Jiří Kaucký (*1973)

Vystudoval Právnickou fakultu Univerzity Karlovy v Praze. Předsedou Úřadu pro ochranu osobních údajů byl jmenován v září roku 2020. Předtím byl ředitelem správního odboru Ministerstva vnitra ČR, kde byl do jara roku 2020 státním tajemníkem. Ve státní správě působí po dvě desetiletí. Byl předsedou Etické komise České republiky pro ocenění účastníků odboje a odporu proti komunismu a před jmenováním do funkce předsedy ÚOOÚ měl členství i v dalších poradních orgánech. Krom jiných publikací zaměřených na správní řízení je spoluautorem komentáře k zákonu o státní službě.

Marika Vitnerová

Jiří Kaucký: V souvislosti s kybernetickými útoky je třeba klást důraz na prevenci

Téma ochrany osobních údajů vyvolalo spoustu pochybností ještě před účinností GDPR, zejména se hovořilo o astronomických pokutách. Jak se daří popularizovat povědomí o normě, která už čtyři roky v českém právu funguje, a jak mají správci systémů postupovat v případě kybernetického útoku, nejen o tom jsme v rozhovoru mluvili s Jiřím Kauckým, předsedou Úřadu pro ochranu osobních údajů.

Ochrana osobních údajů a nakládání s nimi rezonovalo zejména v době před účinností GDPR. Kam se Úřad od té doby posunul?

Obecně by se dalo říci, že před přijetím GDPR u nás ochrana osobních údajů přešlapovala na okraji propasti a všichni se báli, že se posuneme ještě o krok dále. To se ale nestalo. Naopak, mám za to, že jistá panika, která před přijetím GDPR panovala, měla pozitivní efekt – ochrana osobních údajů přestala být vnímána jako něco, co se vyčerpává tím, zda kamery na domě občana A zabírají kousek veřejného prostranství před jeho domem, a do obecného povědomí se dostal obrovský rozsah zpracování osobních údajů, k němuž neustále dochází, i nutnost jejich důsledné ochrany. GDPR, trestněprávní směrnice a jejich implementace do českého právního řádu prostřednictvím zákona o zpracování osobních údajů skutečně přinesly zásadní změnu. V první řadě je to širší evropský rozměr.

V čem se to tedy změnilo?

Dříve ÚOOÚ vydával svá vlastní stanoviska k problémům ochrany osobních údajů a po implementaci GDPR v roce 2018 se najednou těžiště regulace ochrany osobních údajů přeneslo na úroveň Evropské unie, a to včetně rozhodování některých konkrétních případů. Konkrétně tedy na úroveň Evropského sboru pro ochranu osobních údajů (EDPB), jehož jsme zároveň členy. Národní pozice, pokud nemají přesah do jiného členského státu EU, pak vydávají jednotliví regulátoři. Za pozitivní bych označil naprostou nezávislost našeho Úřadu v České republice. To se zásadně projevilo při pandemii koronaviru. GDPR došlo k jasnému vymezení role Úřadu pro ochranu osobních údajů jakožto nezávislé „exekutivy“ ochrany osobních údajů, ale dokonce i maličké součásti zákonodárné moci, a to ve vztahu odpovědnosti za přípravu a nastavení systému ochrany osobních údajů, kdy nám GDPR dává pravomoc i bez žádosti poskytovat Parlamentu vyjádření k návrhu právního předpisu, který upravuje zpracování osobních údajů, a my se ji snažíme odpovědně využívat. Zásadním aspektem jednotnosti ochrany osobních údajů je možnost a také povinnost koordinovat přípravy kontrol a stanovisek ve společné evropské síti dozorových úřadů.

Daří se vám popularizovat povědomí o ochraně osobních údajů?

Propagace důležitosti ochrany osobních údajů se dosud děje nárazově v zásadě jako naše reakce na významná společenská témata, čímž nechci říci, že by s tím nebylo obrovské množství práce. Chybí nám však ucelená koncepce propagace ochrany osobních údajů a ochrany soukromí. Systémový problém je zakotven v povaze našeho úřadu jako dozorové instituce, která přichází k problémům s osobními daty většinou až ve chvíli, kdy obdrží podnět, nebo při plnění svých kompetencí dohlíží na dodržování zákona. Pak může veřejnosti prezentovat výsledky svých zjištění. Nelze na to ale svést všechno. Přístup, že „nemůžeme říkat, jak by to bylo dobře, protože pak bychom nebyli nezávislí v kontrole“, neuznávám. Naším cílem je přece výsledek – tedy důsledná ochrana osobních údajů – nikoli nezávislost sama o sobě jako fetiš. Ve svém předchozím působení jsem byl vychován v tom, že metodická činnost je minimálně stejně důležitá jako incidentní kontrola (protože jde o řádný výkon veřejné správy jako takový), a vůbec jsem neměl pocit, že by to nějak ohrozilo důslednost našich kontrol.

