PRO

OCHRANA OSOBNÍCH ÚDAJŮ V PRAXI

Číslo 3/2022, ročník II. Měsíčník SMS-služby s.r.o. www.dpopro.cz

Vážení čtenáři,

s prvními jarními dny je tu i březnové číslo časopisu DPO PRO, měsíčníku pro pověřence pro ochranu osobních údajů. A nejen pro ně. Co se v něm dočtete?

Nenechte si ujít rozhovor s odborníkem na IT bezpečnost a ochranu osobních údajů Michalem Mertou, s nímž jsem si povídala o důležitosti spolupráce mezi jednotlivými útvary správce osobních údajů, pověřencem a IT.

Ani tentokrát nechybí aktuální informace o činnosti Spolku pro ochranu osobních údajů, který na konci března uzavře nominace na ocenění Pověřence pro ochranu osobních údajů roku.

Podrobněji se věnujeme rozhodnutí Evropského soudu pro lidská práva, jenž se zabýval otázkou, zda je možné v posluchárně veřejné vysoké školy pořizovat videozáznam.

Otázkou, kdy je sdělování osobních údajů o opatrovanci přípustné a kdy nikoliv, se zabývala Veronika Gabrišová.

Ptáte se, zda je to vše? Kdepak. Časopis obsahuje mnohem více. Tak tedy ničím nerušené čtení a mnoho inspirativních podnětů pro vaši práci přeje.

Eva Janečková
šéfredaktorka DPO PRO

Rozhovor

Řetěz je tak silný jako jeho nejslabší článek

Bezpečnost osobních údajů nabývá v souvislosti s událostmi posledních měsíců stále více na významu. Národní úřad pro kybernetickou a informační bezpečnost vydává varování před útoky každý týden, zvýšené nebezpečí se začíná dotýkat každého z nás. Jaká rizika přináší nespolupráce mezi jednotlivými útvary správce osobních údajů navzájem a pověřencem? A proč by pověřenec měl mít znalosti IT? Nejen na tyto otázky odpovídá odborník na IT a ochranu osobních údajů Michal Merta.

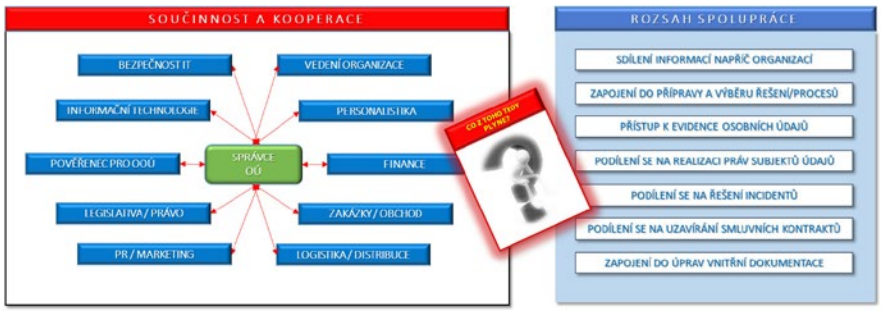
Poskytujete služby pověřence pro ochranu osobních údajů (OÚ). Z praxe víme, že jedním z největších problémů při ochraně osobních údajů je nespolupráce mezi jednotlivými útvary správce, ať už v soukromém nebo veřejném sektoru. Co patří mezi největší rizika této nespolupráce?

Obecně platí, že nesdílení informací či neposkytování součinnosti při plnění požadovaných činností způsobuje větší či menší potíže a může vést k vzniku bezpečnostního incidentu. Mějme na paměti zlaté pravidlo, že *řetěz je tak silný jako jeho nejslabší článek*.

Co z toho plyne v našem případě?

Sdílení informací a součinnost mezi jednotlivými útvary správce je nezbytná pro řádné a efektivní zajištění plnění požadavků ochrany osobních údajů a potažmo kybernetické bezpečnosti. V dnešní velmi turbulentní kybernetické době, kdy únik dat může být otázkou okamžiku, je nezbytné reagovat na případné

Další obsah



incidenty velmi rychle a efektivně. Z hlediska ochrany je lepší spíše incidentům předcházet, a to preventivními opatřeními, která se skládají z kombinace procesů, technologií a lidského faktoru. Takže pokud je slabý článek řetězu právě v nesoučinnosti, respektive nespolupráci mezi jednotlivými útvary, které se podílí na ochraně osobních údajů, zvyšuje se potenciální riziko vzniku incidentů. To samé se týká i rizik spojených s povinnostmi, které má správce řádně a včas plnit.

V čem se mohou rizika, která vyplynou z nespolupráce, projevit?

Například ve špatných procesech zpracování OÚ, ve špatné evidenci OÚ, účelů a lhůt zpracování apod., ve špatném plnění práv subjektu údajů, v nedostatečné ochraně OÚ, v nedostatečné identifikaci a řešení incidentů či v nedostatečně kvalitní smluvní a interní dokumentaci.

Tato rizika mají následně vliv na plnění povinností plynoucích z příslušné legislativy. Z toho je zřejmé, že nesoučinnost v rámci řešení problematiky ochrany osobních údajů může vést k situacím, kdy nebude řádně plněna legislativa či „best practicies" z oblasti ochrany osobních údajů či kybernetické bezpečnosti.

Pověřencem bývá často právník, který přesně neví, co má požadovat například po útvaru odpovědném za IT. Jak má pověřenec od základu nastavit vztahy s IT?

Takový pověřenec by se měl nejprve seznámit se základy fungování IT, aby věděl, co má po útvaru IT požadovat, a rozuměl i tomu, co dostane od IT za informace.

Proč je to důležité?

Je to z toho důvodu, že právník se velmi dobře orientuje v oblasti práva a IT odborník zase v IT. Avšak jednotlivé pojmy a popisy situací nejsou v jazyku „právním" a „IT" stejné. Současně pověřenec by měl disponovat IT znalostmi:

1. aby si uvědomil jednotlivé hrozby, které vyplývají:
   a. z neplnění legislativy
   b. z IT bezpečnosti, kybernetické bezpečnosti;
2. aby měl představu o tom, kde, jak, proč dochází v prostředí IT ke zpracování osobních údajů. Co dělají jednotlivé komponenty, kudy data protékají, tudíž kde jsou zpracovávány osobní údaje, a to nejen lidmi, ale právě i IT technologiemi. Takové zpracování téměř na 99 % uniká pozornosti DPO či osobám odpovědným za ochranu osobních údajů, především pokud nemají dostatečné IT povědomí.

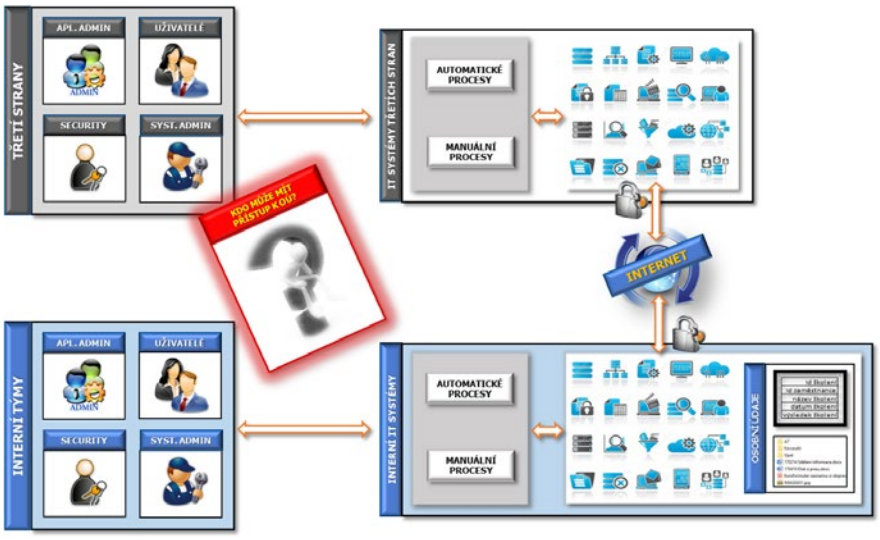
Jak jsme si dříve řekli, právníci bez dostatečné znalosti IT prostředí a fungování musí velice úzce spolupracovat s někým, kdo jim s danou oblastí IT prostředí pomůže, což jsou pracovníci IT útvarů. Je tedy jasné, proč si nastavit „vztah" s IT útvarem.

Proč je nezbytné znát fungování IT prostředí při zpracování OÚ?

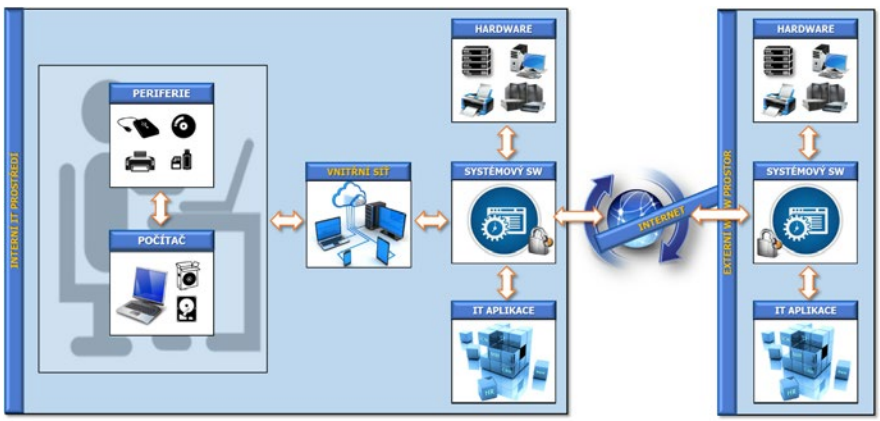
Především proto, abyste si dokázali odpovědět na tyto otázky:

- Jak jsou OÚ zabezpečeny v rámci IT prostředí?
- Jaké OÚ jsou v IT prostředí zpracovávány?
- Jakým způsobem jsou OÚ přenášeny v rámci IT prostředí (v mém, ale i v IT prostředí poskytovatele IT služeb, programů, portálů či třetích stran)?
- Kde jsou OÚ uloženy?
- Kde jsou OÚ zálohovány?
- Kde jsou zpracovávány OÚ?
- Kdo má k OÚ přístup?
- Kdo OÚ zpracovává (lidé, ale i IT řešení)?
- Proč a jakým způsobem jsou OÚ zpracovávány?
- apod.

