Věřím, že územní samospráva bude brát náš úřad jako důležitého a důvěryhodného partnera

Jiří Kaucký je od září novým předsedou Úřadu pro ochranu osobních údajů (ÚOOÚ). Už při svém nástupu do funkce avizoval, že se hodlá zaměřit také na intenzivnější spolupráci se samosprávou a osvětovou činnost, například ve formě partnerství se školami, neziskovým sektorem nebo s médii. Kam směřuje ÚOOÚ pod vedením nového předsedy a jak si lze konkrétně představit zamýšlenou spolupráci se samosprávou i odbornou veřejností?

Rozhovor

Ve vašem vystoupení na konferenci GDPR 2020 jste uvedl, že byste se chtěl mimo jiné zaměřit na partnerství s územní samosprávou. Jak toho chcete dosáhnout?

Tento cíl jsem měl již jako kandidát na předsedu ÚOOÚ, protože ve svém předchozím působení na Ministerstvu vnitra, které má podporu územní samosprávy takříkajíc v gesci, jsem se opakovaně setkával s kritickými názory představitelů územních samosprávných celků jak na samotnou matérii zpracování osobních údajů, tak na úroveň komunikace státních orgánů v této oblasti. V rámci přípravy aplikace GDPR a zákona o zpracování osobních údajů byly oba relevantní státní orgány, tedy ÚOOÚ i Ministerstvo vnitra, ve vztahu k územní samosprávě velmi aktivní, ale zdálo se mi, že územní samospráva přesto vidí v edukační roli státu rezervy. Po seznámení se s činností ÚOOÚ zevnitř bych rád řekl, že je rozhodně na co navazovat. Dosavadní spolupráce zahrnovala individuální osobní, telefonické a písemné konzultace a semináře uspořádané právě pro pověřence pro ochranu osobních údajů buď samostatně ÚOOÚ, nebo ve spolupráci s dalšími organizátory. Úřad průběžně spolupracoval se Svazem měst a obcí, se kterým se mimo jiné autorsky podílel na vydání metodické příručky. Dále bych velmi rád zmínil velmi důležitou spolupráci se Sdružením místních samospráv a Ministerstvem vnitra při pořádání metodických setkání pro obecní úřady s rozšířenou působností. Pokud se tedy podaří prohloubit dosavadní spolupráci a zejména restartovat zájem o ochranu osobních údajů na úroveň z doby přípravy na aplikaci GDPR, věřím, že územní samospráva bude ÚOOÚ brát jako důležitého a důvěryhodného partnera v této oblasti. Tomu napomáhá i skutečnost, že ÚOOÚ ve vztahu k územní samosprávě postrádá nejinvazivnější mocenské nástroje, tedy možnost ukládání pokut.

Můžete svoji představu ještě více přiblížit?

Kromě prohloubení stávající spolupráce je mým záměrem využít ve prospěch plnění zákonných úkolů ÚOOÚ, a v tomto případě i územních samosprávných celků, mou zkušenost s legislativní činností a s aplikací norem správního práva. A to především ve vztahu k nové kompetenci, kdy se ÚOOÚ, i bez návrhu, vyjadřuje k legislativním návrhům týkajícím se zpracování osobních údajů. Již jsme si to vyzkoušeli u návrhu novely exekučního řádu, který se věnuje nahrávání telefonátů exekutorům. Rozhodně v tom chceme pokračovat, a to i v oblastech, kde se ochrana osobních údajů stýká s výkonem práva na samosprávu ve smyslu čl. 100 odst. 1 Ústavy, nebo například tam, kde má ochrana osobních údajů význam ve vztahu k rovnému přístupu k veřejným funkcím dle čl. 21 Listiny základních práv a svobod, respektive obecně k ochotě občanů podílet se na správě věcí veřejných. Intenzivní spolupráce se samosprávou se v poslední době v této oblasti díky Sdružení místních samospráv týkala například realizace praktických dopadů nálezu Ústavního soudu č. 149/2020 Sb. ohledně registru ke střetu zájmů ještě před jeho účinností, tedy před 1. lednem 2021.