Města měla v souvislosti s GDPR obavy z výše postihů. Jaká je v tomto směru praxe?

Před účinností obecného nařízení Úřad při porušení předchozího zákona o ochraně osobních údajů města občas pokutoval. Nemám dost informací, abych posoudil, zda hodně, nebo málo, nicméně se podařilo vzbudit dostačenou averzi vůči tomu, aby při projednávání návrhu stávajícího zákona o zpracování osobních údajů převážilo stávající řešení, tedy že města, stejně jako jiné veřejné subjekty, za porušení GDPR pokutovat nelze. Ve vztahu

k územní samosprávě to zatím v praxi zásadní problémy nečiní, i když z formálního hlediska to může budit zdání, že jako Česká republika porušujeme čl. 83 GDPR, který mimo jiné stanoví, že každý dozorový úřad zajistí, aby ukládání správních pokut za porušení tohoto nařízení bylo v každém jednotlivém případě účinné, přiměřené a odrazující.

V posledních týdnech zesílily kybernetické útoky. Co když se ztratí osobní údaje obyvatel v důsledku kybernetických útoků?

V případě, kdy dojde k úspěšnému hackerskému útoku a budou odcizeny osobní údaje, takzvaná data breach, musí správce všechny případy porušení zabezpečení evidovat a vyhodnotit, je-li potřeba takové porušení nahlásit Úřadu (čl. 33 GDPR). Oznamovat není nutné ty případy, kdy je nepravděpodobné, že by takové porušení mělo za následek riziko pro práva a svobody fyzických osob. Pokud je ovšem pravděpodobné, že určitý případ porušení zabezpečení osobních údajů bude mít za následek vysoké riziko pro práva a svobody fyzických osob, je správce osobních údajů povinen oznámit takové porušení, a to bez zbytečného odkladu, nejen Úřadu, ale i dotčeným subjektům údajů.

Jak na takovou situaci Úřad nahlíží?

Jakkoliv v žádném případě nehodláme trestat oběti například hackerských útoků, jsou případy, kdy správce natolik zásadním způsobem zanedbal své povinnosti chránit osobní údaje, že bude na místě uplatnění sankčních pravomocí. V této souvislosti je třeba klást důraz na otřepaný fakt, že základem je prevence. To znamená udělat vše, co je technologicky, ekonomicky, personálně i administrativně možné. Pokud už přeci jen k porušení zabezpečení dojde, nastupují pro správce zákonné povinnosti, jako právě ohlašovací povinnost, a to nám, i třeba NÚKIBu, spadá-li správce do povinných osob dle zákona o kybernetické bezpečnosti. Důležitá je i minimalizace škod a náprava stavu. Teprve následně se řeší, zda případně bylo možné situaci předejít. Nemůžeme tak položit rovnítko mezi únik dat, způsobený kybernetickým útokem, a sankční odpovědností správce osobních údajů. Vždy je nutné posoudit míru zabezpečení v kontextu zpracování osobních údajů.

Úřad má kromě metodické činnosti i dozorovou činnost. Dodržují obce nařízení o ochraně osobních údajů?

Úroveň dodržování GDPR ze strany obcí je obecně dána jejich skutečnými možnostmi, které jsou objektivně jiné, než jaké mají například jednotlivá ministerstva. My k tomu tak také přistupujeme. Stížnosti, které obdržíme a které směřují proti postupu obcí, se už tradičně týkají zveřejňování osobních údajů žadatelů při zveřejnění žádostí o poskytnutí informací podle zákona č. 106/1999 Sb., o svobodném přístupu k informacím. V těchto případech obce neprovedou na zveřejňovaném dokumentu anonymizaci žadatele. Dalším častým předmětem stížností je zveřejnění záznamů (zápisů) z jednání zastupitelstva nebo rady měst a obcí na internetu, opět bez provedení anonymizace osobních údajů občanů či třetích osob. Tyto příklady jsou ve srovnání s důsledky kybernetických útoků poslední doby poněkud úsměvné. Jakkoli se tyto věci nesmějí zanedbávat, hlavní důraz je nutno klást na co nejlepší ochranu svěřených osobních údajů občanů.

Daří se územním samosprávám skloubit konzultační roli s dozorovou činností tak, aby Úřad nekontroloval sám sebe?