Bez odpovědí na tyto otázky, nemůže být řeč o tom, že mám dostatek informací o OÚ a o jejich zpracování. S ohledem na skutečnost, že v současné době dochází ke zpracování OÚ především v IT prostředí, je nezbytné disponovat těmito znalostmi.



Základní schéma IT prostředí při zpracování osobních údajů:



Odpovědi na výše uvedené otázky jsou následně zdrojem k vytvoření *základního modelu* zpracování OÚ v prostředí IT. Tento model je odrazovým můstkem pro mapování zpracování OÚ v IT prostředí, ukazuje, na co se zaměřit, kde hledat OÚ, kde se zpracovávají, kudy protékají, kdo k nim má přístup, jak se s nimi nakládá, jak jsou zabezpečeny, jak jsou uloženy apod. Což jsou základní informace pro vytváření přehledu o zpracování OÚ. Z daných informací lze následně vytvářet příslušnou dokumentaci (záznamy o činnostech zpracování, informační povinnost apod.), identifikovat s kým a proč je nezbytné uzavírat smluvní vztahy řešící zpracování a ochranu osobních

údajů, dále slouží jako podklad pro plnění práv subjektu údajů apod. Je tedy zcela evidentní význam daných informací.

Kybernetické útoky v nejrůznější podobě jsou stále častější. Jak souvisí kybernetická bezpečnost s ochranou osobních údajů?

Kybernetická bezpečnost a ochrana osobních údajů jsou více méně spojené nádoby. Hrozba v kybernetickém prostoru, tedy jinak řečeno v IT prostředí (o tom už byla řeč), se vztahuje k datům. No a mezi daty jsou současně i osobní údaje. Útočníci se zaměřují na kompromitaci informací (údajů) a je jedno, zda jsou to OÚ nebo ne. Proto je třeba přemýšlet v tomto kontextu. Neznamená to, že když nespadám pod zákon o kybernetické bezpečnosti (zákon 181/2014 Sb.), kybernetická bezpečnost se mě netýká. S ohledem na rozvoj v oblasti elektronizace služeb je rizikem i samotný přístup k údajům pracovníků úřadů či organizací.

Proč?

V případě, že se mi útočník dostane do mého počítače, může se dostat i k údajům, ke kterým má přístup daný uživatel počítače. Je tedy vidět, že i takový způsob může vést ke kompromitaci OÚ.

Jaké další situace mohou nastat?

Například se vám do počítače „dostane" tzv. RANSOMWARE[1]. Pak může dojít k situaci, kdy nebude možné poskytovat informace, protože budou zašifrované, případně počítač nebude vůbec funkční. Pokud jsou data pravidelně a řádně zálohována, lze vše postupně a v klidu opravit, daný RANSOMWARE se odstraní a počítač funguje dál. Proto hlavně doporučuji dodržovat tu základní a nezbytnou podmínku: pravidelně a řádně zálohujte!

Ale pozor, i taková banalita, jako je zaslání e-mailu, může skončit špatně. Ukážeme si to na dalším příkladu, kdy kybernetický útok začíná odchytáváním informací zaslaných pomocí e-mailu.

Schéma vlevo dole ukazuje, jak může dojít ke kompromitaci údajů, když komunikace není zabezpečená (e-mailová nebo jen přes prohlížeč). Jedná se o situaci zobrazenou v horní polovině obrázku (růžový podkres). Na zeleném podkresu naopak vidíte situaci, kdy komunikace zabezpečená je a případný kybernetický útok zaměřený na odchytávání informací nezabezpečenou formou komunikace je eliminován.

Jaké typy útoků jsou podle vašich zkušeností v praxi nejčastější? Jaké požadavky má klást pověřenec na zaměstnance, aby se riziko co nejvíce snížilo?

Příslušná pravidla či požadavky na eliminaci rizik plynoucích z kybernetických útoků by měla vycházet z prevence. Tedy musí existovat příslušná pravidla a procesy, které je nezbytné uživatelům vštěpovat, a to neustále. Kybernetické útoky jsou stále více sofistikované a dynamicky se mění. Proto je potřeba znalosti sdílet a přetvářet je do pravidel a procesů bezpečného chování (reprezentovaných např. pomocí směrnic). Školení a znalost hrozeb a způsobů je asi ten nejjednodušší a nejefektivnější způsob, jak takové hrozby eliminovat. Samozřejmě, že je nezbytné mít i zabezpečené IT prostředí, poučené správce IT prostředí a technologie eliminující hrozby.

Obecně lze ale shrnout pravidla do těchto bodů:

- Dodržujte směrnice a bezpečnostní pokyny.
- V případě, že si nejste jisti, co to přišlo e-mailem, pak takový e-mail neotevírejte, neposílejte jej dále, ale informujte příslušnou osobu, jež má odpovědnost za IT bezpečnost.
- Neposílejte OÚ nezabezpečené e-mailem.
- Používejte jen oficiální SW.
- Když se váš počítač chová nestandardně (je pomalý, nejdou otevřít soubory, které běžně otevřít šly), neprodleně o tom informujte příslušnou osobu.
- Někdo volá a není možné u něj ověřit identitu? Vezměte si na něj kontakt, spojte se s DPO či jinou pověřenou osobou, situaci konzultujte.

Pokud už k útoku dojde a pověřenec má podezření na bezpečnostní incident, jaké by měly být jeho první kroky?

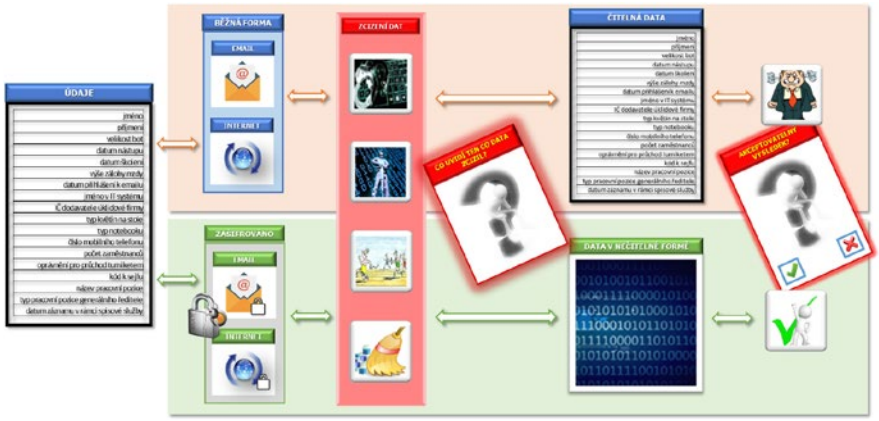
Obecně je třeba zachovat chladnou hlavu. Ono totiž ne všechno, co se na začátku může jevit jako bezpečnostní incident, incidentem být musí. V žádném případě to ale neznamená, že máte být v pohodě, to nikoliv.

Na začátku by měl pověřenec zahájit vyšetřování. To začíná tím, že informuje příslušnou osobu (statutární orgán, případně jinou pověřenou osobu) o zahájení daného šetření. Následně musí získat maximum informací o dané situaci, v případě, že si šetření vyžádá spolupráci s pracovníkem IT bezpečnosti či IT, je nezbytné okamžitě získat danou součinnost (pro takový případ musí být vše předem připraveno a součinnost zajištěna). Po vyhodnocení situace je třeba rozhodnout, zda se jedná o incident a identifikovat rizika, rozsah dopadů na OÚ, subjekty údajů apod. Následně se sestaví plán eliminace rizika a informuje se příslušná odpovědná osoba (jako viz výše). Dále je nutné rozhodnout, zda je třeba tento incident hlásit (čl. 33 obecného nařízení). Musíte také informovat uživatele, zvážit informování a spolupráci s orgány činnými v trestním řízení, ÚOOÚ či jinými příslušnými orgány dle stupně závažnosti. Nakonec je nutné spustit plán eliminace incidentu a v neposlední řadě incident zaznamenat krok po kroku a zajistit příslušné skutečnosti a důkazy.

Děkuji za rozhovor!

Připravila Eva Janečková

Kybernetické útoky na nezabezpečenou komunikaci v prostředí internetu (e-mail, WEB prohlížeč)



1) **Ransomware** je škodlivý kód, který zamyká přístup k infikovanému zařízení nebo šifruje jeho obsah. Po uživateli požaduje výpalné s příslibem (samozřejmě negarantovaným), že po zaplacení dojde k zpřístupnění zařízení a/nebo odšifrování dat. Jde o specifický druh škodlivého kódu, který se používá pro vydírání uživatelů. Po úspěšném infikování zařízení blokuje přístup k zařízení nebo šifruje definovaná data na disku. Na obrazovce se zobrazí výzva k zaplacení „výpalného", v některých případech i s informací, kolik času uživateli na zaplacení zbývá. Po uplynutí doby se požadovaná částka navýší. (https://www.eset.com/cz/ransomware/)

Spolek pro ochranu osobních údajů a aktuální témata ochrany dat

V souvislosti s napadením Ukrajiny vojsky Ruské federace a změněnou geopolitickou situací upozornil i Spolek pro ochranu osobních údajů na některá témata v oblasti ochrany soukromí a osobních údajů, která v důsledku válečné situace získají na významu. Stanovisko publikoval Spolek v češtině a rovněž v angličtině na webových stránkách Evropské federace pověřenců pro ochranu osobních údajů.