Uvažujete, v rámci zvýšení kvality výkonu funkce pověřence a následně v rámci zvýšení zabezpečení osobních údajů a soukromí, o nastavení systému vzdělávání pro pověřence ve státní správě a samosprávě? Například o nějaké období zkoušek odborné způsobilosti?

Na zvyšování kvality práce jednotlivých pověřenců se má dozorový ÚOOÚ podílet především nepřímo, tedy téměř všemi zveřejňovanými výstupy z činnosti a poradenstvím. Do nástupu pandemie Covid-19 to bylo několik desítek externích odborných akcí ročně. Formální úlohu v systému vzdělávání ovšem náš úřad nemá. Obecné nařízení o ochraně osobních údajů nic takového ve vztahu k pověřencům pro ochranu osobních údajů ani nepředpokládá. Potřebná úroveň znalostí by měla v každém jednotlivém případě odpovídat obsahu zpracování osobních údajů, které příslušný správní úřad provádí a pro něž je pověřenec jmenován, a nárokům na ochranu zpracovávaných osobních údajů. Kvalifikační požadavky na ty, kdo funkci pověřence pro ochranu osobních údajů vykonávají, Obecné nařízení ani žádný platný právní předpis plošně nestanoví. I proto Evropský sbor pro ochranu osobních údajů nepřipouští ani vydávání osvědčení podle čl. 42 pro funkci pověřence pro ochranu osobních údajů.

Jaká pravidla v tomto ohledu panují?

V České republice jsou právním předpisem stanoveny požadavky na tyto osoby působící v orgánech státní správy, které jsou služebními úřady. Ve služebních úřadech má být činnost pověřence vykonávána státními zaměstnanci ve služebním poměru na dobu neurčitou, kteří vykonali úřednickou zkoušku v oboru státní služby Ochrana osobních údajů. Podle nařízení vlády č. 302/2014 Sb., o katalogu správních činností, ve znění pozdějších předpisů, mohou být zařazeni do 12., příp. 13. platové třídy, a to s ohledem na povahu činnosti, která může kromě konzultací zahrnovat mimo jiné kontrolní činnost a řešení stížností. Osoba, která tuto funkci vykonává, musí složit zkoušku. Pro služební úřady s výjimkou Ministerstva vnitra lze v tomto oboru vykonat zkoušku právě na ÚOOÚ, který je rovněž garantem oboru státní služby Ochrana osobních údajů. Ke zkoušce

se mohou přihlásit i zájemci aktuálně nevykonávající státní službu. Teoreticky si tak lze představit, že by si ji z pilnosti složili i někteří úředníci územních samosprávných celků, nelze jim to ovšem logicky nařídit, a to ani formou stanovení požadavku ve vztahu k zastávanému pracovnímu místu. Konkréta upravuje služební předpis náměstka ministra vnitra pro státní službu č. 4/2015, kterým se stanoví výše paušální částky nákladů spojených s vykonáním úřednické zkoušky a § 35 zákona č. 234/2014 Sb., o státní službě, pro ty, kdo se následně stanou státními zaměstnanci (mohou žádat refundaci nákladů).

Z nařízení vlády č. 222/2010 Sb., o katalogu prací ve veřejných službách a správě, pro obce a územně samosprávné celky rovněž vyplývá, že je-li pověřenec zaměstnancem obce, má povinnost dosáhnout požadovaného stupně vzdělání nepřímo ze zařazení do příslušné platové třídy.

