PRO

OCHRANA OSOBNÍCH ÚDAJŮ V PRAXI

Číslo 1/2021, ročník I. | Měsíčník SMS-služby s.r.o. | www.dpopro.cz

Vážení čtenáři,

právě jste se začetli do prvního čísla časopisu DPO PRO, které vychází symbolicky v Den ochrany osobních údajů. Od okamžiku, kdy Rada Evropy přijala tzv. Úmluvu o ochraně osob se zřetelem na automatizované zpracování osobních údajů, uplynulo právě 40 let. Na tento dokument navázaly další právní předpisy zaměřené na ochranu osobních údajů. Patří k nim i Obecné nařízení (GDPR).

Události minulého roku přispěly ke zrychlené elektronizaci kontaktů a přesunu mnoha oblastí lidského života do online prostředí. Tyto okolnosti, spolu s neustále dokonalejšími kybernetickými útoky, ještě více zdůraznily nutnost zabývat se systematicky ochranou osobních údajů.

A právě této problematice je věnován nový časopis DPO PRO, jenž je určený především pověřencům pro ochranu osobních údajů, ale také všem, kteří se o ochranu osobních údajů zajímají a s osobními údaji pracují. Časopis má za cíl zaměřit se na soukromou i veřejnou sféru a pokrýt oblast ochrany osobních údajů v co nejširším spektru.

V prvním čísle najdete rozhovor s předsedou Úřadu pro ochranu osobních údajů (ÚOOÚ) Jiřím Kauckým. Ptali jsme se ho na budoucí směřování ÚOOÚ i zamýšlenou spolupráci se samosprávou a odbornou veřejností.

Upozorňujeme na nejnovější judikaturu týkající se poskytování informací, v tomto případě poskytování informací o platech. Tato po dlouhá léta diskutovaná oblast byla opět korigována „interpretačním" rozsudkem Nejvyššího správního soudu.

Věnovali jsme se i veřejné konzultaci k návrhu pokynů upřesňujících předkládání relevantních a odůvodněných námitek definovaných v čl. 4 odst. 24 Obecného nařízení v rámci konzultačního procesu mezi vedoucím dozorovým úřadem a dotčeným dozorovým úřadem podle článku 60 odst. 4 Obecného nařízení.

Vzhledem k výše zmiňovanému přesunu nejen pracovního života do online prostředí upozorňujeme na možnosti, jak nastavit podmínky pro bezpečnou práci z domova. Současný trh nabízí velké množství nástrojů určených pro videokonference a komunikaci, každý z nich však má nejen svá pozitiva, ale i negativa. Pro úřady je základním kritériem bezpečnost.

Vzhledem k tomu, že právní úprava odesílání obchodních sdělení provedená zákonem č. 480/2004 Sb. je součástí českého právního řádu již delší dobu, a přesto nejsou pravidla dostatečně jasná, nezapomněli jsme ani na článek věnující se této problematice.

Pozornost jsme věnovali i dalším tématům, která, jak vyplývá ze zkušeností, působí v praxi značné potíže.

Na závěr mi dovolte popřát všem, aby letošní rok byl o něco přívětivější a jednodušší, než byl ten předchozí.

Eva Janečková
šéfredaktorka DPO PRO

Co najdete dále uvnitř čísla

Otázka poskytování informace o platech prošla korekcí str. 5

Evropský sbor pro ochranu osobních údajů vydal pokyny k pojmu relevantní a odůvodněná námitka str. 6

Jak bezpečně pracovat z domova? str. 7

Odpovědnost za rozesílání spamů má i objednatel služby str. 8

Při využívání otisků prstů pro vstup do mateřinek je nutné myslet především na ochranu osobních údajů str. 9

Jak se vyhnout porušení ochrany osobních údajů na webech obcí str. 10

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

Rozhovor

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?

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?

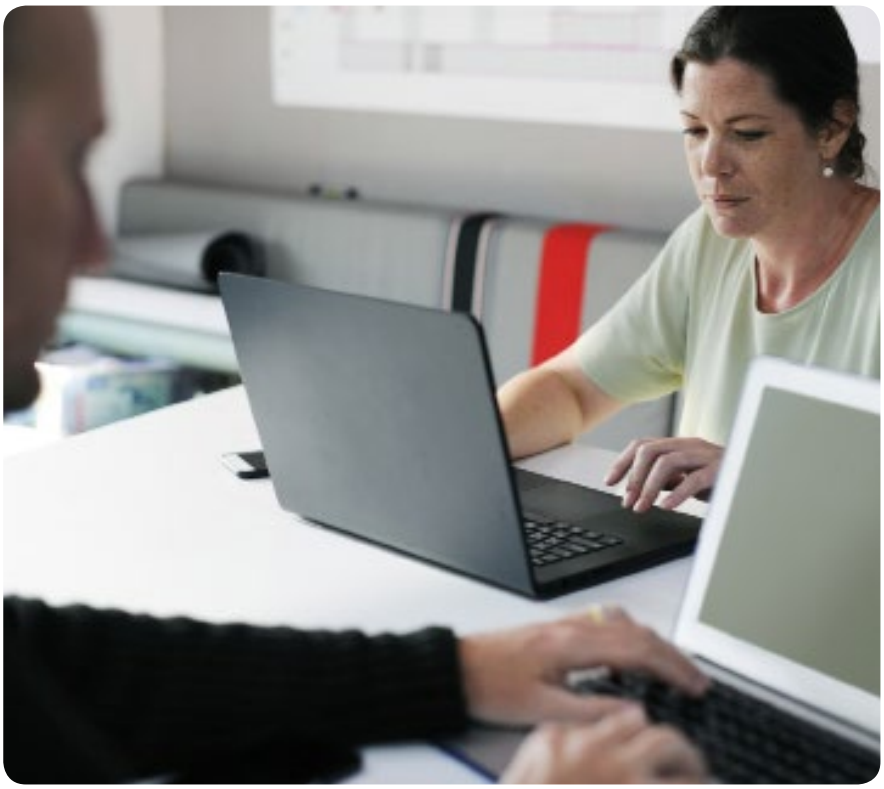
Tento cíl jsem měl již jako kandidát na předsedu ÚOOÚ, protože ve svém předchozím působení na Ministerstvu vnitra, které má podporu územní samosprávy takříkajíc v gesci, jsem se opakovaně setkával s kritickými názory představitelů územních samospráv-

ných 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 čin-

nost 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?

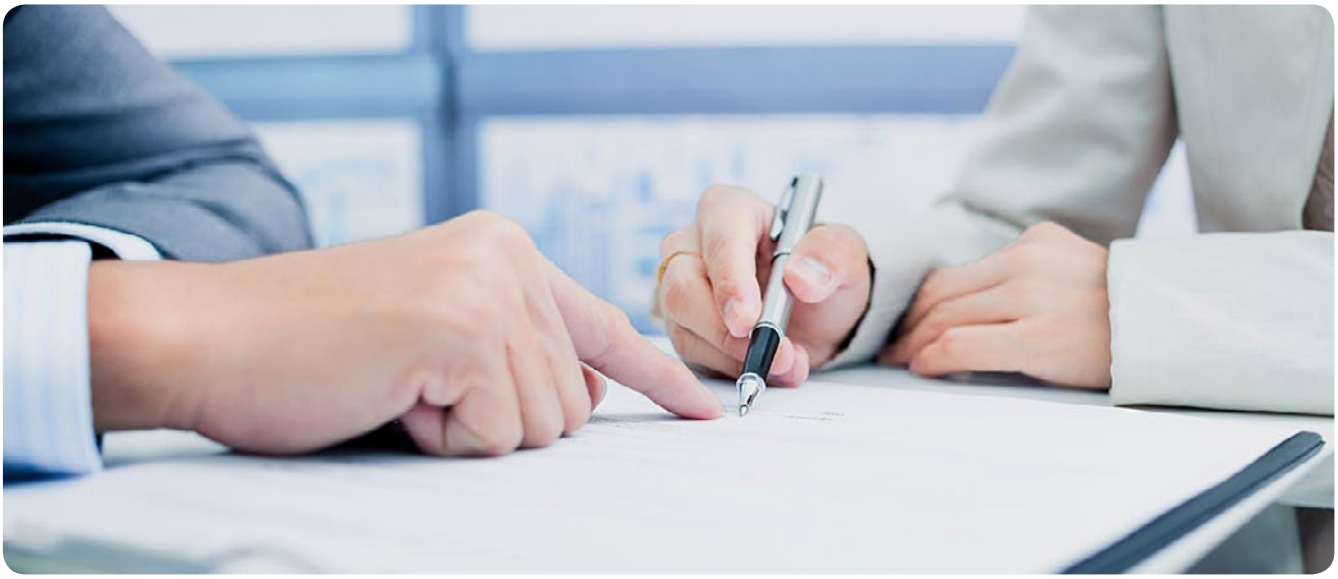
Průběžně vypracovává a podle potřeby aktualizuje požadavky a kritéria pro implementaci obecně i pro provádění. Jedná se nejen o metodické pokyny, ale také stanoviska zpracovaná z vlastní iniciativy Sboru, na žádost Komise nebo Evropského parlamentu. Úroveň implementace spoluvytvářejí a „kritéria“ také 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