Představujeme další pracovní komisi

Informace o činnostech některých pracovních komisí Spolku pro ochranu osobních údajů se objevily v měsíčníku DPO už vloni. Nyní je konečně na řadě další. Představujeme vám komisi, která vznikla koncem minulého roku rozdělením komise pro veřejnou správu a samosprávu na samostatné oblasti, tedy na vyčleněnou oblast státní správy a samostatnou oblast územní samosprávy.

Proč došlo k tomuto rozdělení?

Hlavním důvodem byla zejména snaha více koordinovat některé postupy a návrhy metod v oblasti ochrany osobních údajů, jež za relativně specifických podmínek zpracovávají jinak orgány státní správy a jinak orgány územní samosprávy.

Co je úkolem komise pro státní správu?

Komise pro státní správu se zabývá ochranou osobních údajů v rámci činností ústředních i ostatních orgánů státní správy, tedy především ministerstev a správních úřadů. Primární činností a cílem komise je především vzájemná výměna zkušeností a poznatků jednotlivých členů zabývajících se zpracováním osobních údajů v rámci státní správy a aktivní spolupráce při tvorbě metodických doporučení a pozičních dokumentů Spolku.

Komisi předsedá Jaroslav Hora

Jaroslav Hora působí jako pověřenec na Českém statistickém úřadu, je dlouholetým členem Spolku a zároveň členem poroty prestižní soutěže o nejlepšího pověřence pro ochranu osobních údajů. Komise, jíž Jaroslav Hora předsedá, se schází pravidelně každý měsíc. Předmětem jednání bývá konzultace a vzájemná výměna informací a zkušeností k aktuálním tématům vybraných oblastí zpracování osobních údajů. Setkání členů komise, jež má předem stanovený program, se realizuje pokaždé formou online konferenčního jednání a připravené sdílené prezentace.

Jaroslav Hora

A o čem už se diskutovalo?

Na jednáních, jež proběhla v koordinaci s činností a závěry dalších souvisejících komisí (především komisí pro elektronické komunikace a komisí pro územní samosprávu), se diskutovalo zejména o problematice cookies s přihlédnutím ke specifickým omezením ve státní správě, a to hlavně v kontextu novelizace zákona o elektronických komunikacích účinné od letošního 1. ledna. Předseda komise představil konkrétní postupy pro kontrolu nastavení a doporučeného použití cookies v praxi. Kromě diskuse o specifických omezeních při použití cookies a marketingových a analytických nástrojů byla na programu jednání také aktuální problematika whistleblowingu, a to v souvislosti s účinností evropské směrnice na ochranu oznamovatelů.

Spolek začal spolupracovat s Rozhodčím soudem při HK ČR a AK ČR

Spolek rovněž navázal spolupráci s Rozhodčím soudem při Hospodářské komoře České republiky a Agrární komoře České republiky. Spolupráce se orientuje na zvyšování povědomí o rozhodčím řízení jako vhodné formě řešení sporů týkajících se otázek zpracování osobních údajů. Spolek zároveň povede seznam rozhodců doporučovaných pro spory v oblasti ochrany osobních údajů. Více v tiskové zprávě.

Seminář o budoucnosti ochrany dat z amerického a evropského pohledu

V úterý 22. března uspořádal Spolek ve spolupráci s International Association of Privacy Professionals online seminář nazvaný Budoucnost ochrany dat z amerického a evropského pohledu. Více informací o semináři přineseme příště.

Nominace na ocenění Pověřenec roku uzavřeme na konci března

Na konci března uzavřeme nominace na ocenění Pověřenec pro ochranu osobních údajů roku. Nominované nyní vyhodnotí porota. Vyhlášení výsledků a předání ocenění se uskuteční ve čtvrtek 26. května v Praze. Více informací je dostupných na našem webu.

Rozsudek Evropského soudu pro lidská práva ve věci č. 70838/13 Antović a Mirković proti Černé Hoře

Natáčením posluchárny na univerzitě bylo porušeno právo vyučujících této univerzity na respektování jejich soukromého života. Takový rozsudek vynesl dne 28. listopadu 2017 senát druhé sekce Evropského soudu pro lidská práva ve Štrasburku (dále „ESLP“) ve věci Antović a Mirković proti Černé Hoře. Soud se týkal práva na respektování rodinného a soukromého života podle článku 8 Evropské úmluvy o ochraně lidských práv a základních svobod (dále „EÚLP“, po ratifikaci Českou republikou v roce 1992 je vyhlášena pod č. 209/1992 Sb.).

Kdy, kde, co?

Stěžovatelé podali žalobu k ESLP v říjnu 2013. Oba vyučovali na Černohorské univerzitě v Podgorici. Co jim vadilo? V roce 2011 nechal děkan Přírodovědecko-matematické fakulty do některých prostor včetně poslucháren instalovat videokamery. O této skutečnosti byli vyučující na fakultě informováni. Důvodem pro nasazení monitorovacího systému měla být ochrana majetku a osob, šlo také o dozor nad vyučováním. Získané údaje byly šifrovány a klíč znal pouze děkan. Záznamy se ukládaly po dobu jednoho roku, nicméně kvůli nedostatečné kapacitě úložiště se staré záznamy po 30 dnech automaticky přehrávaly novými.

Jen se souhlasem subjektu údajů

Podle černohorského zákona o ochraně osobních údajů lze osobní údaje zpracovávat jen se souhlasem subjektu údajů, jenž má možnost souhlas kdykoli odvolat. Subjekt má být informován o právním základě zpracování. Veřejné instituce mohou dle zákona kamerami monitorovat vstupní prostory svých budov. Monitorovat lze i s cílem zajistit bezpečí osob anebo majetku nebo kvůli ochraně důvěrných informací, jestliže to nelze zařídit jiným způsobem.

K pořizování záznamu v posluchárně nedali vyučující souhlas

Oba pedagogové podali stížnost u Agentury na ochranu osobních údajů. Napadli zejména pořizování záznamu v posluchárně, kde přednášeli. K pořizování totiž nedali souhlas. Ochrana majetku byla zajištěna tak, že se posluchárna po konci hodiny vždy zamykala, navíc jediným vybavením byly židle, lavice a tabule. Vyučující žádali odstranění kamer a zničení záznamů. Agentura provedla inspekci a následně vydala rozhodnutí, že sledování pomocí kamer byla v souladu s vnitrostátním zákonem na ochranu osobních údajů. Stěžovatelé podali námitku, v níž zdůraznili, že přínos kamer používaných v posluchárně k ochraně osob a majetku není jasný. Jiné kamery snímaly vstupy a východy z budovy, což mohlo zajistit dostatečnou ochranu. Poukázali rovněž na to, že o sledování pomocí kamer nebyli informováni předem a informace jim byla sdělena pouze ústně. Námitku agentura přijala a vydala nové rozhodnutí, podle kterého skutečně škola neprokázala, že by byl nějak ohrožen majetek či osoby a že monitoring vyučování (který univerzita zřejmě uvedla jako další účel) nebyl dostatečným důvodem pro rozmístění kamer v posluchárnách. Škola poté odstranila kamery z poslucháren a vymazala záznamy.

Vyučující se domáhali také náhrady škody za narušení práva na soukromí

Oba vyučující rovněž podali žalobu, jíž se domáhali náhrady škody za narušení práva na soukromí od univerzity, Agentury na ochranu osobních údajů a také státu. Porušení práva na soukromí mělo spočívat v nedovoleném sběru a zpracování jejich osobních údajů. Konkrétně tvrdili, že toto narušení soukromí, které neměli jak ovlivnit, nebylo podloženo žádným právním předpisem, tudíž bylo nezákonné a došlo k porušení čl. 8 odst. 2 EÚLP. Další právní argumenty žalobců zahrnovaly ustanovení zákona o ochraně osobních údajů a příslušnou judikaturu ESLP.

Prvoinstanční soud rozhodl ve prospěch žalované strany

Prvoinstanční soud rozhodl ve prospěch žalované strany. Odůvodnil to mj. skutečností, že univerzita je veřejnou institucí vykonávající činnosti ve veřejném zájmu. Mezi ně zařadil i výuku. Z tohoto důvodu nemohlo snímání posluchárny narušit soukromý život žalobců – jedná se o pracovní prostor, kde vyučující nejsou nikdy o samotě, a proto se lze v této souvislosti stěží domáhat práva na soukromí. Takto získané údaje nelze považovat za údaje osobní.

Žalobci se odvolali

Žalobci se odvolali, v odvolání opět argumentovali článkem 8 EÚLP. Tvrdili, že monitorování poslucháren nebylo v demokratické společnosti nezbytné a že prvoinstanční soud svůj výrok neopřel o žádné konkrétní právní ustanovení. Vrchní soud v Podgorici dal za pravdu soudu první instance v tom, že žalobci nedoložili, že by došlo k narušení jejich práva na soukromí.

Podání k ústavnímu soudu by (ne)bylo účinným opravným prostředkem?

K Ústavnímu soudu Černé Hory se žalobci neobrátili, což byl při řízení o přípustnosti žaloby k ESLP jeden z argumentů vlády Černé Hory. Tvrdila, že nedošlo k vyčerpání všech dostupných účinných vnitrostátních opravných

prostředků. Žalobci však u ESLP uspěli s protiargumentem, že podání k ústavnímu soudu by nebylo účinným opravným prostředkem. Toto nicméně platí ve vztahu k říjnu 2013, kdy oba pedagogové podali žalobu k ESLP. U jiné žaloby podané v březnu 2015 totiž ESLP uznal, že podání k Ústavnímu soudu Černé Hory lze ze zásady za účinný opravný prostředek považovat.

Vyučování probíhá ve veřejném zájmu…

V řízení o přípustnosti žaloby ESLP vláda Černé Hory vznesla námitku, že ne všechny pracovní nebo obchodní aktivity patří do sféry soukromého života. Univerzita podle ní byla veřejnou institucí a vyučování probíhá ve veřejném zájmu. Kamery zabíraly prostor pracovní mimo rámec osobní autonomie – na rozdíl od kabinetů, kde se soukromý prostor do určité míry předpokládá.

