optimální technické řešení vnitřního oznamovacího systému. Zákon o ochraně oznamovatelů ukládá povinným subjektům, aby oznamovatelům umožnily podat oznámení písemně, ústně a osobně.

Konvenční prostředky v podobě například dedikované telefonní linky nebo e-mailové či dokonce „fyzické schránky“ nejsou ideálním řešením. Problematické je zpravidla zabezpečení těchto prostředků právě proti úniku osobních údajů, jejich použitelnost pro různé skupiny osob či možnost doložit k oznámení fyzickou dokumentaci. To je například při použití telefonní linky jen těžko představitelné.

Bezpečné nastavení vnitřního oznamovacího systému nelze brát na lehkou váhu. Za poskytnutí údajů o totožnosti oznamovatele a některých dalších osob totiž může hrozit pokuta až ve výši 100.000 Kč. V případě, že by kvůli úniku informací byl oznamovatel vystaven odvetnému opatření, může se případná pokuta vyšplhat až k 1.000.000 Kč.

Nařízení GDPR v zásadě umožňuje uchovávat osobní údaje výhradně po dobu, která je nezbytně nutná pro dosažení účelu uchovávání. Zákon o ochraně oznamovatelů povinnému subjektu stanoví povinnost k uchovávání oznámení a související dokumentace po dobu 5 let od přijetí oznámení.

Je otázkou, zda lze osobní údaje uchovávat i delší dobu. Domníváme se, že to možné je, pokud bude delší doba uchovávání opodstatněna legitimním cílem, tedy například ochranou práv povinného subjektu, třeba v rámci probíhajícího soudního nebo správního řízení.

Třecí plochou může být taktéž požadavek právní regulace ochrany osobních údajů na transparentnost zpracování osobních údajů. Ten může v souvislosti s whistleblowingem narážet na zájem na ochranu oznamovatele a dalších osob. Subjekty, jejichž osobní údaje jsou zpracovávány, mají standardně právo na informace ohledně důvodu zpracování jejich osobních údajů, na přístup k osobním údajům, právo na opravu osobních údajů či jejich výmaz.

Řádný výkon uvedených práv by však mohl znamenat narušení procesu prověřování oznámení či odhalení totožnosti oznamovatele nebo jiných osob, proto se zde nevyhnutelně musí uplatnit zvláštní výjimka, na základě které může být výkon těchto práv omezen z důvodu nezbytnosti k zajištění důležitého cíle veřejného zájmu a ochrany práv a svobod osob.

Ochranu osobních údajů v souvislosti se zákonem o ochraně oznamovatelů tedy nelze brát na lehkou váhu a je nutné své vnitřní systémy nastavit i v tomto směru odpovídajícím způsobem. /