Otázka poskytování informace o platech prošla korekcí

Judikatura

Rozhodnutí Nejvyššího správního soudu, č. j. 2 As 88/2019 – 29, ze dne 27. 5. 2020

Dne 27. 5. 2020 vydal Nejvyšší správní soud rozhodnutí, doplnil a interpretoval předchozí nález Ústavního soudu č. j. IV. US 1378/16. Nejvyšší správní soud (NSS) konstatoval, že je na něm na jako *„vrcholném soudním orgánu zajišťujícím jednotu rozhodování ve věcech patřících do pravomoci soudů ve správním soudnictví, aby alespoň v obecných rysech blíže stanovil konkrétnější úvahová východiska, resp. jejich mantinely, z nichž je třeba při provádění modifikovaného testu proporcionality vycházet; takový přístup přitom není nerespektováním či relativizováním nálezu Ústavního soudu, neboť jej pouze dále rozvádí a naplňuje, a to při zachování respektu k jeho esenciální myšlence.“*

V tomto přelomovém (z hlediska převažujícího výkladu) rozsudku Nejvyšší správní soud připomíná, že *„Ústavní soud v platovém nálezu pouze obecně předestřel čtyři podmínky pro poskytnutí informací o platech a odměnách: 1) účelem vyžádání informace je přispět k diskusi o věcech veřejného zájmu, 2) informace samotná se týká veřejného zájmu, 3) žadatel plní úkoly či poslání dozoru veřejnosti či roli tzv. „společenského hlídacího psa“, 4) informace existuje a je dostupná. Ústavní soud však tato kritéria nerozvádí a necharakterizuje pojmy v nich obsažené (např. plnění úkolů či poslání dozoru veřejnosti nebo tzv. „společenský hlídací pes“). Bližší interpretace těchto podmínek je ovšem ponechána na povinných subjektech, resp. následném soudním přezkumu prováděném správními soudy.“* [bod 24 rozsudku, kráceno].

NSS dále dvě první otázky spojil: *„splnění podmínky druhé bude většinou znamenat i naplnění (i když tomu tak zdaleka nemusí být vždy) té prvé;“*, anebo *„Posouzení povahy samotné informace a toho, k čemu má být využita, zpravidla bude třeba provádět společně a uvážit, zda žadatel s touto informací hodlá přispět k veřejné diskusi a nedomáhá se jí například pouze ze soukromých důvodů“*. [bod 25 rozsudku]

K zodpovězení první i druhé otázky NSS uvedl: *„Není již však na místě zkoumat, natož chtít po žadateli, aby sám prokázal, zda poskytnutá informace skutečně následně vzbudí žadatelem avizovanou veřejnou diskusi; relevantní pouze je, zda ji žadatel v podobě k tomu podle běžných zkušeností způsobilé hodlá veřejnosti k diskusi předložit a tím i potenciálně umožnit.“* [bod 25 rozsudku]

Dále uvedl, že pro zodpovězení otázky *„je klíčové, jaké postavení ve struktuře veřejné správy (a s tím související řídící a organizační kompetence, odpovědnost a patřičné finanční ohodnocení) dotčená osoba má. Jde-li o zcela „běžnou“ úřední osobu bez jakýchkoli řídících pravomocí, je nezbytné, aby žadatel v žádosti uvedl rozumné důvody, pro něž by měl právě v dané konkrétní situaci existovat veřejný zájem na vyhovění jeho žádosti.“* [bod 28 rozsudku, kráceno]

Původní platový rozsudek NSS, platový nález ÚS ani aktuální upřesňující rozsudek NSS přitom doposud neprovedly důsledné rozlišení mezi nárokovými složkami platu a mimořádnými odměnami z hlediska proporcionálního posouzení proti sobě stojících základních práv. Je přitom zřetelné, že u mimořádné odměny je tato proporcionalita nutně vychýlena směrem k potřebě ještě vyšší transparence, než jakou konstatoval platový rozsudek NSS obecně ve vztahu k platům a odměnám vypláceným z veřejných prostředků. Na jedné straně totiž posouzení, co je takovým splněným mimořádným úkolem, je zcela na volné úvaze nadřízeného. Riziko svévole výrazně zvyšuje korupční potenciál a tedy veřejný zájem na takové informaci. Na druhé straně odměna díky své mimořádnosti významně méně vypovídá o celkovém ekonomickém statusu příjemce než výše ostatních, nárokových složek, a tedy méně zasahuje do jeho soukromí.

Ústavní soud v platovém nálezu uvedl (a NSS v aktuálním judikátu zopakoval), že *„nemusí se v případě tzv. „společenského hlídacího psa“ zdaleka jednat pouze o profesionální novináře, nýbrž také o neziskové organizace či spolky věnující se otázkám transparentnosti, hospodaření a odměňování v rámci veřejné správy nebo tuto roli mohou naplňovat i jednotlivci (např. nejrůznější političtí aktivisté, blogeři či jinak se o veřejné záležitosti zajímající lidé), kteří relativně koncentrovaně (ať už v dlouhodobějším časovém horizontu nebo v širším záběru „hlídaných“ povinných subjektů) do veřejného prostoru jakýmkoli kvalifikovaným způsobem vnášejí informace či názory ohledně fungování veřejného života, díky čemuž o nich může být zahájena a vedena diskuse, případně se s nimi širší veřejnost alespoň může seznámit. Podmínkou pro naplnění role tzv. „společenského hlídacího psa“ tedy je, aby si žadatel jemu dříve poskytnuté informace (zde o příjemcích veřejných prostředků) nenechával výlučně pro sebe a svou vlastní soukromou potřebu, nýbrž s nimi veřejně „pracoval“ (typicky s nimi seznamoval veřejnost, komentoval je apod.) … nelze trvat na tom, aby žadatel takto získané informace nutně sám přímo explicitně hodnotil, analyzoval či metodologicky dále zpracovával; jejich pouhé zveřejňování, zvláště má-li systematičtější povahu, je samo o sobě pro veřejnost přidanou hodnotou.“*

Shrnutí

„Interpretační“ rozsudek NSS tedy lze zhruba shrnout tak, že poskytování informací o platu a odměně vrací do podoby blízké původnímu závěru tohoto soudu z r. 2014 (8 As 55/2012 – 62): Informace o platu a odměně se v zásadě poskytují vždy. Neposkytnou se však zejména v případech, kdy jde o plat „běžných“ zaměstnanců (rozsudek z r. 2014 to fomuloval jako „profese pomocné a servisní povahy“). Přesto se však i v této skupině poskytnou, pokud žadatelů předloží relevantní důvod převahy veřejného zájmu, například konkrétní podezření na zneužití veřejných prostředků.