Soud se s tvrzením vlády neztotožnil

Soud se s tvrzením vlády neztotožnil a prohlásil, že soukromý život zahrnuje i pracovní aktivity nebo aktivity ve veřejném prostředí. Většina lidí má během pracovního života významnou či dokonce největší příležitost rozvíjet vztahy s vnějším světem. Dělící linie mezi pracovním, resp. veřejným, a soukromým životem je nejasná a veřejné anebo pracovní aktivity mohou být součástí soukromého života. V tomto případě soud uznal výuku jako takovou za veřejnou, ale jiné interakce se studenty už mohly být soukromého rázu. Již dřívější rozhodnutí ESLP stanovila, že skrytý monitoring zaměstnance na pracovišti prostřednictvím kamer má být považován za významný zásah do soukromí. V tomto případě soud neshledal důvod pro to, aby totéž nevztáhl také na monitoring kamerami, kterého si je zaměstnanec vědom.

V čem spočívalo jádro žaloby?

Jádro žaloby spočívalo v tom, že napadené snímání kamerami bylo nezákonné, nemělo

žádný oprávněný účel a nebylo v demokratické společnosti nezbytné. Jako subjekty údajů žalobci neměli možnost účinně rozhodovat o svých osobních údajích. Vláda namítla, že pořízený záznam nebyl narušením soukromého života, kterým by se stal až v případě předání jiné osobě nebo zveřejnění. Instalace kamer měla zabránit bezpečnostním incidentům a pomoci při jejich vyšetřování. Konkrétně se mělo jednat o krádeže a vloupání, při kterých by došlo k odcizení majetku univerzity i jejích vyučujících. Stejně tak měly zabránit vnášení zbraní a nepovolenému přivedení zvířat, žebrání a incidentům, při nichž by bylo vyučujícím vyhrožováno fyzickým násilím.

Nešlo to i jinak?

Zásadní byla otázka, zda účelu rozmístění kamer nešlo dosáhnout méně invazivním způsobem. Kromě ochrany majetku a osob mělo rozmístění kamer v tomto případě také za cíl monitorování výuky. Tento účel pořizování videozáznamu neměl podle ESLP oporu v zákoně. Agentura pro ochranu osobních údajů navíc dospěla k výslovnému závěru, že k ohrožení osob ani majetku nedošlo. Ani tento účel tedy nebyl dostatečným základem. V této souvislosti ESLP dospěl k závěru, že vnitrostátní soudy tuto klíčovou otázku ve svém rozhodování vůbec neřešily. Vláda Černé Hory ohrožení majetku či osob nedoložila a ani neprokázala, že by se předem zvážily alternativy k rozmístění kamer. Konečný výrok proto potvrdil, že čl. 8 EÚLP byl porušen.

Soud dal žalobcům zapravdu. Hlasování bylo těsné

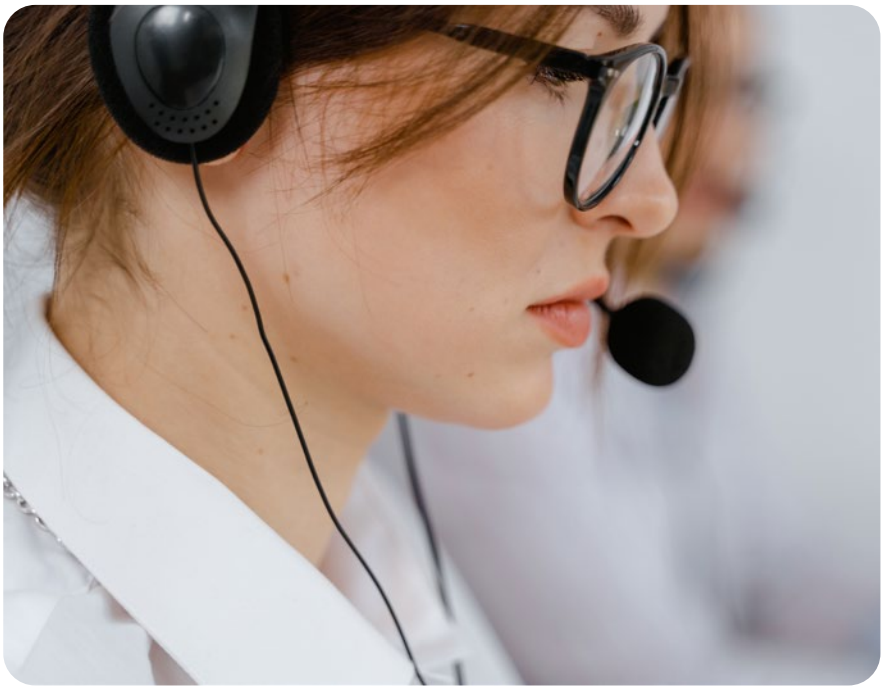
Soud žalobcům přiznal náhradu za nemajetkovou újmu a uložil vládě Černé Hory uhradit jim také náhrady spjaté s řízením před vnitrostátními soudy i ESLP. Hlasování bylo těsné, pro se vyslovili čtyři soudci ze sedmi. Důvodem nesouhlasu tří soudců bylo z jejich pohledu příliš široké vnímání „soukromého života" a skutečnost, že očekávání soukromí žalobců vykonávajících pracovní činnost ve veřejném prostoru, jakým je posluchárna vysoké školy, a navíc s vědomím, že jde o prostor monitorovaný kamerami, musela být velmi omezená.

Pavel Janeček
Autor je odborník
na mezinárodní vztahy

Telemarketing po novele zákona o elektronických komunikacích
Konec nežádoucích nabídek po telefonu

Nevyžádané telefonáty od letošního roku výrazně omezuje novela zákona o elektronických komunikacích (ZEK). Spotřebitele je možné kontaktovat jen tehdy, pokud k telemarketingu udělí souhlas. Právní konstrukce a formulace, které zákonodárce zvolil, však vytváří jisté výkladové nejasnosti.

Novela zákona č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů, byla přijata vloni v září v návaznosti na přijetí směrnice Evropského parlamentu a Rady (EU) 2018/1972 ze dne 11. prosince 2018, kterou se stanoví evropský kodex pro elektronické komunikace. S účinností od 1. ledna 2022 nastaly ve světě elektronických komunikací poměrně zásadní změny. Nejen v oblasti využívání cookies (o níž jsme informovali v únorovém čísle DPO), ale také v telemarketingu. Tyto změny bezprostředně souvisí s nastavením procesů zpracování osobních údajů, a tedy s plněním povinností vyplývajících z GDPR.[1)]



Telemarketing: Cílem bylo zamezit nevyžádaným hovorům

Telemarketing, případně marketingová sdělení obecně, je další oblastí, do níž se přijatou novelou ZEK promítl princip opt-in. Deklarovaným cílem změn v přístupu k telemarketingu bylo zamezit obtěžujícím marketingovým hovorům, což je nepochybně žádoucí. Právní konstrukce a formulace, které zákonodárce zvolil, však vytváří jisté výkladové nejasnosti.

Volat s nabídkou zboží či služeb (marketingové volání) je podle nového znění § 96 odst. 1 ZEK možné již jen těm účastníkům a uživatelům,[2)] kteří ve veřejném seznamu uvedli, že si přejí být za tímto účelem kontaktováni (dříve platil opačný princip: ve veřejném seznamu bylo možno uvést přání nebýt kontaktován). Na základě § 96 odst. 2 a § 95 odst. 5 ZEK se pak tento zákaz vztahuje i na automatická volací zařízení a na náhodně vygenerovaná telefonní čísla, což byl častý způsob, jak volající požadavky ZEK a GDPR obcházeli. Potud se zdá být situace jasná.

Veřejný charakter seznamu ale není výslovně uvedený...

Komplikaci při výkladu představuje fakt, že zákaz obtěžujícího marketingového volání je formulován jako zákaz využívat za tímto účelem veřejné účastnické seznamy, resp. účastnické seznamy,[3)] přičemž legální definice nebo rozlišení těchto pojmů ZEK neobsahuje.[4)] Z § 95 odst. 1 ZEK, na který zákaz marketingu odkazuje, lze dovodit, že seznamem účastníků je takový seznam (přehled), který byl vytvořen a vydán za účelem vyhledávání kontaktů na základě jména nebo jiného identifikátoru účastníka. Veřejný charakter seznamu zde výslovně uveden není.

Další rozšíření významu účastnického seznamu přinesla novelizovaná podoba § 95 odst. 5 ZEK, jejímž cílem bylo rozšířit zákaz obtěžujícího marketingového volání i na náhodně generovaná čísla, a v níž se uvádí, že kromě vygenerovaných čísel je účastnickým seznamem „rovněž seznam telefonních čísel bez jiných identifikačních údajů nebo seznam, ve kterém se uvádí telefonní čísla či osobní nebo identifikační údaje účastníků, kteří neuvedli, že si přejí být kontaktováni za účelem marketingu." Z uvedeného vyplývá, že princip opt-in dopadá na veškeré kontaktní údaje, které jsou v seznamu uvedeny, nikoli pouze na telefonní čísla. Zákaz nevyžádaného marketingu se tak týká nejen telefonních hovorů, ale např. i newsletterů zasílaných e-mailem. Ani zde není výslovná vazba na veřejný typ účastnického seznamu.

Zákaz marketingového využití kontaktů bez předchozího souhlasu účastníka či uživatele tak platí pro kontaktní údaje uvedené v/ ve:

- veřejném seznamu (§ 96 odst. 1 ZEK),
- účastnickém seznamu (§ 96 odst. 2 ZEK),
- náhodně vygenerovaném seznamu telefonních čísel (§ 95 odst. 5 ZEK, věta první),
- seznamu telefonních čísel bez jiných identifikačních údajů (§ 95 odst. 5 ZEK, věta druhá),
- seznamu, ve kterém se uvádí telefonní čísla či osobní nebo identifikační údaje účastníků (§ 95 odst. 5 ZEK, věta druhá).