Výkon funkce pověřence je v kapitole státní správa a samospráva přiřazen referentu správy osobních údajů. Zákon o úřednících územních samosprávných celků ukládá územnímu samosprávnému celku povinnost zajišťovat správní činnosti stanovené vyhláškou č. 512/2002 Sb., o zvláštní odborné způsobilosti úředníků územních samosprávných celků, prostřednictvím úředníků, kteří prokázali zvláštní odbornou způsobilost. Z výše uvedeného lze dovodit, že se jedná o správní činnosti, tedy externí agendy ÚOOÚ zaměřené na adresáty veřejné správy, přičemž činnost pověřence takovou agendu zpravidla nepředstavuje. Legislativní praxe jde ve srovnatelných případech spíše opačným směrem, tedy výkon interních činností pro územní samosprávné celky spíše vyjímat z požadavků prokázání zvláštní odborné způsobilosti. Jako příklad lze uvést interní audit, který byl do 30. října 2018 vymezen jako správní činnost, na jejíž vykonávání se povinnost prokázání zvláštní odborné způsobilosti váže. Na základě novelizace vyhlášky o zvláštní odborné způsobilosti provedené vyhláškou č. 222/2018 Sb. již úředník, který vykonává činnost interního auditu, nemá povinnost prokázat zvláštní odbornou způsobilost při finančním hospodaření územních samosprávných celků a jeho přezkumu.

Možnost ovlivnit kvalitu pověřence mají tedy i samotné územní samosprávné celky?

Dovolím si doplnit čistě osobní pohled daný možná mou zkušeností legislativce: kultura příkazů a zákazů nebývá ve svobodné společnosti tou nejlepší. Územní samosprávné celky mají své jasně dané povinnosti vyplývající z Obecného nařízení o ochraně osobních údajů a je jen na nich, jak kvalitními zaměstnanci i co do stupně a zaměření vzdělání budou tyto povinnosti plnit. Pokud chtějí angažovat vysoce kvalifikované specialisty, anebo vzdělávat úředníky, kteří nejsou přímo vystudovaní v oboru, a to možná včetně výše uvedené zkoušky pro samoplátce, je to čistě na nich. V tom bych ctil i zde princip subsidiarity jako nejlepší. Koneckonců, kdyby ochrana osobních údajů nebyla (státní) službou, neměli by zkoušku ani státní zaměstnanci a ochrana osobních údajů by byla vykonávána v režimu zákoníku práce bez dalších požadavků. A snad ještě drobnost: čtenáři si jistě vzpomenou na poměrně značný odpor vůči požadavku stupně a zaměření vzdělání, který se v přestupkové agendě zdvihl napříč veřejnou správou. Nemá, myslím, smysl prosazovat novoty, které většina adresátů normy nebude ochotna a často ani schopna dobrovolně plnit.

Praxe ukazuje, že zavádění GDPR se uskutečnilo v různé kvalitě. Domníváte se, že by bylo žádoucí nastavit kritéria úrovně implementace GDPR a provádění auditů, minimálně ve veřejné správě?

Začal bych tím, že implementace Obecného nařízení o ochraně osobních údajů probíhá v podstatě v celé Evropské unii. Je to dáno nejen podobou adaptačních zákonů v jednotlivých členských státech, ale zejména tím, že Obecné nařízení se implementuje přes ohromnou spoustu dalších unijních a národních právních předpisů a až na vzácné výjimky s každým nově přijatým zákonem. Aktuálně diskutovaná novela zákona o ochraně veřejného zdraví zavádějící masivní oprávnění orgánů ochrany veřejného zdraví vůči občanům a jejich soukromí je toho jasným příkladem. Pokud jde o nastavení kritérií úrovně implementace, i tady dává základní vodítka a rámec samo Obecné nařízení o ochraně osobních údajů. Nařízení stanoví pravidelný přezkum a hodnocení implementace nařízení.

Jakou úlohu má Evropský sbor pro ochranu osobních údajů?

