Rozhovor s **Jiřím Žůrkem**, ředitelem odboru konzultačních agend ÚOOÚ

Kolik závažných případů porušení zabezpečení již bylo ohlášeno? Co poradit pověřencům, kteří se často setkávají s neochotou vedení udělat patřičné změny? Zeptali jsme se JUDr. Jiřího Žůrka z Úřadu pro ochranu osobních údajů.

JUDr. Jiří Žůrek vystudoval Právnickou fakultu Univerzity Karlovy v Praze a specializuje se na ochranu osobních údajů. Na Úřadu pro ochranu osobních údajů působí jako ředitel odboru konzultačních agend. Je držitelem mezinárodního certifikátu CIPP/E.

V době okolo účinnosti GDPR vzrostl počet dotazů na ÚOOÚ. Opadla již tato vlna, nebo je Úřad i nadále dotazy zahlcován? Pominuly již nejasnosti, které firmy v oblasti GDPR mají?

Největší nápor dotazů ohledně GDPR byl od začátku roku 2018 až do počátku letních prázdnin, kdy jsme skutečně evidovali až dvojnásobek dotazů, než bylo obvyklé za srovnatelné období předchozího roku. Pomoci veřejnosti s GDPR a také vyvrátit mýty, které kolem něj panovaly, jsme se pokusili i výraznou aktualizací a transformací sekce často kladených otázek a průběžným doplňováním informačních dokumentů na stránkách ÚOOÚ tak, aby si z nich vybral každý, tj. jak drobný živnostník, tak profesionál-pověřenec. Od účinnosti GDPR jsme začali provozovat informační linku, jejímž účelem je poskytovat rychlé odpovědi na jednodušší otázky, zejména u malých a středních podnikatelů.

V současné době je patrně největší vlna dotazů za námi. Ve spojitosti s dotazy bych rád zmínil, že ÚOOÚ je především dozorovým úřadem, jehož primární rolí je monitorovat a vymáhat dodržování GDPR. Nemůže tak nahrazovat metodickou činnost například ministerstev nebo roli profesních sdružení v odpovídání na dotazy, a už vůbec ne roli pověřenců. Kvalifikovaným dotazům od pověřenců však věnujeme v rámci konzultační agendy zvýšenou pozornost. Kvalifikovaným dotazem se rozumí nikoliv pouhé položení otázky, ale současné zaslání analýzy daného problému. Jinými slovy musí být z dotazu patrné, že se jím pověřenec odborně zabýval. Pověřencům doporučuji rubriku Pověřenci v sekci GDPR na stránkách ÚOOÚ.

K otázce nejasností ve vztahu ke GDPR je možné konstatovat, že u většiny právních předpisů, ačkoliv jde o negativní jev, budou vždy panovat větší či menší výkladové nejasnosti z důvodu jejich aplikace na konkrétní životní situace. S ohledem na fakt, že je GDPR velmi obecným právním předpisem, se lze v praxi mnohdy setkat s hraničními případy. Na druhou stranu některé nejasnosti již vyřešily například pokyny Evropského sboru pro ochranu osobních údajů. U dalších to lze očekávat s účinností tzv. adaptačního zákona.

S jakými dotazy se na vás veřejnost nejčastěji obrací?

Jelikož ochrana osobních údajů při jejich zpracování prolíná celým spektrem života, setkáváme se s velmi pestrou paletou dotazů od všech možných správců či zpracovatelů, ale samozřejmě i od subjektů údajů.

Na přelomu účinnosti GDPR jsme velmi často dostávali dotazy, zda musí konkrétní organizace pověřence jmenovat, či nikoliv. V této oblasti již došlo k určité kultivaci, organizace si už vesměs určily, zda se na ně taková povinnost vztahuje, nebo ne. Velmi často se setkáváme s dotazy na právní důvod konkrétního zpracování a dále na výklad některých institutů GDPR, či přímo jejich aplikaci v praxi v konkrétním případě. Tazatele též zajímá, jaké jsou možnosti šířit obchodní sdělení.

Pokud přijde na ÚOOÚ stížnost, jak Úřad konkrétně postupuje?

Na úrovni odboru konzultačních agend se vyhodnotí obsah stížnosti a následně se rozhoduje o dalším postupu. Při odůvodněném podezření z porušení GDPR postupujeme v rámci ÚOOÚ věc kontrolnímu odboru k dalším opatřením, u méně závažných podezření na úrovni odboru konzultačních agend nejprve informujeme správce či zpracovatele o jeho povinnostech, přičemž očekáváme, že se k možnému problému postaví aktivně čelem a zjedná nápravu, aniž by bylo nutné dále formální porušení GDPR řešit. Tyto informativní dopisy se velmi osvědčily a vesměs jsou prostředkem rychlé nápravy drobného prohřešku. U nedůvodných stížností stěžovatele informujeme, proč jsme neshledali podezření z porušení GDPR. Některé stížnosti také samozřejmě postupujeme jiným příslušným orgánům či Policii České republiky.

Jak zabránit tomu, aby GDPR bylo nástrojem vyřizování účtů v rámci konkurenčního boje?

Nejlepším řešením je být v souladu s GDPR, jelikož tím organizace výrazně sníží manévrovací možnosti při podávání účelové stížnosti. V tuto chvíli nevíme o případu, kdy by se GDPR zjevně stalo nástrojem pro vyřizování účtů v rámci konkurenčního boje, ačkoli samozřejmě nelze takové účelové podněty vyloučit. Primárně se však ve stížnostní agendě věnujeme stížnostem přímo dotčených subjektů údajů.