Dále se informace o platu a odměně neposkytne, pokud žadatel žádným způsobem nehodlá získanou informaci vnést do veřejné diskuse. Nemusí je však nijak vyhodnocovat, stačí, když je zveřejní. Nemusí ani nijak zvlášť dokládat svou roli hlídacího psa, pokud je alespoň blogerem, politickým aktivistou, přispívá do diskusí na webu, je členem zastupitelstva, natož pokud by byl novinářem, datovým analytikem či pracoval v neziskovém projektu odpovídajícího zaměření. Z druhé strany řečeno, povinný subjekt musí doložit, že jde o „osamělého vlka“, jenž by si poskytnuté informace nechával výlučně pro sebe a svou vlastní soukromou potřebu.

Podmínkou poskytnutí informace dále zůstává test proporcionality, byť jeho velká část bude spíše formální a citující závěry rozsudku NSS z r. 2014, zejména co se týká posouzení vhodnosti, potřebnosti a přiměřenosti. První dvě kritéria budou v případě platů a odměn z veřejných prostředků splněny vždy. Přiměřenost většinou také, byť korigována výše uvedeným postavením osoby ve struktuře povinného subjektu. V těchto pasážích povinného testu lze pouze na uvedený rozsudek odkazovat.

Jelikož je informační řízení asymetrické a poskytnutí informace je faktickým úkonem, nikoli rozhodnutím, bude takový test proporcionality pouze součástí spisu. Poslední procesní podmínkou je oslovení dotčených osob a jejich vyjádření, které však závěr povinného subjektu o poskytnutí informací neurčuje.

Oldřich Kužílek
Autor je poradce pro otevřenost veřejné správy a ochranu soukromí.

Eva Janečková
Autorka je právník a odborník na ochranu osobních údajů.

Evropský sbor pro ochranu osobních údajů vydal pokyny k pojmu relevantní a odůvodněná námitka

Evropský sbor/Soudní dvůr EU

Obecné nařízení zřídilo koordinační orgán – Evropský sbor pro ochranu osobních údajů (Sbor), který připravuje pokyny k různým aspektům s cílem harmonizovat provádění GDPR v rámci Evropské unie, resp. Evropského hospodářského prostoru (EHP). Ve dnech 13. 10. až 24. 11. 2020 probíhala veřejná konzultace k návrhu pokynů upřesňujících předkládání relevantních a odůvodněných námitek definovaných v čl. 4 odst. 24 GDPR v rámci konzultačního procesu mezi vedoucím dozorovým úřadem a dotčeným dozorovým úřadem podle článku 60 odst. 4 GDPR.

Spolupráce mezi dozorovými úřady byla do nabytí účinnosti Obecného nařízení upravena jen velmi stručně. Obecné nařízení se věnuje vztahům mezi dozorovými úřady poměrně podrobně, mimo jiné také v čl. 60, kde jsou stanovena pravidla spolupráce mezi vedoucím dozorovým úřadem a dotčenými dozorovými úřady. Je obecným pravidlem, že dozor nad činností přeshraničního zpracování nebo činností zpracování týkající se občanů více než jedné země EU vykonává pouze jeden dozorový úřad, který se nazývá vedoucí dozorový úřad. Jedná se o subjekt, který má hlavní odpovědnost za přeshraniční zpracování, například pokud se prošetřuje společnost, která vykonává zpracování v několika členských státech. Mechanismus vedoucího dozorového úřadu se aktivuje pouze v souvislosti s přeshraničním zpracováním. Je proto nutné určit, zda se nějaké přeshraniční zpracování provádí.[1)]

Relevantní a odůvodněná námitka se tedy týká vztahu mezi dozorovými úřady a nelze ji zaměňovat s právem subjektu údajů vznést námitku podle čl. 21 Obecného nařízení.

Využití námitek, na jejichž podání má dotčený dozorový úřad lhůtu čtyři týdny, je nejzazším řešením. Jak Obecné nařízení, tak pokyny zdůrazňují, že případné rozdíly názorů dozorových úřadů v rámci konkrétních kauz by měly být řešeny ideálně už v přípravné fázi s cílem dosažení konsensu.

Pokud už dojde k podání námitek a nejsou přijaty, rozpor řeší Sbor svým závazným rozhodnutím na základě čl. 65 odst. 1 písm. a) Obecného nařízení.

Nové pokyny se zaměřují na bližší definování relevantních a důvodných námitek. Za prvé, dotčený dozorový úřad musí jasně sdělit, s kterými částmi návrhu rozhodnutí nesouhlasí. Námitka musí zejména obsahovat určení, v čem navrhované rozhodnutí špatně řeší otázku případného porušení Obecného nařízení, nebo v jaké části neuvádí přiměřené úkony vůči správci či zpracovateli.[2)] Námitka se může týkat obou částí. Námitky se musí týkat závěru rozhodnutí a lze je předkládat až k návrhu rozhodnutí vedoucího dozorového úřadu.

Předmětem námitky nemůže být otázka, zda má dozorový úřad, který se v daném případu ujal vedoucí role, pravomoc vydat v tomto případu rozhodnutí. Kompetenční spor má v Obecném nařízení jiný právní základ [čl. 65 odst. 1 písm. b)]. Závazně jej rozhoduje Sbor, a to v jakékoliv fázi případu.

Za druhé, podmínky relevance a odůvodněnosti musí být splněny obě, což má oporu v ustanovení čl. 60 odst. 4 Obecného nařízení – vedoucí dozorový orgán postoupí Sboru záležitost v případě, že námitku považuje za „irelevantní či nedůvodnou".

Relevantnost námitky

Aby byla námitka relevantní, musí mít přímý vztah k návrhu rozhodnutí. Musí buď napadnout závěr o porušení či neporušení Obecného nařízení (nebo prezentovat názor, že se jedná o porušení jiné, než je v návrhu uvedeno), nebo předpokládaná opatření vůči správci či zpracovateli, případně obojí. Relevantní námitkou není připomínka k formulaci nebo právnímu zdůvodnění, pokud nezpochybňuje samotný závěr o porušení Obecného nařízení či navržené úkony vůči správci či zpracovateli. Stejně tak nejsou námitkou teoretické a obecné komentáře. Relevantní a odůvodněnou námitkou je i taková, která se týká procedurálních otázek, jestliže dojde k situaci, kdy vedoucí dozorový úřad ignoroval procesní požadavky předepsané v Obecném nařízení, což ovlivnilo závěry navrhovaného rozhodnutí – například že provedené vyšetřování bylo nedostatečné do té míry, že by v případě řádnějšího šetření vedlo k odlišnému rozhodnutí. V případě úkonů vůči správci či zpracovateli se jedná např. o rozdílné chápání intenzity porušení, za které vedoucí dozorový úřad navrhuje napomenutí, dotčený dozorový úřad pak doloží dopad na velký počet subjektů údajů a navrhne uložení pokuty.

Odůvodněnost námitky

Znaky odůvodněnosti námitka splní, když jasně vysvětlí, proč k podání námitky došlo, a uvede, jak by úprava rozhodnutí vedla k odlišnému závěru buď o porušení Obecného nařízení, nebo úkonech vůči správci, resp. zpracovateli. Samozřejmostí by měly být právní argumenty, tj. odkazy na konkrétní ustanovení komunitního či vnitrostátního práva, i příslušné argumenty věcné. Jako vhodné, mj. z hlediska lepšího chápání námitky, Sbor v pokynech doporučuje, aby námitka obsahovala též návrh nového znění rozhodnutí.