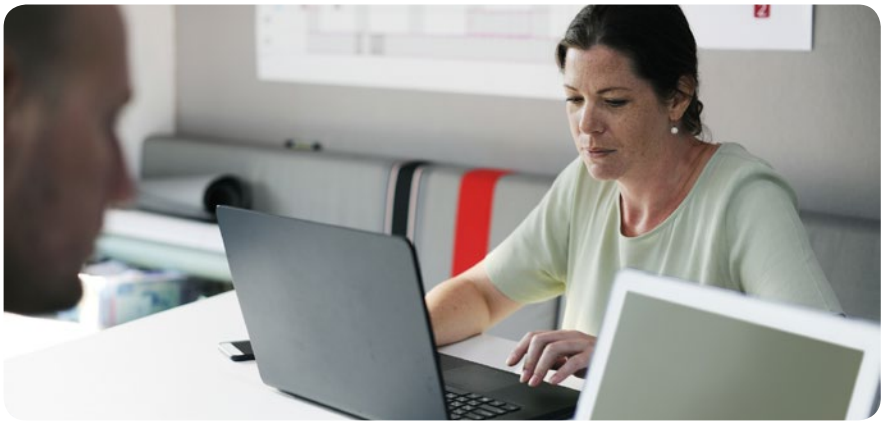
Průběžně vypracovává a podle potřeby aktualizuje požadavky a kritéria pro implementaci obecně i pro provádění. Jedná se nejen o metodické pokyny, ale také stanoviska zpracovaná z vlastní iniciativy Sboru, na žádost Komise nebo Evropského parlamentu. Úroveň implementace spoluvytvářejí a „kritéria" také formulují rozhodnutí přijímaná v mechanismu jednotnosti, tedy rozhodnutí v případech přeshraničního zpracování, která mají celounijní dosah. Na zpracování osobních údajů mimo tento mechanismus, tedy zpracování prováděná při výkonu státní správy, se velmi často použije vedle Obecného nařízení o ochraně osobních údajů také jeden nebo několik vnitrostátních předpisů, které v mezích stanovených v článku 23 Obecného nařízení výslovně upravují některé parametry zpracování, nejčastěji rozsah zpracovávaných údajů a jednotlivá práva subjektů údajů. To platí v určité míře i mimo veřejnou správu.

I výklad daňových předpisů, správního řádu, zdravotnické legislativy a dalších příslušnými národními dozorovými úřady zahrnuje zohlednění národních kritérií jednotlivých členských států. Ideálním stavem, o který ÚOOÚ dlouhodobě usiluje, je jednotná aplikace a implementace Obecného nařízení o ochraně osobních údajů.

U kontrol se ve všech členských státech výrazně uplatňují vnitrostátní procesní předpisy, tedy v ČR zejména správní řad a kontrolní řád. V této oblasti jsou výrazné rozdíly mezi členskými státy jak v oprávněních a postupech dozorových úřadů při kontrole, tak při vynucování souladu s Obecným nařízením v návaznosti na zjištění z kontroly nebo v jiném typu řízení. Z toho plyne, že jednotnosti lze v současné době dosahovat pouze postupně a pouze na určité úrovni.

Webové stránky ÚOOÚ obsahují celou řadu stanovisek a názorů, některá z nich jsou ale již několik let stará. Neplánujete jejich přehodnocení, případně i ve spolupráci s odbornou veřejností?

Užší spolupráce s odbornou veřejností je jedním z mých důležitých cílů. S kolegy vedeme na téma aktuálnosti zveřejněných textů debatu a chtěli bychom se dobrat toho, aby aktualizace neprobíhala jen incidentně, ale abychom ji prováděli alespoň u podstatných částí periodicky. Úřad má od účinnosti Obecného nařízení, které upravuje detailně jeho úkoly, nastaven širší systém projednávání materiálů s odbornou veřejností. Jedná se o následující materiály, které jsou při přípravě předkládány veřejnosti k připomínkám. Především výkladová stanoviska a vodítka k Obecnému nařízení o ochraně osobních údajů – tzv. Pokyny evropského Sboru, u nichž je ÚOOÚ (coby součást Sboru) spoluautorem a často velmi aktivním. Dosud se jedná o více než dvacet materiálů vykládajících uceleně pojmy, požadavky a nástroje ochrany osobních údajů, včetně příkladů. Další kategorií materiálů diskutovaných



s veřejností jsou metodické návody k posouzení rizik a vlivu na ochranu osobních údajů, ale také akreditační a certifikační kritéria. Příkladem takového návodu pro správce a zpracovatele a jejich odpovědné osoby (pověřence pro ochranu osobních údajů) je metodika DPIA. Vzhledem k tomu, jak budou v budoucnu v ČR postupně zaváděny nové nástroje ochrany osobních údajů stanovené Obecným nařízením, lze předpokládat publikaci výstupů z diskusí týkajících se příprav kodexů chování, certifikací či předběžných konzultací poskytovaných úřadem na žádost správců.