---

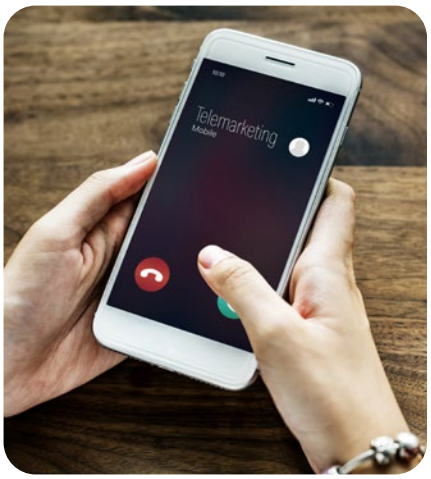
1) Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (Obecné nařízení o ochraně osobních údajů).
2) Účastníkem je podle § 2 písm. a) ZEK „každý, kdo uzavřel s podnikatelem poskytujícím veřejně dostupné služby elektronických komunikací smlouvu na poskytování těchto služeb", uživatelem pak podle § 2 písm. b) ZEK „každý, kdo využívá nebo žádá veřejně dostupnou službu elektronických komunikací."
3) Ustanovení § 96 odst. 1 ZEK odkazuje na veřejný seznam podle § 95 odst. 1 písm. b) nebo § 95 odst. 2. V § 96 odst. 2 ZEK je po novele odkaz na účastnické seznamy podle § 95.
4) Zkratku „účastnický seznam" zavádí ZEK v § 36 odst. 6, a to pro seznam telefonních čísel účastníků veřejně dostupné telefonní služby. Dále v textu se však tento pojem objevuje i v jiném významu, např. i pro označení seznamu všech podnikatelů poskytujících veřejně dostupné telefonní služby (§ 41 odst. 1 ZEK).

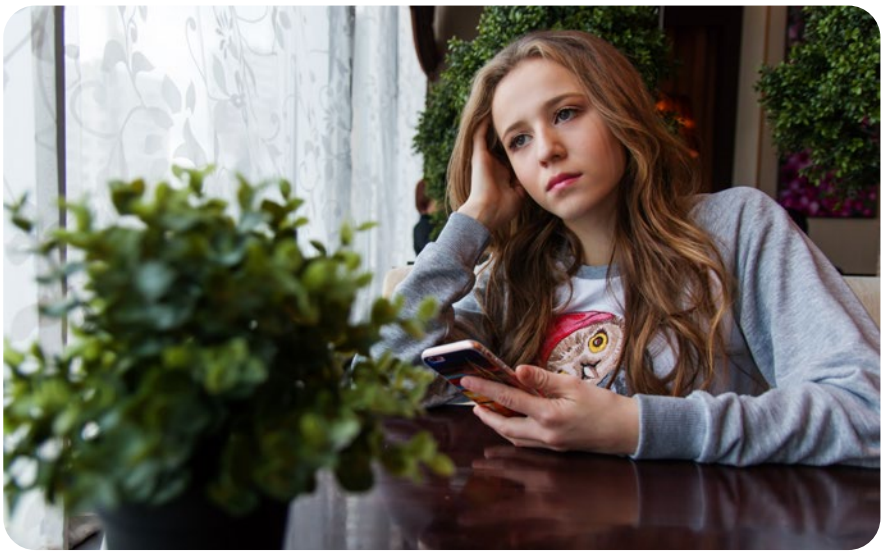
Nejednotnost názvosloví vytváří prostor pro výkladové pochybnosti

Tato nejednotnost názvosloví pak vytváří prostor pro výkladové pochybnosti. A zejména v případě posledních dvou typů seznamů, které zmiňuje § 95 odst. 5 ZEK, není zřejmé, zda je vždy myšlen tentýž typ seznamu – veřejný, resp. určený k vydání, anebo zda regulace dopadá na jakékoli seznamy tohoto typu bez ohledu na jejich neveřejný charakter.

Samotným jazykovým výkladem ustanovení § 95 odst. 5 ZEK lze totiž dospět k závěru, že toto ustanovení se vztahuje na všechny seznamy, přehledy či databáze (zahrnující telefonní čísla či jiné kontaktní údaje) bez ohledu na to, kdo je vytvořil, a především bez ohledu na to, zda jsou určeny k vydání (zveřejnění) či nikoli. Novela ZEK by se při takovém výkladu vztahovala např. i na podnikatele a jejich interní databáze kontaktních údajů zákazníků.

Tento výklad by však zásadně měnil dosavadní praxi, kdy je zpracování kontaktních údajů zákazníků pro marketingové účely možné na základě oprávněného zájmu daného prodejce či poskytovatele služeb. Uvedené vyplývá z § 7 odst. 3 zákona č. 480/2004 Sb., o některých službách informační společnosti a o změně některých zákonů (zákon o některých službách informační společnosti)[5], resp. pro osobní údaje ve spojení s čl. 6 odst. 1 písm. f) GDPR.[6] Podle citovaných ustanovení je možné využívat kontaktní údaje získané v souvislosti s vyřizováním předchozích zakázek také pro marketingové nabídky na vlastní podobné zboží či služby. Teprve poté, co zákazník další marketing odmítne, je nutno jej z databází určených pro marketing odstranit (resp. označit zde jeho přání nebýt nadále kontaktován). Ani zákon č. 480/2004 Sb., ani GDPR neumožňují v tomto případě další využití kontaktních údajů s odkazem na případný převyšující zájem na pokračování v marketingových aktivitách.





Předchozí souhlas je vyžadován až v případě, kdy má obchodník či poskytovatel služeb zájem sdělovat či zasílat svým zákazníkům nabídky z jiné oblasti svého sortimentu či služeb anebo obecnější informace o své činnosti (např. nabídky na účast v zákaznických soutěžích nebo pozvánky na akce).

Pokud by se však aplikoval výše uvedený jazykový výklad, tedy že zákaz marketingu bez předchozího souhlasu se (s odkazem na nové ustanovení § 95 odst. 5 ZEK) aplikuje i na interní databáze a systémy s kontaktními údaji zákazníků, fakticky by od 1. ledna 2022 nebylo možné oslovovat stávající zákazníky v režimu podle § 7 odst. 3 zákona č. 480/2004 Sb. a na základě oprávněného zájmu ve smyslu čl. 6 odst. 1 písm. f) GDPR.

Co bylo záměrem zákonodárce není z důvodové zprávy zřejmé

Z důvodové zprávy ke stávajícímu znění ZEK ani z důvodové zprávy k novele ZEK nelze zjistit, zda bylo záměrem zákonodárce vytvořit několik kategorií účastnických seznamů, ani zda bylo cílem podřídit regulaci i interní zákaznické databáze. Není zřejmý ani zamýšlený vztah s právními předpisy, které řeší související problematiku, konkrétně využití kontaktních údajů pro zasílání obchodních sdělení (zákona č. 480/2004 Sb.) a zpracování osobních údajů za tímto účelem (GDPR).

Regulace dopadá výhradně na veřejné seznamy účastníků

S odkazem na působnost a znění evropské legislativy, která byla novelou ZEK transponována, lze ale soudit, že takový záměr sledován nebyl. Tento závěr potvrdily ve svém společném vyjádření i příslušné státní úřady (Český telekomunikační úřad, ÚOOÚ a Ministerstvo průmyslu a obchodu).[7] Z odpovědí na otázky zodpovězené v tomto stanovisku vyplývá, že regulace obsažená v ZEK dopadá výhradně na veřejné seznamy účastníků, nikoli na interní kontaktní databáze zákazníků. V odpovědi na dotaz č. B.2 se výslovně uvádí, že změna režimu na opt-in nemění nic na možnosti kontaktovat vlastní zákazníky s relevantní nabídkou zboží či služeb, neboť zdrojem kontaktu není v tomto případě veřejný účastnický seznam.

Pro budování, správu a další využívání databází zákaznických kontaktů (tj. kontaktních údajů získaných od zákazníků individuálně, v kontextu s poskytováním služby či prodejem zboží) tak i nadále platí pravidla stanovená v zákoně č. 480/2004 Sb. a GDPR. Teprve v případě, že by zdrojem kontaktů pro marketing byl veřejný seznam účastníků, platí, že s účinností od 1. ledna 2022 lze v souladu s ZEK oslovit pouze ty, u nichž je uvedeno, že s takovým využitím svých údajů předem souhlasili.

Ludmila Probstová
Autorka je GDPR specialistka ve společnosti Bosch.

5) § 7 odst. 3 zákona č. 480/2004 Sb. říká, že kontaktní údaje zákazníka („podrobnosti elektronického kontaktu pro elektronickou poštu"), které byly získány v souvislosti s prodejem výrobku nebo služby, lze využít pro potřeby šíření obchodních sdělení, pokud se týkají vlastních obdobných výrobků nebo služeb (zákazníkovi je současně nutno umožnit jednoduchým způsobem odmítnout další zpracování údajů za tímto účelem).

6) Informování o zboží či službách souvisejících s předchozím nákupem lze nepochybně považovat za oprávněný zájem; balanční test by v tomto případě měl – při zachování rozumného rozsahu informací a doby uchování – vyznít ve prospěch správce.