Významnost rizik

Z definice obsažené v čl. 4 odst. 24 Obecného nařízení vyplývá i povinnost, aby námitka zjevně dokázala „významnost rizik vyplývajících z návrhu rozhodnutí, pokud jde o základní práva a svobody subjektů údajů, případně volný pohyb osobních údajů v rámci Unie". Z logiky věci je nutno významnost rizik ve vztahu k základním právům a svobodám subjektů údajů prokázat v každé námitce, rizika ve vztahu k volnému pohybu osobních údajů se hodnotí jen tehdy, kdy je to vhodné (a dotčený dozorový úřad to musí doložit). Námitku, která prokazuje pouze rizika vůči volnému pohybu osobních údajů, ale nikoliv vůči právům a svobodám subjektu údajů, pokyny nepovažují za dostatečně relevantní. Relevantní však může být taková námitka, která argumentuje rizikem vůči volnému pohybu osobních údajů na základě toho, že navrhované rozhodnutí ve vztahu ke správci či zpracovateli předpokládá opatření, které není přiměřené k rozhodnutím jiných dozorových úřadů v totožných či podobných situacích. Velké rozdíly v rozhodovací praxi mohou vytvořit nerovné podmínky v rámci EHP, rozdílné úrovně standardů ochrany osobních údajů, tím i právní nejistotu na straně správců a zpracovatelů, v horším případě snahu situace zneužít např. přesunem zpracování do zemí, kde je riziko sankcí minimální. V tomto pokyny společně s ustanoveními GDPR i dalšími pokyny Sboru (např. Pokyny k uplatňování a stanovování správních pokut pro účely nařízení 2016/679 z roku 2017) směřují k nastolení určité míry harmonizace rozhodování dozorových úřadů.

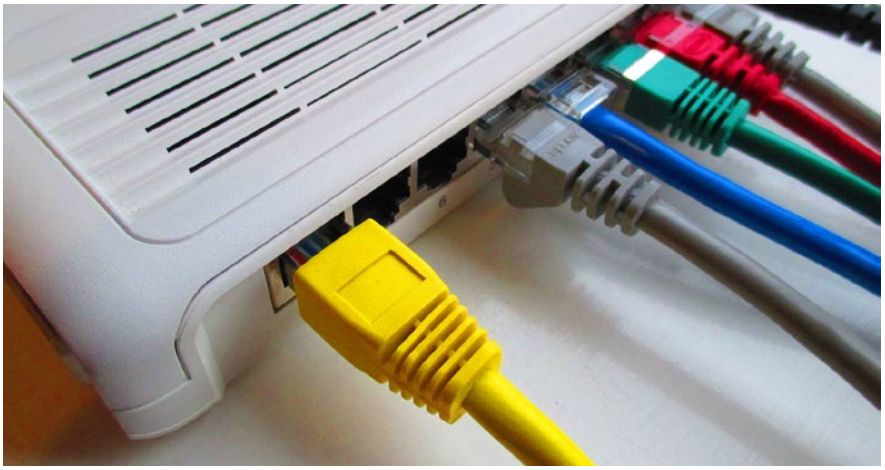
Pavel Janeček
Autor je odborník na mezinárodní vztahy.

1) Pokyny pro určení vedoucího dozorového úřadu správce nebo zpracovatele (Často kladené otázky), https://www.uoou.cz/schvalene-pokyny/d-28603

2) Čl. 4 odst. 24 Obecného nařízení – „relevantní a odůvodněnou námitkou" je námitka za účelem posouzení, zda došlo k porušení tohoto nařízení či nikoli, nebo zda je zamýšlený úkon v souvislosti se správcem či zpracovatelem v souladu s tímto nařízením, která jasně dokazuje významnost rizik vyplývajících z návrhu rozhodnutí, pokud jde o základní práva a svobody subjektů údajů, případně volný pohyb osobních údajů v rámci Unie.

Jak bezpečně pracovat z domova?

Epidemie Covid-19 přiměla mnoho zaměstnavatelů, včetně úřadů, co nejvíce vyprázdnit kanceláře a umožnit zaměstnancům tzv. home office (práci z domova). Současný trh nabízí velké množství nástrojů určených pro videokonference a komunikaci. Každý z nich má svá pozitiva, ale i negativa. Pro úřady je základním kritériem bezpečnost, zorientovat se v podmínkách a parametrech nástrojů však není vždy jednoduché.



V souvislosti s pokračující situací, kdy mnoho zaměstnanců využívá tzv. home office, tedy pracují z domova, musí mnoho úřadů řešit problém se zabezpečením dlouhodobé práce vykonávané vzdáleně. V případě zaměstnanců úřadu se jedná především o umožnění přístupu k agendovým systémům, spisové službě a zajištění komunikace jak s občany, tak i s kolegy.

Nejbezpečnější způsob pro přístup k agendovým systémům je prostřednictvím zabezpečené – šifrované VPN s použitím certifikátů s vyšší úrovní zabezpečení, a to i pro autentizaci uživatelů. Při výběru správného nástroje je nutné se podívat nejen na jejich cenu či uživatelské funkcionality, ale také na způsob uživatelského přístupu, možnosti administrátorského nastavení, způsobu ukládání vstupů a výstupů z videokonference atd.

Nástroje pro videokonferenci můžeme rozdělit na ty, které má organizace ve vlastní správě, a na nástroje provozované v cloudu.

Nástroje ve vlastní správě

V prvním případě organizace provozuje nástroj ve vlastní síti, na vlastním HW a pečuje o něj vlastní administrátor organizace. To znamená, že má plný vliv na administrátorské nastavení aplikace a má také **pod kontrolou vstupy a výstupy z jednání** (podkladové materiály, zápisy, audiovizuální záznam jednání apod.).

Do této skupiny patří nástroje:

- Cisco Meeting Server
- YEALINK
- POLYCOM

Nástroje provozované v cloudu

V případě interního cloudu poskytovaného například krajem nebo magistrátem pro podřízené organizace je nutné mít smluvně sjednané konkrétní podmínky nastavení, správy a přístupů uživatelů, včetně způsobu zálohování a výmazu dat dokumentů v rámci skartace. V tomto případě poskytovatelská organizace vystupuje vůči úřadu v roli zpracovatele. Je tedy nutno smluvně definovat, kdo bude mít za zpracovatele přístup k datům a s jakým oprávněním. Další postup nakládání s datovými soubory a dokumenty se bude striktně řídit dohodnutými pravidly.

Do této skupiny mohou patřit nástroje:

- Cisco Meeting Server

V současnosti jsou však nejvíce rozšířené služby videokonferencí poskytované komerčními poskytovateli – komerční cloud. Tito poskytovatelé většinou videokonference obohacují o další funkcionality či služby. Jedná se o tzv. kolaborativní nástroje, kdy je možné si mezi jednotlivými uživateli sdílet dokumenty, vyhodnocovat data apod.

Výhodou těchto nástrojů je cena, kdy je možné je využívat za nízký měsíční poplatek nebo dokonce zdarma. Z pragmatického hlediska je však nutné upozornit na to, že nikdy nic není zcela zdarma a cloudové služby zvláště. Proto vždy **při výběru cloudového nástroje doporučuji nejprve si důkladně a pozorně přečíst jak obchodní podmínky, tak bezpečnostní zásady**, které daný poskytovatel deklaruje.

Důležité je zaměřit se zvláště na pasáže definující místo uložení uživatelských dat, účely případného dalšího využití dat poskytovatelem služby, způsoby výmazu dat, způsoby uživatelských přístupů atd. Z povahy věci při využívání komerční cloudové služby **nemáte nad daty vzniklými a uloženými v takovém cloudu žádnou kontrolu**. Naopak máte, jako správce, za tato data odpovědnost a v případě, že dojde k bezpečnostnímu incidentu, který se bude týkat i osobních údajů, budete jej muset hlásit a řešit.