Jakou další formu komunikace má vámi vedený úřad na starosti?

Mimo to, co jsem popsal, poskytl do této doby ÚOOÚ řadu konzultací v agendách, v nichž nemůže být gestorem ani spoluautorem příprav zpracování, k návrhům stanovisek a metodik vydávaných ministerstvy odpovědnými za jednotlivé oblasti zpracování osobních údajů.

Tento výčet ale rozhodně neznamená, že bychom stávající stav považovali za ideální. Naším cílem je zásadní změna v metodické oblasti jak směrem k vyšší intenzitě a aktuálnosti poskytovaných informací, tak zejména ve vztahu k jejich čtivosti a srozumitelnosti pro adresáty z řad odborné a především laické veřejnosti.

Situace, která nastala při koronavirové epidemii, vytvořila podmínky pro rychlou elektronizaci kontaktů. To zároveň přineslo i širokou škálu kybernetických hrozeb. Domníváte se, že by bylo vhodné nastavit standardy ochrany osobních údajů z pohledu kybernetické bezpečnosti a eIDAS?

Účelem nařízení eIDAS je především zvýšit celkovou důvěryhodnost elektronických transakcí na evropském vnitřním trhu, protože poskytuje jednotnou bezpečnou elektronickou komunikaci mezi orgány veřejné moci, firmami, ale také občany. ÚOOÚ i další úřady jsou samozřejmě vázány zákonem a vyhláškami o kybernetické bezpečnosti a nařízením eIDAS, nicméně na ochranu osobních údajů je z její podstaty nutné hledět v daleko širší perspektivě, než je kybernetická bezpečnost.

S kybernetickými hrozbami a s neustále se zdokonalujícími technikami útočníků se potýkáme nejen při řízení našeho vnitřního IT, ale i u kontrolovaných subjektů z důvodu úniků dat způsobených právě kybernetickými útoky. Úroveň zabezpečení se postupně zvyšuje, k čemuž nám pomáhá i dobře nastavená legislativa, konkrétně vyhláška č. 82/2018 Sb., o kybernetické bezpečnosti, která posouvá vyžadovaný standard na moderní úroveň.

Jak u našich zaměstnanců, tak také obecně ale stále apelujeme na kontinuální školení kybernetické bezpečnosti, kybernetických hrozeb a v neposlední řadě sociálního inženýrství, kdy se útočník snaží využít nějaké znalosti prostředí a zranitelnosti uživatelů k tomu, aby z nich vylákal citlivé informace. I phishingové útoky už jsou dnes na velmi vysoké úrovni a ani zkušený uživatel je nemusí ihned rozpoznat.

Koronavirová epidemie přispěla také k nastavení distanční výuky na školách. Běžně používané nástroje typu MS Teams, Google Classroom a Meets nebo ZOOM ukládají vstupy a výstupy u této výuky (přístupové údaje, chatovou komunikaci, audiovizuální záznamy apod.) automaticky do cloudových úložišť, u nichž není jistota, kde jsou data uložena, kdo k nim má přístup a jak je s nimi později nakládáno. Nebylo by vhodné, aby stát inicioval podmínky pro poskytování služeb pro vzdálenou výuku tak, aby byla data ukládána na území EU a správce měl kontrolu nad jejich správou a výmazem?