Musím přiznat, že se jedná o velmi důležité a zároveň citlivé věci. Nepřekročitelným mantinelem naší konzultační činnosti je zachování nezávislosti Úřadu při výkonu dozorové působnosti. Naším úkolem nejen ve vztahu k územní samosprávě by mělo být pomáhat těm, kteří o to skutečně stojí. Dozorový úřad ovšem nemůže sloužit jako servisní organizace. Je třeba rovněž mít na zřeteli, že kvalita odpovědi zpravidla odpovídá kvalitě otázky. Při běžné konzultační činnosti nemůže být cílem jakéhokoliv záměru ze strany Úřadu schvalovat či navrhovat k nim jiná řešení, to je odpovědností správce. Pověřenci územních samospráv se při konzultacích s ÚOOÚ dozvědí, jaké nároky a povinnosti na ně GDPR klade, na co všechno pamatovat a zda se nejedná o již známý problém, který jsme prověřili kontrolou. Konzultaci je třeba chápat jako prevenci porušení pravidel. Na druhou stranu i kontrola má zpravidla velký edukativní význam, a to bez ohledu na její výsledek.

> Nemůžeme tak položit rovnítko mezi únik dat, způsobený kybernetickým útokem, a sankční odpovědností správce osobních údajů. Vždy je nutné posoudit míru zabezpečení v kontextu zpracování osobních údajů.

Města často využívají průzkumy názorů a spokojenosti občanů, které radnici umožňují sledovat názory, postoje i potřeby obyvatel. Čeho by se města v tomto případě při zpracování osobních údajů měla vyvarovat?

Tady platí dvě zásadní věci. Předně by se místní samospráva, stejně jako každý jiný správce, měla vyvarovat shromažďování těch osobních údajů, které jsou pro vyhodnocení průzkumu nepodstatné. Zadruhé platí, že pokud si najmu společnost, která za mne průzkum provede či vyhodnotí, jedná se o zpracovatele osobních údajů a obec s ním musí uzavřít zpracovatelskou smlouvu se všemi náležitostmi podle čl. 28 GDPR.

Obce v místech, kde jsou kontejnery pro tříděný odpad, umísťují fotopasti nebo kamery. Mají z důvodu udržení veřejného pořádku v těchto místech pravomoc využívat záznamy a pokutovat?

Fotopasti fungují na podobných principech jako další bezpečnostní nebo sledovací systémy. Nejčastěji je právním důvodem pro zpracování osobních údajů prostřednictvím kamer nebo fotopastí zpracování z důvodu oprávněného zájmu správce (čl. 6 odst. 1 písm. f) GDPR). Pokud je záměrem provozovatele, tedy obce, využití fotopasti jako nástroje pro zajištění veřejného pořádku, resp. obecně k ochraně majetku před škodou způsobenou jinými osobami, bude se jednat o zpracovávání osobních údajů a musí být uplatněno obecné nařízení o ochraně osobních údajů. Obec tedy musí respektovat základní zásady zpracování osobních údajů a další povinnosti pro správce vyplývající z GDPR. Jejich podrobný výčet je například na internetových stránkách Úřadu www.uoou.cz.

Jak dlouho mohou správci kamerového systému uchovávat záznamy?

Vždy to musí být v návaznosti na účel, pro který se kamery instalují. Ve většině případů by patrně měla stačit lhůta 72 hodin.

A ve kterých případech je správce může poskytnout občanům?

Tady platí obecná zásada, že pokud subjekt údajů požádá o poskytnutí kamerových záběrů své osoby, které zpracovává správce, tak ten by je měl poskytnout.

Od začátku roku došlo ke změně právní úpravy ohledně zpracování takzvaných cookies. Zaznamenal Úřad v této souvislosti podněty na porušení u obecních webů?

Podněty a stížnosti, které nám byly po novele zákona o elektronických komunikacích ve vztahu ke zpracování osobních údajů prostřednictvím souborů cookies doručeny, se téměř ve všech případech týkají soukromoprávních subjektů. Podněty směřované vůči územním samosprávným celkům jsme zatím obdrželi tři.

Kam se mohou obce obracet v případě nejasností v ochraně osobních údajů?

Primárně na svého pověřence pro ochranu osobních údajů, který musí být jmenován ze zákona. Je možné se obrátit i na nás, konkrétně na oddělení konzultací.

Jaké jsou podle vás možnosti rozvoje Úřadu v mezinárodním měřítku?

Z celoevropského pohledu je velmi důležité posilovat spolupráci při šetření případů přeshraniční povahy, jejichž četnost a zejména složitost přitom stále postupně narůstá. Příležitost vidím také v členství Úřadu ve Světovém shromáždění pro ochranu soukromí (Global Privacy Assembly). Tato platforma nabízí možnost postoupit ještě o krok dále a postupně se začleňovat do spolupráce v globálním měřítku. Důvodem je to, že ochrana osobních údajů a soukromí čelí zásadním globálním výzvám a je deklarovanou prioritou EU. ■

foto: Marika Vitnerová, Kancelář Senátu PČR