Vzhledem k výše uvedenému tedy doporučuji videokonferenční nástroje používat striktně pro videokonferenci. Nepropojovat tyto nástroje s dalšími aplikacemi nebo je dokonce používat jako dokumentové úložiště. Audionahrávky z videokonferencí nebo printscreeny obrazovek ukládejte do zabezpečeného úložiště pod vlastní kontrolou. V případě, že nativní nahrávací funkcionalita takového nástroje neumožňuje ukládat data do vámi zvoleného úložiště, používejte raději externí nástroje nebo funkcionalitu nahrávání obrazovky xboxu u MS Windows 10.

Nechte administrátora nastavit aplikaci, případně zakázat nebezpečné funkcionality, jako je přidávání dalších aplikací, sledování polohy uživatelů, umožnění zasílání pozvánek pozvanými osobami atd. V případě, že není možné některé z funkcionalit zakázat nebo bezpečně nastavit v aplikaci, zakažte jejich používání v návodu nebo v rámci školení.

Do této skupiny patří nástroje:

- ZOOM
- MS Skype
- MS Teams
- Google Workspace (aplikace Meets)
- Cisco Webex
- Lifesize

Závěrečné doporučení

Jako správce nezapomeňte zahrnout používání nových nástrojů a nakládání s novými typy dat a dokumentů do dokumentace jako např. evidence zpracování osobních údajů, analýza rizik nebo archivační a skartační řád úřadu. Zároveň je vhodné mít zpracované a zveřejněné návody pro zaměstnance, jak s nástroji zacházet, a provádět pravidelná školení týkající se ochrany osobních údajů a kybernetické bezpečnosti vůbec.

Vladimíra Hloušková
Autorka je místopředsedkyně Komory pověřenců.

Odpovědnost za rozesílání spamů má i objednatel služby

Přestože právní úprava odesílání obchodních sdělení provedená zákonem č. 480/2004 Sb. je součástí českého právního řádu již delší dobu, nejsou pravidla dostatečně jasná, případně se objevují snahy tato pravidla obejít. Je však třeba si uvědomit, že odpovědný je nejen případný odesílatel, ale i ten, kdo si rozeslání obchodní sdělení objednal. Za první tři čtvrtletí roku 2020 udělil Úřad pro ochranu osobních údajů za rozesílání nevyžádaných obchodních sdělení pokuty ve výši 7, 447 milionu korun.

Elektronické rozesílání spamu, tedy nevyžádaných obchodních sdělení, reguluje především zákon č. 480/2004 Sb., o některých službách informační společnosti a o změně některých zákonů (zákon o některých službách informační společnosti). Ten v § 7 odst. 2 a 3 upravuje dvě možné situace, dva právní tituly, pro legální šíření elektronických obchodních sdělení: předchozí souhlas adresáta, nebo zaslání obchodního sdělení stávajícímu zákazníkovi s nabídkou stejného nebo obdobného zboží či služby. Ustanovení § 7 odst. 4 téhož zákona pak vypočítává povinné náležitosti obchodního sdělení, jako je jeho označení, identifikace odesílatele atd. Pro účely tohoto článku je rovněž důležité zmínit znění souvisejícího přestupku: Podle § 11 odst. 1 písm. a) se porušení zákona č. 480/2004 Sb. dopustí ta právnická osoba, která hromadně nebo opakovaně šíří elektronickými prostředky obchodní sdělení v rozporu se zákonem.

Rozšiřující výklad Úřadu pro ochranu osobních údajů

Dle poznatků Úřadu pro ochranu osobních údajů (ÚOOÚ), který tento přestupek stíhá, se některé subjekty snažily své odpovědnosti zbavit tím, že si k faktickému rozesílání najímaly další osoby. V případě kontroly ze strany ÚOOÚ se pak snažily zbavit odpovědnosti právě s odkazem na tyto technické rozesílatele, kteří často byli, například z důvodu sídla mimo EU, jen obtížně dosažitelní. ÚOOÚ proto na základě několika kontrol vydal již v roce 2017 veřejné vyjádření, že za rozesílání obchodních sdělení nejsou právně odpovědni jen ti, kdo je fakticky (technicky) šíří, ale i ti, kteří si rozeslání obchodní sdělení objednají.[1)]

ÚOOÚ tento rozšiřující výklad odpovědnosti za rozesílání spamů aplikoval i nadále. Někteří účastníci řízení, kterým byla s tímto výkladem za rozesílání obchodních sdělení, resp. jeho objednání uložena pokuta, se proti tomu pochopitelně bránili u soudu.

Současná judikatura

Městský soud v Praze k této otázce poprvé judikoval na jaře tohoto roku a potvrdil výklad ÚOOÚ.[2)] Na půdorysu konkrétního případu soud mj. konstatoval, že za osobu, jež ve smyslu zákona č. 480/2004 Sb. šíří obchodní sdělení elektronickými prostředky, nelze považovat pouze jejich přímého odesílatele, ale rovněž toho, kdo jejich odeslání inicioval, dal k němu příkaz či z něj profitoval.[3)] Účastník řízení se v tomto případě snažil bránit mj. tím, že s faktickým rozesílatelem uzavřel smlouvu, ve které mu tento další subjekt garantoval rozesílání obchodních nabídek v souladu s právními předpisy. Argumentoval rovněž další komunikací s daným dodavatelem, se kterým řešil stížnosti týkající se nevyžádaných obchodních sdělení, při které dodavatel znovu potvrdil, že marketingová komunikace probíhá dle smlouvy a v souladu se zákonem. Soud k tomu uvedl, že takováto opatření nestačí k vyvinění, protože se nejedná o maximální možné úsilí, které bylo možné požadovat, aby účastník řízení přestupku předešel, jak to uvádí § 21 zákona č. 250/2016 Sb., o odpovědnosti za přestupky a řízení o nich.[4)]

Jak ÚOOÚ v původním řízení[5)], tak Městský soud v Praze konstatují, že smluvní ujednání mezi zadavatelem rozesílky obchodních sdělení a tím, kdo jej fakticky (technicky) realizuje, obsahující i záruky faktického rozesílatele, nemohou vyloučit odpovědnost zadavatele. V tomto konkrétním případě na smluvní ujednání navazovala i další komunikace, kdy se objednatel po obdržení informace o stížnostech adresátů na spamový charakter obchodních sdělení u dodavatele ujišťoval, zda je rozesílání zákonné a zda dodavatel dodržuje dotčená smluvní ujednání. ÚOOÚ i soud konstatovaly, že takováto opatření nepostačí. Bohužel už neuvádějí ani nenaznačují, jaká opatření by měl ten, kdo si faktické rozesílání obchodních sdělení objednává u dodavatele, přijmout, aby se vyhnul riziku porušení zákona č. 480/2004 Sb., které mu následně bude přičteno.

Závěrečné doporučení

Na základě upřesněného výkladu odpovědnosti za šíření obchodních sdělení ze strany ÚOOÚ a soudu můžeme tedy doporučení v této oblasti shrnout následujícím způsobem: Za elektronické rozesílání obchodních sdělení není z pohledu zákona č. 480/2004 Sb. odpovědný jen ten, kdo je fakticky zajišťuje, ale i subjekt, který si toto rozesílání objedná a v jehož prospěch je prováděno. Při využití třetí strany pro zajištění určité části rozesílky obchodních sdělení je klíčové zajistit, aby ani v tomto procesu nedocházelo k porušení zákona, zejména k zasílání obchodních sdělení bez dostatečného právního titulu či obchodních sdělení, která nesplňují další požadavky zákona. Pouhé smluvní ujištění dodavatele, že vše bude provádět v souladu s obecně závaznými předpisy, není z tohoto pohledu dostatečné. Objednatel, tedy ten, v jehož prospěch budou obchodní sdělení rozesílána, by měl pečlivě zvážit rizika spojená s takovýmto využitím služeb externího subjektu a přijmout dostatečná opatření, aby k porušení zákona dojít nemohlo.