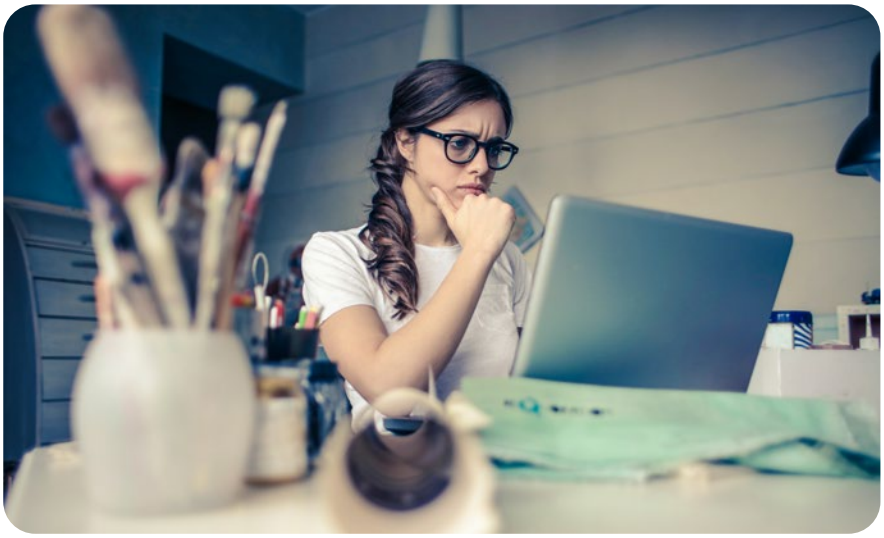
7) Telemarketing – výkladové stanovisko s odpověďmi na nejčastější dotazy veřejnosti (www.uoou.cz).

Když jde o výzkum? Aneb některé problematické body zpracovávání osobních údajů ve výzkumu

Obecné nařízení o ochraně osobních údajů se ve srovnání s předchozí právní úpravou poměrně široce věnuje zpracovávání osobních údajů pro účely vědeckého a historického výzkumu. Ustanovení čl. 89 GDPR a s ním související ustanovení obsahují určité výjimky, pokud je účelem zpracování výzkum. Těmito výjimkami jsou výjimky z omezení účelem, z omezení doby zpracování, ze zákazu zpracování zvláštních kategorií údajů, z informační povinnosti nebo z práva na výmaz. To je také důvod, proč nařízení v prvním odstavci klade důraz na vhodné záruky pro práva a svobody subjektu údajů spočívající v přijetí dostatečných technických a organizačních opatření. Pokud je to pro splnění účelu možné, musí správce osobní údaje anonymizovat. Demonstrativní výčet těchto opatření je uveden v § 16 zákona č. 110/2019 Sb., o zpracování osobních údajů. Jsou jimi například minimalizace údajů a jejich pseudonymizace, jmenování pověřence, šifrování, umožnění přístupu pouze pověřeným osobám, poučení těchto osob a uchovávání logů, ochrana systémů nebo testování přijatých opatření.

Subjekt provádějící výzkum

Vědecký výzkum chápe nařízení široce. Zahrnuje technologický vývoj a technologické demonstrace, základní výzkum, aplikovaný výzkum a výzkum financovaný ze soukromých zdrojů (bod 159 odůvodnění). Výzkumem není pouze výzkum k tomu zřízenými institucemi, vysokými školami a výzkumnými ústavy. Výzkum mohou provádět i soukromé společnosti a využívat k tomu výjimek obsažených v GDPR.[1] Za neaktuální je proto nutné považovat stanovisko Úřadu pro ochranu osobních údajů č. 2/2006,[2] který pro zpracování pro vědecký účel vyžadoval dvě podmínky: 1) existenci zadání nebo záměru úkolu, jenž



vykazuje znaky vědeckého bádání a 2) výzkum prováděný kvalifikovaným subjektem, tj. subjektem vykazujícím formální předpoklad (právní status) nebo vykazujícím veřejně či jakkoli reálně uznávanou vědeckou či výzkumnou zkušenost. Po účinnosti GDPR došlo k demokratizaci předpokladů použití výjimky pro účely výzkumu, nicméně stále je třeba posuzovat výzkumnou aktivitu nikoliv podle označení, ale podle faktické náplně. Jak uvádí pokyn D-288 vydaný Ministerstvem financí k provedení § 34 odst. 4 a 5 zákona o daních z příjmů,[3] který zmiňuje i judikatura Nejvyššího správního soudu,[4] základním kritériem pro odlišení výzkumu a vývoje od ostatních činností je přítomnost ocenitelného prvku novosti a vyjasnění výzkumné nebo technické nejistoty.

Slučitelnost účelů a právní důvod zpracování

Zpracovávání osobních údajů ve výzkumu podléhá principům a pravidlům nařízení. Osobní údaje mohou být shromážděny přímo pro účel výzkumu, tedy výzkumník je již od subjektu údajů získá s úmyslem použít tyto údaje pro konkrétní výzkumný projekt. Osobní údaje mohou být ale také získány pro jiný účel, a až následně je rozhodnuto o jejich zařazení do výzkumného projektu. Pokud bude mít zpracování pro výzkum za následek vysoké riziko pro práva a svobody fyzických osob z důvodů uvedených v čl. 35 GDPR, bude muset správce vypracovat posouzení vlivu na ochranu osobních údajů (DPAI). Posouzení vlivu bude třeba např. pro zpracování citlivých údajů zranitelných osob v rámci výzkumných projektů.[5]

1) Koščík, Michal a kol. *Výzkumná data a výzkumné databáze: právní rámec zpracování a sdílení vědeckých poznatků*. Vydání první. Praha: Wolters Kluwer, 2017, s. 68, nebo European Data Protection Supervisor. A Preliminary Opinion on data protection and scientific research, 2020, s. 6. Dostupné z: https://edps.europa.eu/sites/edp/files/publication/20-01-06_opinion_research_en.pdf
2) Stanovisko Úřadu pro ochranu osobních údajů č. 2/2006, revidováno v dubnu 2013. Zpracování osobních údajů v rámci vědy. Dostupné z: https://www.uoou.cz/files/stanovisko_2006_2.pdf
3) Pokyn D-288 ze dne 3.10.2005 Ministerstva financí k jednotnému postupu při uplatňování ustanovení § 34 odst. 4 a 5 zákona č. 586/1992 Sb., o daních z příjmů. Dostupné z: https://www.financnisprava.cz/assets/cs/prilohy/d-zakony/D-288.pdf
4) Např. Rozsudek Nejvyššího správního soudu ze dne 24. 11. 2017, č.j. 10 Afs 77/2017 – 53 nebo rozsudek Nejvyššího správního soudu ze dne 26. 7. 2018, čj. 1 Afs 97/2018-41.
5) Pokyny pro posouzení vlivu na ochranu údajů a stanovení, zda „je pravděpodobné, že zpracování údajů bude mít za následek vysoké riziko" pro účely nařízení 2016/679, s. 13.

Přestože musí být osobní údaje shromážděny pro konkrétní účel nebo účely, pamatuje GDPR na situace, kdy je možné osobní údaje získané pro jiný účel zpracovávat ve výzkumu (čl. 5 odst. 1 písm. b) GDPR). Zpracovávání ve výzkumu se nepovažuje za neslučitelné s původním účelem zpracování. Podle bodu 50 odůvodnění by další zpracování osobních údajů pro účely vědeckého či historického výzkumu mělo být považováno za slučitelné s původním účelem. Podle komentářové literatury se nejedná o fikci slučitelnosti účelů, jinými slovy ne každé zpracování pro účely výzkumu bude slučitelné s původním účelem.[6] Správce musí i pro tento účel provést test slučitelnosti podle čl. 6 odst. 4 GDPR.

Neslučitelnost účelů zpracování může nastat zejména v případě, kdy neexistuje žádná vazba mezi původním účelem a zpracováním pro účely výzkumu, nebo za okolností, za nichž byly údaje původně shromážděny, kdy nemohl subjekt údajů legitimně očekávat, že jeho osobní údaje budou zpracovávány ještě za účelem výzkumu. Tuto situaci si lze představit, pokud je výzkum založen např. na analýze velkých dat apod.

Pokud byly osobní údaje původně shromážděny k jinému účelu, mohou se instituce a soukromé společnosti spolehnout i na jiný titul, než je souhlas?

Právním základem zpracování může být kromě souhlasu veřejný zájem (čl. 6 odst. 1 písm. e) GDPR) nebo oprávněný zájem správce nebo třetích osob (čl. 6 odst. 1 písm. f) GDPR). Veřejný zájem musí být založen na právu EU nebo na právu členského státu. Veřejný zájem je protipólem soukromých a komerčních zájmů.[7] Výzkum na základě veřejného zájmu bude splňovat veřejná výzkumná instituce nebo vysoká škola.[8] Podle § 2 odst. 1 zákona č. 341/2005 Sb., o veřejných výzkumných institucích, je veřejná výzkumná instituce právnickou osobou, jejímž hlavním předmětem činnosti je výzkum, včetně zajišťování infrastruktury výzkumu, vymezený zákonem o podpoře výzkumu, vývoje a inovací. Veřejná výzkumná instituce svou hlavní činností zajišťuje výzkum podporovaný zejména z veřejných prostředků v souladu s podmínkami pro poskytování veřejné podpory stanovenými právem Evropských společenství. Dalšími institucemi, které mají povinnost provádět vědu a výzkum, jsou vysoké školy. Podle § 1 písm. a) zákona č. 111/1998 Sb., o vysokých školách, vysoké školy uchovávají a rozhojňují dosažené poznání a podle svého typu a zaměření pěstují činnost vědeckou, výzkumnou, vývojovou a inovační, uměleckou nebo další tvůrčí činnost.

Pokud správce nedisponuje souhlasem subjektů údajů se zpracováním pro účely výzkumu ani se nemůže opřít o veřejný zájem, lze za určitých podmínek zpracovávat osobní údaje pro tento účel na podkladě oprávněného zájmu (čl. 6 odst. 1 písm. f) GDPR). Výzkum jako oprávněný zájem je zmíněn ve stanovisku WP 29 k tomuto pojmu.[9] Správce je povinen provést balanční test mezi oprávněným zájmem na zpracování a zájmy a právy subjektů údajů. Správce musí také zhodnotit, zda subjekt údajů mohl zpracování pro tento účel důvodně očekávat. Balanční test a test slučitelnosti účelů nelze zaměňovat. Zatímco test slučitelnosti účelů zkoumá vztah mezi původním a novým účelem zpracování, balanční test poměřuje oprávněný zájem správce a práva subjektů údajů. I pokud výsledek testu slučitelnosti účelů dopadne ve prospěch zpracování pro účely výzkumu, neprojde zpracování balančním testem, protože v konkrétním případě práva subjektů údajů převáží nad oprávněnými zájmy správce. V případě, že je zpracování osobních údajů prováděno z titulu oprávněného zájmu, má subjekt údajů právo vznést námitku proti zpracování (čl. 21 odst. 6 GDPR).