Toto se samozřejmě děje ze samotné podstaty Obecného nařízení o ochraně osobních údajů. Pokud má být využívaná služba v souladu v souladu s ním, musí být osobní údaje ukládány na území EU a správce má mít kontrolu nad jejich správou a výmazem. Na státu, potažmo ÚOOÚ pak je, aby ještě více apeloval na školy a jejich pověřence, aby využívali pouze služby, které v souladu jsou.

Zároveň si uvědomujeme, že současný obrovský, někdy až překotný rozvoj digitalizace s sebou přináší rizika a témata, týkající se zejména veřejných cloudových služeb, jsou v našich zemích zatím legislativně velmi málo akcentována. Spolupracujeme proto s Národním úřadem pro kybernetickou a informační bezpečnost (NÚKIB) na jimi připravované tzv. cloudové vyhlášce, která by měla využíváním veřejně dostupných cloudových služeb ve veřejné správě nastavit jasnější pravidla.

Obdobné problémy patrně řeší i v jiných zemích…

Problematiku moderních cloudových služeb a osobních údajů je potřeba vnímat minimálně v celoevropském kontextu, kdy v členských státech přecházejí z důvodu vyšší flexibility a výrazně nižších nákladů na cloudové služby nejen pro běžnou kancelářskou činnost, jako je posílání e-mailů nebo videokonference, ale i na zpracování osobních údajů, citlivých nevyjímaje. Vzhledem k tomu, že většina poskytovatelů cloudových služeb má svou mateřskou společnost mimo země EU, střetávají se zde různé přístupy k ochraně osobních údajů a je potřeba brát velký zřetel na dodržování společného evropského práva i práva jednotlivých členských států. Příkladem může být nizozemské ministerstvo spravedlnosti a bezpečnosti, které velkou část své agendy obstarává prostřednictvím cloudových služeb nebo francouzský „Health Data Hub" shromažďující citlivé osobní údaje o zdravotním stavu občanů. Nedávný rozsudek Soudního dvora EU známý jako „Shrems II" mimo jiné zrušil tzv. „Privacy Shield", který umožňoval společnostem sídlícím v USA přijímat data z EU a garantovat jejich setrvání na území EU navzdory americké legislativě. Nyní je před námi v rámci celoevropské spolupráce jasný úkol - nebránit rozvoji moderních technologií, ale vždy chránit data našich občanů.

Rozhovor vedla Eva Janečková

Mgr. Jiří Kaucký (*1973)

Vzdělání

Po absolvování Gymnázia Oty Pavla v Praze vystudoval Právnickou fakultu Univerzity Karlovy v Praze.

Profesní zkušenosti

Od září 2020 předseda Úřadu pro ochranu osobních údajů

1997 – 2020 Ministerstvo vnitra ČR

- ředitel odboru správního
- státní tajemník
- sekce státní služby – zastupování ve funkci vrchního ředitele
- sekce pro přípravu státní služby – pověřen řízením ve funkci ředitele
- ředitel odboru legislativy a koordinace předpisů
- sekce (později odbor) legislativy, koordinace předpisů a kompatibility s právem ES, oddělení správního řízení

Členství v poradních a dalších orgánech (do srpna 2020)

- předseda Etické komise ČR pro ocenění účastníků odboje a odporu proti komunismu
- místopředseda Pracovní komise LRV pro veřejné právo I – správní právo č. 1
- místopředseda Komise pro rozhodování ve věcech pobytu cizinců
- místopředseda rozkladové komise ministra vnitra, člen rozkladové komise ministra životního prostředí a vedoucího Úřadu vlády
- místopředseda poradní komise ministra vnitra ve věcech služebního poměru policistů a příslušníků hasičského záchranného sboru
- člen Poradního sboru ministra vnitra pro správní řád a správní trestání
- člen Poradního sboru náměstka ministra vnitra pro státní službu k zákonu o státní službě

Členství v poradních orgánech z titulu funkce státního tajemníka (do dubna 2020)

- člen Vládního výboru pro osoby se zdravotním postižením
- člen Rady vlády pro seniory a stárnutí populace
- člen Rady vlády pro rovnost žen a mužů