Jak konkrétně dopadne český adaptační zákon na pověřence, potažmo na celé firmy a organizace? Co musejí po předchozí implementaci GDPR opět změnit?

Konečná podoba adaptačního zákona ještě není v tuto chvíli známa, ačkoli je alespoň již dostupná jeho podoba schválená Poslaneckou sněmovnou. Pro většinu správců a zpracovatelů by neměla účinnost adaptačního zákona představovat nové „implementace", jelikož povinnosti stanovuje přímo GDPR a ty musejí zohledňovat již nyní. Každá organizace si, stejně jako u jakéhokoliv jiného předpisu dotýkajícího se její činnosti, musí sama určit, v jakém rozsahu a do jaké míry se na ni vztahuje a jak ovlivní její činnost, a tomu se přizpůsobit.

Kolik případů porušení zabezpečení bylo ohlášeno? Byla tato porušení závažná?

Doposud ÚOOÚ obdržel přes 200 ohlášení porušení zabezpečení osobních údajů. Obsahově jsou velmi různorodá a samozřejmě se mezi nimi našla i porušení závažná. Pověřencům doporučuji, aby se vždy, pokud budou přistupovat k ohlašování porušení zabezpečení, ujistili, že ohlášení obsahuje náležitosti dle čl. 33 odst. 3 GDPR. Velmi často se totiž zapomíná na popis pravděpodobných důsledků nebo na popis opatření, která byla přijata či navržena k vyřešení daného porušení zabezpečení.

Co je největším nedostatkem u kodexů chování, s nimiž se na vás obracejí sdružení nebo jiní zástupci správců či zpracovatelů s žádostí o jejich schválení?

Obecně by se za největší nedostatek dalo označit nepochopení účelu a funkce kodexu chování. To se pak odráží v tom, že Úřad obdrží návrh

Účelem kodexu chování není opětovné stanovování či přepisování povinností, které již vyplývají z GDPR, ale jejich upřesnění s ohledem na charakteristiky daného odvětví či sektoru.

kodexu chování, který z větší části obsahuje pouze předpis ustanovení GDPR, a nereflektuje specifika daného odvětví, čímž nesplňuje požadavky na obsah kodexu chování jako takového. GDPR je obecným právním předpisem upravujícím pravidla pro zpracování osobních údajů, která se musejí aplikovat na zpracování prováděná správci či zpracovateli v určitých odvětvích.

Představme si banku, nemocnici a cestovní kancelář. Společné mají to, že zpracovávají osobní údaje, ale každý tento subjekt se bude v praxi při aplikaci GDPR potýkat s různými otázkami či problémy. A kodex chování by měl sloužit k tomu, aby právě správcům či zpracovatelům v různých odvětvích ukázal správnou cestu, jak na to, tj. měl by zohledňovat specifika daného odvětví a upřesňovat chování konkrétního správce či zpracovatele v rámci pravidel GDPR v daném odvětví.

Dalším vysledovatelným nedostatkem je cílení na malou skupinu správců či absence zdůvodnění potřeby a obsahu kodexu. Též zpravidla chybějí doložení proběhlých jednání nezbytných před zahájením tvorby kodexu, která dokladují, že na zpracování kodexu a jeho obsahu panuje v rámci daného odvětví širší shoda.

S čím se podle vaší zkušenosti pověřenci v praxi nejvíce potýkají? A jak jim v tom ÚOOÚ může pomoci?

Institut pověřenců obecně přispěje – a již i přispívá – ke kultivaci prostředí zpracování osobních údajů. S činností pověřence úzce souvisí i přístup organizace k ochraně osobních údajů, tzn. jak funkci pověřence chápe. Pokud ji chápe jako příležitost být zase o něco lepší, dá se konstatovat, že se u ní pověřenec nebude potýkat s výraznými problémy, jelikož bude mít zpravidla dostatečné zázemí k řádnému plnění úkolů a jeho funkce bude v organizaci respektována.

Je-li pověřenec v organizaci vnímán jen jako nutné zlo, pak je pravděpodobnější, že se bude skutečně s různými překážkami setkávat. Nadto je otázkou, zda bude v takové organizaci skutečně působit i kvalitní pověřenec. Jednou z překážek může být rovněž nedostatečná komunikace ze strany správce vůči pověřenci, s čímž jsme se již setkali u případu, kdy organizace komunikovala s ÚOOÚ, aniž by o tom pověřenec věděl.

Jednou z překážek může být nedostatečná komunikace ze strany správce vůči pověřenci

Co byste poradil pověřencům, kteří se často setkávají s neochotou vedení udělat patřičné změny?

Vysvětlit účel pověřence pro ochranu osobních údajů. To, že některé organizaci vznikne povinnost jmenovat pověřence, již značí, že provádí do jisté míry rizikové zpracování osobních údajů. Je tudíž namístě, aby existovala konkrétní osoba, která bude na soulad zpracování dohlížet z pohledu compliance. Organizaci se to vrátí tím, že výrazně sníží riziko nesprávných postupů při zpracování osobních údajů, a tedy i riziko pokuty.

Je také nutné si uvědomit, že veřejnost dnes osobní údaje vnímá velmi citlivě a nesprávné postupy při jejich zpracování mohou vyústit i v medializaci, což může mít velmi negativní vliv na reputaci organizace a v konečném důsledku horší dopad než „pouze“ udělená pokuta. Proto je důležité být návrhům pověřence otevřený. Každý navrhovaný krok by však měl pověřenec patřičně zdůvodnit, čímž sníží riziko, že by organizace bezdůvodně odmítala přijmout jeho návrhy ke zlepšení procesů spojených se zpracováním osobních údajů.

▪▪▪