Souhlas s budoucím výzkumem

Souhlas pro konkrétní výzkumný projekt nebo záměr zpravidla nebude činit větší problémy. Správce nebude mít větších obtíží splnit všechny požadavky, které GDPR na souhlas klade. Jak by měl ale souhlas vypadat, pokud bude správce vědět, že v budoucnu bude pravděpodobně osobní údaje potřebovat ještě pro jiné projekty, které nemůže v okamžiku udělení souhlasu specifikovat? Bod 33 odůvodnění výslovně stanoví, že subjektům údajů by proto mělo být umožněno, aby udělily svůj souhlas ohledně určitých oblastí vědeckého výzkumu v souladu s uznávanými etickými normami pro vědecký výzkum. Subjekty údajů by měly mít možnost udělit svůj souhlas pouze pro některé oblasti výzkumu nebo části výzkumných projektů v rozsahu přípustném pro zamýšlený účel. Správce by měl konkrétně vymezit oblast výzkumu nebo část výzkumu a před udělením souhlasu subjekt údajů o tomto vymezení informovat.

Subjekt údajů by tedy měl mít možnost udělit jeden souhlas pro konkrétní projekt a druhý souhlas pro další projekty v určité oblasti, které se budou řídit etickými pravidly. Subjekt údajů může sice svůj souhlas kdykoliv odvolat, ale ani v takém případě není dotčena zákonnost zpracování osobních údajů před jeho odvoláním. Subjekt údajů může uplatit právo na výmaz. Tomuto právu však nemusí správce zpracovávající osobní údaje pro účely výzkumu vyhovět, pokud by bylo pravděpodobné, že by výmaz znemožnil nebo vážně ohrozil splnění cílů zpracovávání, tedy ohrožení pravdivosti a správnosti výsledků výzkumu.

Eva Fialová
Autorka je právnička se specializací na ochranu osobních údajů a právo ICT. Působí v advokátní kanceláři GHS Legal.

6) Uřičař, Miroslav; Rámiš, Vladan a kol. *Obecné nařízení o ochraně osobních údajů.* Praha: C.H.Beck, 2021, s. 352.
7) European Data Protection Supervisor. A Preliminary Opinion on data protection and scientific research, 2020, s. 23.
8) Polčák, Radim a kol. *Metodika aplikace GDPR na výzkumná data v prostředí vysokých škol v ČR.* Brno: Masarykova univerzita, 2018, s. 39.
9) Pracovní skupina podle článku 29. Stanovisko č. 6 /2014 k pojmu oprávněných zájmů správce údajů podle článku 7 směrnice 95/46/ES. s. 25. Dostupné z: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_cs.pdf

Veřejné opatrovnictví: Zastupitelé by se měli dozvědět pouze nezbytné informace

Když jeden orgán obce (starosta) sděluje osobní údaje týkající se výkonu veřejného opatrovnictví jinému orgánu obce (zastupitelstvu a jeho členům), nemusí to na první pohled vypadat jako porušení zákona. Neděje-li se tak za přítomnosti veřejnosti, zůstávají všechny tyto informace tzv. „pod jednou střechou" – zpracovává je jeden správce osobních údajů (obec). Zdánlivě neškodným předáním osobních údajů však může v určitých případech docházet k porušení právních předpisů. Proto je namístě připomenout obecné zásady poskytování informací mezi orgány územních samospráv, abychom si uvědomili, kdy je sdělování osobních údajů o opatrovanci přípustné a kdy nikoliv.

Základní zásady zpracování osobních údajů při výkonu veřejného opatrovnictví

Člověk omezený ve svéprávnosti, kterému soud ustanovil veřejného opatrovníka, neztrácí právo na ochranu svého soukromí a osobních údajů.[1)] Akceptujeme-li, že už samotné ustanovení veřejného opatrovníka nepochybně představuje podstatný zásah do soukromí opatrovaného, přináší výkon veřejného opatrovnictví v prvé řadě pro každého, kdo se této role ujme, závazek nastavit pravidla pro výkon veřejného opatrovnictví tak, aby respektovala vedle principů veřejného opatrovnictví coby podpůrného opatření[2)] právo opatrovance na ochranu před neoprávněným zasahováním do soukromého života, jakož i jeho právo před neoprávněným shromažďováním, zveřejňováním nebo jiným zneužíváním údajů o své osobě.[3)] Zjednodušeně to znamená nejprve posoudit, komu a co o opatrovanci může veřejný opatrovník sdělovat.

Opatrovník musí znát potřeby opatrované osoby

Aby opatrovník mohl řádně vykonávat svou funkci, musí znát potřeby opatrované osoby, její názory, přesvědčení, vyznání, poměry, ve kterých žije, i dřívější způsob života. Nezbytnou podmínkou řádného výkonu opatrovnictví tudíž je, aby byl opatrovník s opatrovancem v pravidelném kontaktu a srozumitelně s ním komunikoval o všech záležitostech, které se jej týkají, a aby uměl, třeba i za pomoci dalších osob podílejících se na péči o opatrovance, kvalifikovaně posoudit jeho potřeby. Právě takto se opatrovník seznamuje s osobními údaji opatrovaného a jeho nejbližšího okolí, tyto údaje dále systematicky shromažďuje (zpracovává[4)]).

Informace musí opatrovník zpracovávat přehledně a systematicky

Zvláště u veřejného opatrovníka, kde opatrovnictví jedné osoby mohou postupně či zároveň reálně vykonávat různí lidé a kde není výjimkou, že obec vykonává opatrovnictví nad větším množstvím osob, se z hlediska řádného výkonu opatrovnictví jeví jako nezbytné, aby opatrovník přehledně a systematicky zpracovával informace ohledně opatrovance (vedl dokumentaci), které v maximální možné míře vypovídají o osobě opatrovance a všech krocích, jež byly učiněny v souvislosti s výkonem opatrovnictví, a zahrnují údaje o hospodaření s finančními prostředky opatrovance i komunikaci s dalšími subjekty – rodinou, úřady, zařízením sociálních služeb, poskytovateli zdravotních služeb apod.[5)]

Osobním údajem je jakákoliv informace týkající se opatrovaného

Vyjdeme-li z definice pojmu „osobní údaj"[6)], je osobním údajem jakákoliv informace týkající se opatrovaného. Osobním údajem může být údaj o jeho zdravotním stavu, o podmínkách, v nichž žije, bydlení, ale i o jeho právních prohlášeních, názorech a přáních.

1) Srov. čl. 22 Úmluvy o právech osob se zdravotním postižením vyhlášené ve Sbírce mezinárodních smluv pod č. 10/2010 Sb. m. s., ve znění účinném od 28. října 2009.
2) Účelem opatrovnictví není v oblastech vyjmenovaných v rozsudku o omezení svéprávnosti nahrazovat rozhodování opatrovance a bez dalšího jednat namísto něj. Účelem opatrovnictví je naopak podporovat opatrovance v jeho samostatném rozhodování, je-li to možné, jednat v souladu s opatrovancovými rozhodnutími založenými na jeho názorech, přáních či na jeho přesvědčení nebo vyznání. Teprve není-li to možné, opatrovancova rozhodnutí v oblastech, v nichž je omezen ve svéprávnosti, korigovat s ohledem na jeho zájmy.
3) Srov. čl. 10 odst. 2 a 3 Listiny základních práv a svobod
4) Srov. čl. 4 bod 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 (dále také „Obecné nařízení o ochraně osobních údajů").
5) Srov. zpráva o šetření veřejného ochránce práv ze dne 7. 4. 2015, sp. zn. 548/2015/VOP, dostupná zde: https://eso.ochrance.cz/Nalezene/Edit/2902 včetně dalších doporučení veřejného ochránce práv k výkonu veřejného opatrovnictví dostupných v evidenci stanovisek ochránce (oblast práva 203.9 – výkon veřejného opatrovnictví).
6) Srov. čl. 4 bod 1) obecného nařízení o ochraně osobních údajů.

Správcem osobních údajů opatrovaného je obec

Správcem osobních údajů opatrovaného je obec. Ta musí při jakémkoliv zpracování osobních údajů (tedy jak uvnitř – orgány obce a mezi orgány obce, tak navenek – vůči veřejnosti) dbát na dodržování základních zásad zpracování osobních údajů. Z nich lze za nejvýznamnější v daném kontextu považovat tři – zásadu účelového omezení zpracování údajů,[7] zásadu integrity a důvěrnosti[8] a zásadu zákonnosti.[9]

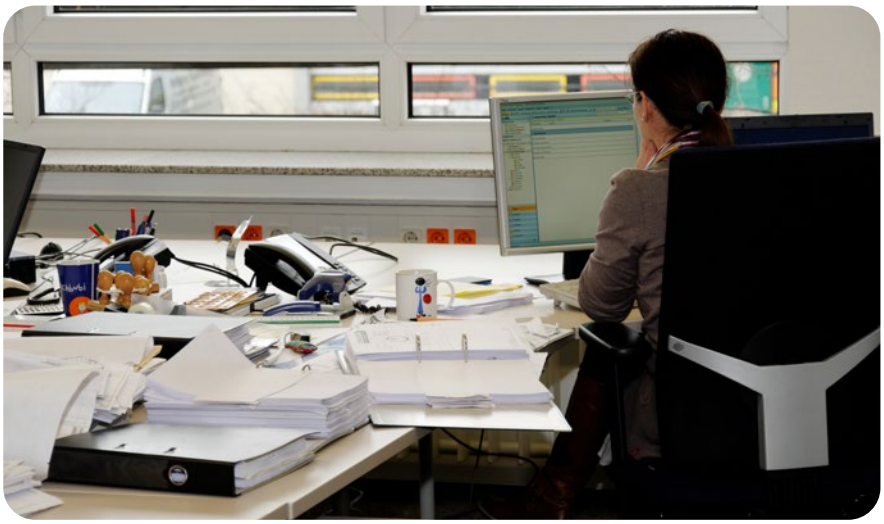
Zákonnost sdělování osobních údajů o opatrovaném mezi jednotlivými orgány obce (starostou a zastupitelstvem)

Stejně jako potřebuje obec zákonnou oporu pro to, aby mohla osobní údaje o konkrétní osobě shromažďovat a dále zpracovávat[10], musí existovat právní titul pro zpřístupňování (šíření) osobních údajů opatrovaného dalším osobám. Z výčtu právních titulů v článku 6 Obecného nařízení o ochraně osobních údajů lze usuzovat, že s osobními údaji opatrovance je osoba pověřená výkonem opatrovnictví oprávněna seznámit kohokoliv dalšího bez souhlasu opatrovance, jen pokud je to nezbytné pro splnění povinnosti, která je opatrovníkovi uložena právním předpisem.