Opatření budou vždy muset být individuální, resp. individualizovaná, ale typicky se bude moci jednat o detailní prověření (due diligence) dodavatele, ověření jeho interních procesů pro správu dat a další činnosti nezbytné k poskytnutí dané služby, nastavení technických a organizačních opatření k zajištění dodržení pokynů objednatele, možnost objednatele ověřit plnění daných opatření a v důvodných případech i faktické ověření na místě atd. Pokud budou tato opatření dostatečně individualizovaná, budou reflektovat konkrétní předmět plnění a jeho rizika a nebudou nastavena pouze formálně, lze uvažovat o tom, že by se objednatel v případě pochybení na straně technického rozesílatele mohl z odpovědnosti vyvinit.

František Nonnemann
Autor je právník. Je také členem Výboru Spolku pro ochranu osobních údajů.

1) https://www.uoou.cz/za%2Dsireni%2Dobchodnich%2Dsdeleni%2Dje%2Dodpovedny%2Dnejen%2Drozesilatel%2Dale%2Di%2Dobjednatel/d-23490
2) Rozsudek Městského soudu v Praze ze dne 7. dubna 2020 č.j. 14 A 242/2018 – 40
3) Bod 45 rozsudku
4) Bod 60 rozsudku
5) Popis související kontroly a správního řízení je např. ve Výroční zprávě ÚOOÚ za rok 2018 na str. 34–35.

Při využívání otisků prstů pro vstup do mateřinek je nutné myslet především na ochranu osobních údajů

Po několika bezpečnostních problémech v mateřských školách začali zřizovatelé hromadně nakupovat pro vstup do zařízení systémy založené na otiscích prstů. Tyto systémy byly propagovány jako jednoduché řešení bezpečnosti ve školách, aniž by zřizovatelé nebo ředitelé škol hned od počátku řešili související oblast ochrany osobních údajů.

V posledních letech se výrazně rozšiřuje technická i finanční dostupnost technologických řešení využívajících biometrické údaje osob, zejména otisky prstů. Takové systémy jsou využívány nejrůznějšími subjekty, včetně mateřských škol, ve kterých mají sloužit pro přístup rodičů (resp. obecně osob, které děti vyzvedávají) a zaměstnanců do prostor školky. Že se nejedná o věc zcela novou, dokládá i kontrolní činnost Úřadu pro ochranu osobních údajů (ÚOOÚ) [1].

Pro pověřence, který vykonává svou činnost pro mateřskou školu, je zásadní, aby se o úmyslu takový systém zavést dozvěděl co nejdříve. Pouze ve fázi záměru lze totiž bez zbytečně vynaložených nákladů vyhodnotit, zda z hlediska předpisů upravujících ochranu osobních údajů, tedy Obecného nařízení [2], je vůbec možné systém provozovat, a pokud ano, za jakých podmínek.

Na zpracování otisků prstů je nutno klást zvýšené nároky, neboť se jedná o zvláštní kategorii osobních údajů dle čl. 9 Obecného nařízení, a to bez ohledu na to, že je v systému otisk prstu převáděn do číselné podoby (tzv. hash).

Problematické prvky zpracování biometrických údajů

Zpracování biometrických údajů s sebou obecně přináší řadu problematických prvků [3]. Předně je třeba uvést, že tyto systémy samy o sobě v žádném případě větší bezpečnost nezajišťují. Biometrická identifikace či autentizace je založena na pravděpodobnosti, a proto vždy existuje i určitá míra chybovosti. Současně prokazatelně existují postupy a techniky, které umožňují obejít biometrické autentizační systémy a předstírat identitu jiné osoby. Navíc, na rozdíl například od systémů založených na heslu, jednou kompromitovaná biometrická informace nemůže být změněna nebo zrušena. Neoprávněný přístup k biometrickým údajům v systému také může umožnit nebo ulehčit přístup k dalším systémům užívajícím tytéž biometrické údaje. Všechny tyto skutečnosti musí správce v případě rozhodování o použití systému vzít v úvahu.

K podmínkám, za nichž lze obdobné systémy zavést, se vyjádřil také ÚOOÚ. Podle něj je nezbytné posoudit přiměřenost konkrétního řešení a rizik s ním spojených, vhodně kombinovat biometrický systém s dalšími bezpečnostními opatřeními a také průběžně posuzovat účinnost systému [4].

Posouzení před zavedením systému

Prvním krokem při zvažování záměru zavést biometrický systém musí být jeho posouzení z pohledu základních zásad zpracování osobních údajů dle čl. 5 Obecného nařízení. Zde je zejména nutno zdůraznit zásadu zákonnosti, korektnosti a požadavek, aby stanovený účel zpracování byl legitimní, resp. aby zpracováním bylo možno stanoveného účelu dosáhnout. Sledovaný účel např. nebude dosažen, pokud (jak zjistil ÚOOÚ v jedné z provedených kontrol) bude vstup do budovy pomocí otisku prstu umožněn nejen identifikované osobě, ale současně s ní i dalším, již bez identifikace [5]. V návaznosti na to konstatoval, že zpracování otisků prstů nebylo nezbytné pro stanovený účel zpracování, tedy zabezpečení vstupu do budovy (v jednom z případů ÚOOÚ zpracování pro tento účel akceptoval poté, co školka doložila dodatečné opatření spočívající v tom, že na vstup do příslušných prostor současně dohlížel i zaměstnanec školky [6]), resp. že skutečným účelem zpracování bylo „usnadnění vstupu osobám, které zvolí tuto metodu a poskytnou otisk prstu“ [7].

Jediným použitelným právním titulem pro zpracování otisků prstů v posuzovaném případě je souhlas dotčených osob, který mu-

1) https://www.uoou.cz/kontrola-zpracovani-osobnich-udaju-pro-ucely-vstupu-do-materske-skoly-materska-skola-hellichova/ds-4949/archiv=0&p1=4986; https://www.uoou.cz/materska-skolka-napajedla-zpracovani-osobnich-udaju-v-souvislosti-s-umoznenim-pristupu-do-budovy/ds-5185/archiv=0&p1=5649

2) Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)

3) viz například materiál Evropského inspektora ochrany údajů „Čtrnáct nedorozumění ohledně biometrické identifikace a autentizace“, dostupný např. na https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=43934

4) https://www.uoou.cz/upozorneni-na-zmenu-v-nbsp-posuzovani-systemu-vyuzivajicich-biometricke-udaje-drive-quot-stanovisko-c-1-2017-biometricka-identifikace-nebo-autentizace-zamestnancu-quot/d-29048

5) https://www.uoou.cz/kontrola-zpracovani-osobnich-udaju-pro-ucely-vstupu-do-materske-skoly-materska-skola-hellichova/ds-4949/archiv=0&p1=4986

6) https://www.uoou.cz/materska-skolka-napajedla-zpracovani-osobnich-udaju-v-souvislosti-s-umoznenim-pristupu-do-budovy/ds-5185/archiv=0&p1=5649

7) https://www.uoou.cz/kontrola-zpracovani-osobnich-udaju-pro-ucely-vstupu-do-materske-skoly-materska-skola-hellichova/ds-4949/archiv=0&p1=4986

sí splňovat podmínky, které na něj Obecné nařízení klade[8]. Osoba tedy musí mít možnost souhlas neudělit a nebýt tím nijak poškozena a zejména musí být řádně informována o účelu zpracování. Nesmí být tedy například vytvářen mylný dojem, že zpracování bude sloužit ke zvýšení bezpečnosti, pokud tomu tak ve skutečnosti není. Splnění podmínek pro řádné udělení souhlasu je přitom správce povinen kdykoli prokázat.

Odpovědnost za zavedený systém nese správce

Dalším problematickým aspektem je, že správce odpovídá za kompletní zvolené technické řešení. To platí bez ohledu na to, že systém dodá třetí strana a správce v podstatě nemůže (s ohledem na své technické možnosti) prověřit např. jeho zabezpečení. Proto je třeba klást vysoké požadavky na smlouvy s dodavateli, aby pokrývaly i případné nároky, které by vůči nim mohly vzniknout (nejen) při případném porušení povinností při zpracování osobních údajů.

V případě, že bude dodavatel při zpracování v postavení zpracovatele[9], je dále třeba zajistit, aby poskytoval dostatečné záruky, že zpracování bude odpovídat požadavkům Obecného nařízení[10]. Ověření této skutečnosti je povinností správce; splnit ji může například provedením průzkumu veřejně dostupných zdrojů, vyžádáním referencí apod. Současně je třeba uzavřít smlouvu o zpracování se všemi stanovenými náležitostmi[11].

Dále je správce povinen posoudit, zda jím zamýšlené zpracování podléhá posouzení vlivu na ochranu osobních údajů , a pokud ano, posouzení řádně provést. Musí také přijmout technická a organizační opatření odpovídající rizikům, která zpracování pro subjekty údajů přináší (a jejich přijetí kdykoli doložit).

Po rozhodnutí o provozování systému zpracovávajícího otisky prstů je nutné se soustředit na další základní zásady zpracování dle čl. 5 odst. 1 Obecného nařízení. Je tedy třeba nastavit procesy, které zajistí, že osobní údaje budou bez zbytečného odkladu smazány, např. v případě, že dítě ukončí docházku nebo některé z osob skončí oprávnění k jeho vyzvedávání. V systému by se neměly hromadit ani údaje shromážděné jeho provozem, tj. informace o tom, kdo a kdy jeho prostřednictvím do školky vstoupil.

Ochrana osobních údajů je soustavný proces

Závěrem je třeba zdůraznit, že ochrana osobních údajů je soustavný proces – provoz systému bude třeba průběžně vyhodnocovat ve všech relevantních kritériích. Dále platí, že správce unese svou odpovědnost za zpracování jen tehdy, jestliže veškeré své kroky (které jsou popsány výše) řádně dokumentuje. A nakonec obecné pravidlo ochrany osobních údajů, které tím spíš platí u jejich zvláštních kategorií: Nejlépe ochráníte osobní údaje tím, že je vůbec nebudete zpracovávat!

Vanda Foldová
Autorka je zaměstnankyně Ministerstva financí, kde se věnuje ochraně osobních údajů a svobodnému přístupu k informacím.

8) V případě zpracování zvláštních kategorií osobních údajů se jedná o požadavky na výslovný souhlas dle čl. 9 odst. 2 ve spojení s čl. 4 bod 11, resp. čl. 7 Obecného nařízení.

9) Závěr, zda dodavatel je současně zpracovatelem, nelze učinit obecně, ale třeba v konkrétních případech vyhodnotit jeho úkoly, které mohou vyplývat jak z uzavřené smlouvy, tak z faktického postupu.

10) čl. 28 odst. 1 Obecného nařízení

11) čl. 28 odst. 2 Obecného nařízení

12) viz čl. 35 Obecného nařízení; vyhodnocení, zda je třeba posouzení provést, se provede dle materiálu ÚOOÚ „Seznam druhů operací zpracování (ne)podléhajících požadavku na posouzení vlivu na ochranu osobních údajů", dostupný na https://www.uoou.cz/seznam-druhu-operaci-zpracovani-ne-podlehajicich-pozadavku-na-posouzeni-vlivu-na-ochranu-osobnich-udaju-dpia/ds-5458/archiv=0&p1=5856

13) viz čl. 5 odst. 2 Obecného nařízení

Jak se vyhnout porušení ochrany osobních údajů na webech obcí

Webové stránky bezesporu patří k hlavním komunikačním kanálům mezi obcí a širokou veřejností. V dnešní době si lze jen těžko představit, že by existovala obec bez vlastního webu. Jeho prostřednictvím však může docházet ke zpracování osobních údajů, například jejich zveřejňováním. Ačkoliv vždy záleží na konkrétním případě, určitá pravidla zpracování osobních údajů lze do určité míry typizovat. Způsobů, jimiž se může správce dopustit deliktu ve vztahu k ochraně osobních údajů, je hned několik. V článku se dozvíte o nejčastějších způsobech porušení ochrany osobních údajů na webech obcí.

Zveřejňování poskytnutých informací na žádost

Zákon č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů (dále jen „Infozákon"), stanoví v § 4 povinnost povinných subjektů poskytovat informace také na základě žádosti, přičemž formální náležitosti dané žádosti jsou popsané v dalších částech Infozákona[1]. Je tedy zřejmé, že žádosti o informace dle Infozákona mohou obsahovat osobní údaje žadatele[2]. V praxi obecních webů se nezřídka stává, že správce osobních údajů (obec) zveřejní na svých webových stránkách celou žádost o poskytnutí informací včetně osobních údajů žadatele.

Lze najít právní titul ke zveřejnění osobních údajů?

Odpověď je jednoznačně záporná, zveřejnění osobních údajů žadatele je zcela nepřípustné. V samotném Infozákoně nenalezneme ani zmínku o tom, že by měl povinný subjekt povinnost zveřejnit samotnou žádost o informace. V § 5 odst. 3 je řečeno, že „Do 15 dnů od poskytnutí informací na žádost povinný subjekt tyto informace zveřejní způsobem umožňujícím dálkový přístup.". Povinný subjekt musí tedy zveřejnit pouze poskytnuté informace, rozhodně však z výše uvedeného nevyplývá povinnost zveřejnit samotnou žádost o informace, natož osobní údaje žadatele. Při zveřejňování odpovědi nebo poskytnuté informace musí platit pravidlo, že žadatel ne-

1) Formální náležitosti žádosti (včetně požadovaných osobních údajů žadatele) jsou definovány v § 14. Zároveň je nutné dodat, že ne každá žádost, respektive správně podaná žádost musí takto definované náležitosti splňovat.

2) Typicky pak jméno, příjmení, datum narození, adresa trvalého pobytu.

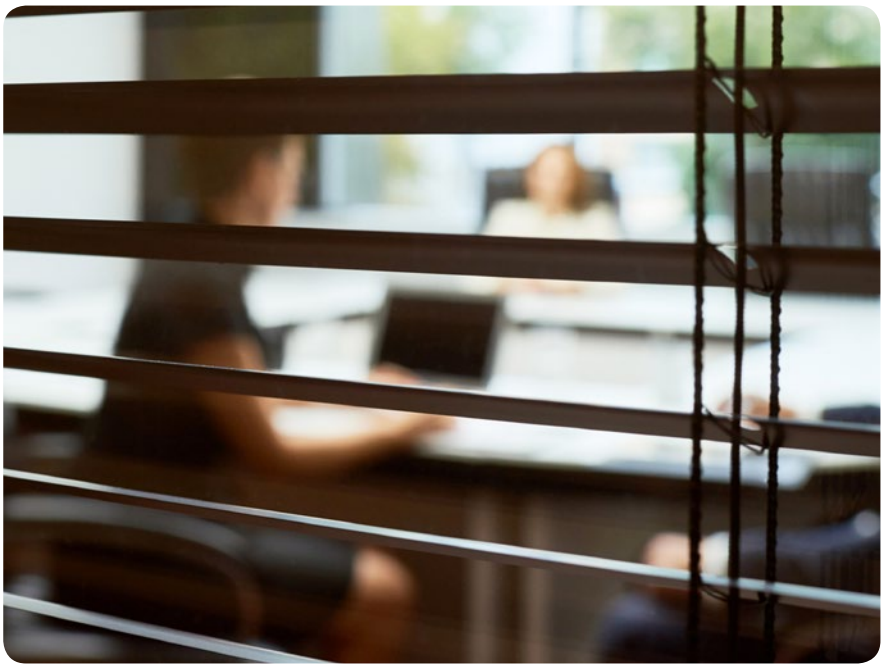
smí být při zveřejnění žádosti a poskytnuté informace [3] jakkoliv identifikovatelný. Na webu obce by se tak neměly zveřejňovat žádné osobní údaje žadatele. V případě, že se poskytnuté informace vkládají na web jako externí dokumenty (word, pdf apod.), je třeba dávat si pozor i na název vkládaného souboru. Ani v názvu souboru by se neměly osobní údaje žadatele objevit [4].

Kapitolou samou o sobě je pak poskytování osobních údajů, o které žadatel žádal. Jako příklad můžeme uvést odměnu konkrétního zastupitele nebo výši platu úředníka. Debata o tom, zdali tyto údaje můžeme poskytnout, by vydala na celou knihu, proto se tímto tématem nebudeme v tomto článku zabývat. Pokud se však zaměříme na následné zveřejňování takových osobních údajů na webu obce [5], platí následující teze: Zveřejnit osobní údaje bez anonymizace lze pouze v takovém případě, pokud bychom tyto osobní údaje poskytli každému bez rozdílu. Znamená to tedy, že pokud poskytujeme určité osobní údaje žadateli jen z toho důvodu, že je např. zastupitelem dané obce (privilegovaný žadatel), pak je třeba takto poskytnuté osobní údaje zcela jistě anonymizovat. Naopak v případě, že bychom osobní údaje poskytli každému bez rozdílu, anonymizace pravděpodobně nebude nutná [6].

Zveřejňování zápisů ze zasedání zastupitelstva obce je dobrovolné

Velmi častým jevem na webech obcí je zveřejňování zápisů ze zasedání zastupitelstva, případně rady obce. Povinnost pořízení zápisu z veřejného zasedání zastupitelstva je definována v § 95 zákona č. 128/2000 Sb., obecní zřízení, ve znění pozdějších předpisů (dále jen jako „Obecní zřízení"), kde je následně definována pouze povinnost pořídit zápis do 10 dnů po skončení zasedání. Obecní zřízení pak stanovuje, že zápis „musí být uložen na obecním úřadu k nahlédnutí" [7]. Zveřejnění zápisů ze zastupitelstva obcí tak není povinnost, jedná se o dobrovolné zveřejnění, které je možné a v rámci transparentnosti velmi využívané. Opírá se o § 5 odst. 6 InfZ [8].

Ve vztahu ke zveřejňování osobních údajů je v tomto případě klíčové, že takové zveřejnění je dobrovolné. V případě zveřejnění takových zápisů je třeba odlišovat originální neanonymizovanou verzi zápisu uloženou na obecním úřadě od verze, která je umístěna na webu obce. Webová verze by tak neměla obsahovat nadbytek osobních údajů. Ve webové verzi zápisů je možné ponechat



osobní údaje o veřejných představitelích a zaměstnancích, stejně tak jako osobní údaje příjemců veřejných prostředků [9]. Zcela bezpochyby je však nutno anonymizovat osobní údaje osob, které jsou typicky zveřejněny v bodě „Různé/Diskuze", tedy takových, které nebyly nezbytné pro vlastní rozhodování zastupitelstva.

Je nutný souhlas se zpracováním osobních údajů v kontaktním formuláři?

V rámci zefektivnění komunikace s občany obce často využívají na svých webech kontaktní formulář, jehož pomocí mohou občané kontaktovat obec přímo. Nezřídka se tak stává, že součástí tohoto kontaktního formuláře je souhlas se zpracováním osobních údajů dle Článku 7 obecného nařízení. Je však tento souhlas nutný?

Za předpokladu, že takto získané údaje občanů nejsou využívány k jinému účelu [10], právním titulem k takovému zpracování je písmeno e) Článku 6 Obecného nařízení – zpracování je nezbytné pro splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci, kterým je pověřen správce. Souhlas se zpracováním osobních údajů tedy není na místě.

V rámci dodržení zásad Obecného nařízení je však třeba myslet na dostatečnou informovanost subjektů údajů a z toho plynoucí povinnost správce informovat o zpracování osobních údajů. V bezprostřední blízkosti takového kontaktního formuláře je tedy nutné umístit odkaz na informace o zpracování osobních údajů, které správce na svém webu zveřejnil [11].

Závěr

Webové stránky obcí bezpochyby obsahují množství osobních údajů, respektive mohou tyto osobní údaje obsahovat. Mezi nejobvyklejší nešvary patří zveřejňování osobních údajů v poskytnutých informacích dle Infozákona, zveřejňování osobních údajů v zápisech ze zastupitelstva obce a získávání souhlasu v kontaktním formuláři.

Obecně lze říci, že ke zveřejňování osobních údajů na obecním webu je třeba přistupovat velmi opatrně, k jejich zveřejnění je třeba hledat konkrétní právní titul a právní základ.

Michal Hinda
Autor je pověřenec
pro ochranu osobních údajů.

3) V praxi se často stává, že povinný subjekt zveřejňuje celou odpověď.
4) Jako např. Hinda_žádost_106_1.pdf
5) Jako součást zveřejnění poskytnutých informací na žádost dle § 5 Infozákona
6) Velmi často se poskytují tzv. příjemci veřejných prostředků, viz § 8b Infozákona.
7) Viz § 95 obecního zřízení
8) „Povinný subjekt může informace podle odstavce 1 zveřejnit i dalšími způsoby a s výjimkami uvedenými v tomto zákoně může zveřejnit i další informace."
9) Osobní údaje lze zveřejnit v rozsahu definovaném § 8b odst. 3 Infozákona.
10) Takovým příkladem mohou být různá sdělení marketingového charakteru.
11) Např. pomocí hypertextového odkazu

TYCOVÁ | DVOŘÁK, advokátní kancelář, s.r.o.

TYCOVÁ | DVOŘÁK POSKYTUJE KOMPLEXNÍ ROZSAH VYSOCE KVALITNÍCH PRÁVNÍCH SLUŽEB PRO PODNIKATELE, OBCE, VEŘEJNÝ SEKTOR, NEZISKOVÉ ORGANIZACE I SOUKROMÉ OSOBY.

TYCOVÁ | DVOŘÁK

ADVOKÁTNÍ KANCELÁŘ

Naše odborné zaměření je občanské právo, vymáhání a správa pohledávek, rodinné právo, nemovitosti a bytové právo, obchodní právo, náhrada újmy, správní právo a místní samospráva, autorské právo, průmyslová práva, cizinecké a azylové právo, veřejné zakázky.

Advokátní kancelář Tycová | Dvořák je rychle se rozvíjející společnost, založená v roce 2018 sdružením do té doby úspěšně spolupracujících samostatných advokátů Lucie Tycové Rambouskové a Karla Dvořáka, jejichž významným dlouholetým klientům se kancelář věnuje i nadále. Za dobu svého působení dosáhla kancelář v rámci své generální praxe mnoha zajímavých pracovních úspěchů a získala značné množství nových klientů, a to jak z řad velkých obchodních společností, menších podnikatelů, územních samosprávných celků či neziskových organizací, tak i soukromých osob. Při řešení konkrétních požadavků a dosahování cílů svých klientů využívají členové kanceláře své dlouholeté praxe, odborných znalostí, zkušeností a vysokých morálních a etických standardů.

Tycová | Dvořák nabízí osobní a zároveň velmi profesionální přístup silného, schopného a respektovaného partnera. Ve snaze o poskytování kvalitního a komplexního právního servisu svým klientům si partneři kanceláře velmi zakládají na svém pracovním týmu, složeném z advokátů a advokátních koncipientů specializovaných na jednotlivé oblasti soukromého práva. Kancelář se dlouhodobě věnuje právní ochraně několika významných českých kolektivních správců práv autorských a souvisejících. Spolupráce v rámci kanceláře i přístup jejích partnerů a zaměstnanců ke klientům a k řešení všech předložených právních problémů reflektují moderní dobu a sledují vývoj právní praxe, přesto jsou však založeny na tradičních hodnotách lidských i profesních, na maximální péči a vzájemné důvěře.

Adresa

Národní 973/41,
110 00 Praha 1 – Staré Město

Telefon

+420 224 282 504

E-mail

info@aktycova.cz

Web

www.aktycova.cz