Veřejný opatrovník má řadu povinností

Občanský zákoník[11] ukládá veřejnému opatrovníkovi řadu povinností, které musí plnit bez ohledu na to, v jakém rozsahu za opatrovaného z rozhodnutí soudu jedná. Zákonné povinnosti odráží základní standard výkonu opatrovnictví a odpovídají principům, jež by opatrovník měl dodržovat při jakékoliv činnosti opatrovníka. K těmto povinnostem náleží především povinnost:

- starat se o naplnění opatrovancových práv a chránit jeho zájmy;
- dbát názorů opatrovance, i když je projevil dříve, včetně jeho přesvědčení nebo vyznání, soustavně k nim přihlížet a zařizovat jeho záležitosti v souladu s nimi, a teprve není-li to možné, postupovat podle zájmů opatrovance;
- dbát, aby způsob opatrovancova života nebyl v rozporu s jeho schopnostmi a aby, nelze-li tomu rozumně odporovat, odpovídal i jeho zvláštním představám a přáním;
- vysvětlovat opatrovanci srozumitelně povahu a následky rozhodnutí, která opatrovník činí o opatrovancových záležitostech;
- udržovat s opatrovancem vhodným způsobem a v potřebném rozsahu pravidelné spojení;
- projevovat o opatrovance skutečný zájem, jakož i dbát o jeho zdravotní stav.[12]



Uvedený výčet povinností opatrovníka nezahrnuje žádnou povinnost, z níž by plynula nezbytnost sdělovat osobní údaje zastupitelstvu obce a jeho členům.

Opatrovnictví je výkonem přenesené působnosti obce

Výkon veřejného opatrovnictví je výkonem přenesené působnosti obce.[13] V obcích, kde není tajemník obecního úřadu, zabezpečuje výkon přenesené působnosti starosta obce.[14] Obec se může rozhodnout, zda výkonem veřejného opatrovnictví pověří konkrétního zaměstnance obecního úřadu, nebo funkci svěří jiné osobě (typicky starostovi obce, protože menší obce nemají potřebné personální kapacity, nebo jinému zastupiteli).

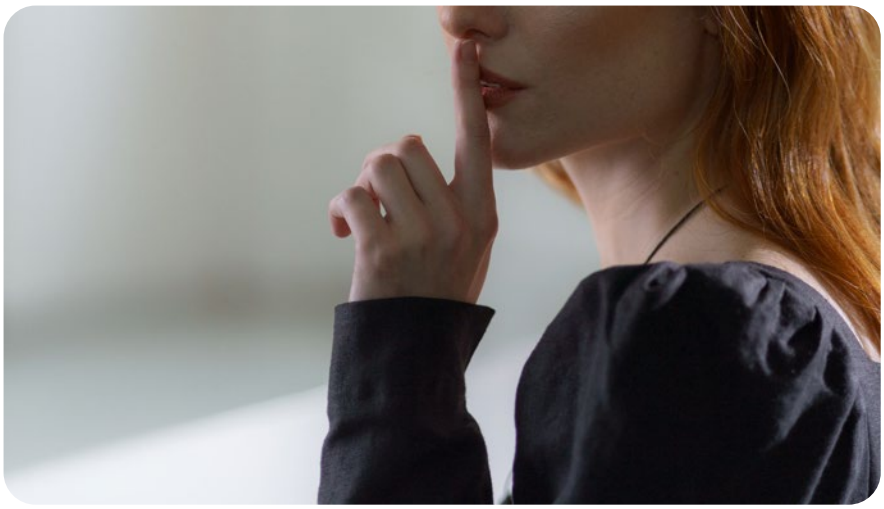
Když je veřejným opatrovníkem starosta

Ujme-li se výkonu veřejného opatrovnictví starosta obce, musí při svém dalším postupu důsledně rozlišovat mezi výkonem starostenské funkce (související se samostatnou působností obce a také demokratickou politickou soutěží) a výkonem veřejného opatrovnictví, na nějž obec pobírá příspěvek na výkon přenesené působnosti ze státního rozpočtu a jejíž výkon musí splňovat určité zákonné standardy.[15] Zatímco v případě starostenské funkce je přirozené, že starosta obce komunikuje se zastupitelstvem a veřejností (občany obce), u výkonu veřejného opatrovnictví jsou jeho přirozenými komunikačními partnery zejména **opatrovnický soud,** jemuž „skládá účty",[16] případně **opatrovnická rada,** je-li zřízena[17], a **krajský úřad**[18], který kontroluje výkon přenesené působnosti[19] a může v případě potřeby poskytnout obci potřebnou metodickou pomoc[20].

Toto rozdělení již naznačuje, komu a za jakých okolností je starosta obce oprávněn sdělovat osobní údaje související s výkonem veřejného opatrovnictví.

---

7) Čl. 5 odst. 1 písm. b) obecného nařízení o ochraně osobních údajů: „Osobní údaje musí být shromažďovány pro určité, výslovně vyjádřené a legitimní účely a nesmějí být dále zpracovávány způsobem, který je s těmito účely neslučitelný; (...)."
8) Čl. 5 odst. 1 písm. f) obecného nařízení o ochraně osobních údajů: „Osobní údaje musí být zpracovávány způsobem, který zajistí náležité zabezpečení osobních údajů, včetně jejich ochrany pomocí vhodných technických nebo organizačních opatření před neoprávněným či protiprávním zpracováním a před náhodnou ztrátou, zničením nebo poškozením."
9) Čl. 5 odst. 1 písm. a) ve spojení s čl. 6 obecného nařízení o ochraně osobních údajů.
10) V případě výkonu veřejného opatrovnictví je tímto „spouštěčem" rozhodnutí soudu, jímž soud jmenuje obec veřejným opatrovníkem.
11) Srov. § 457 a násl. zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů.
12) Základní informace o výkonu veřejného opatrovnictví přehledně zpracovala Kancelář veřejného ochránce práv v letáku Opatrovník, který je dostupný zde: https://www.ochrance.cz/letaky/opatrovnik/
13) Ustanovení § 149b odst. 3 zákona č. 128/2000 Sb., o obcích (obecní zřízení), ve znění pozdějších předpisů (dále „zákon o obcích"), případně také usnesení sp. zn. II. ÚS 995/07, ze dne 10. 7. 2007 (U 9/46 SbNU 519).
14) Srov. § 103 odst. 4 písm. f) zákona o obcích
15) Blíže Čtvrtlíková, V., Juríčková, L. a kol. Veřejné opatrovnictví. Praktický průvodce a rádce úředníka. Ministerstvo vnitra ČR: Praha, 2019. 69 s.
16) Opatrovnickému soudu opatrovník předkládá vyúčtování správy jmění opatrovance. Soud ale ověřuje i další péči opatrovníka, například zda svého opatrovance podporuje v činnostech, o které má opatrovanec zájem; zda dbá o jeho zdravotní stav; zda se zajímá o to, jak se opatrovanci vede v zaměstnání atd.
17) Srov. § 472 a násl. občanského zákoníku
18) V Praze kontroluje činnost městských částí při výkonu opatrovnictví Magistrát hlavního města Prahy.
19) Srov. § 129 zákona o obcích a § 67 odst. 1 písm. e) zákona č. 129/2000 Sb., o krajích (krajské zřízení), ve znění pozdějších předpisů (dále „zákon o krajích")
20) Srov. § 67 odst. 1 písm. c) zákona o krajích



Veřejné opatrovnictví s výkonem funkce zastupitele obce nesouvisí

Zastupitelé obce mají při výkonu své funkce právo požadovat od zaměstnanců obce zařazených do obecního úřadu, jakož i od zaměstnanců právnických osob, které obec založila nebo zřídila, informace ve věcech, které souvisejí s výkonem jejich funkce; informace musí být poskytnuta nejpozději do 30 dnů.[21)] S výkonem funkce zastupitele souvisí věci, které jsou zastupitelstvu jakožto orgánu obce vyhrazeny zákonem o obcích.[22)] Z výčtu tam uvedeného je zřejmé, že jde primárně o záležitosti spadající do tzv. samostatné působnosti obce. Výkon veřejného opatrovnictví jakožto výkon přenesené působnosti proto a priori s výkonem funkce zastupitele obce nesouvisí.

Parametr nezbytnosti a potřebnosti

Obzvlášť citlivě je proto třeba vyhodnotit, zda je naplněn **parametr nezbytnosti a potřebnosti** k tomu, aby bylo na místě prolomit soukromí osob dotčených poskytnutím konkrétní informace. K naplnění tohoto parametru nedojde zvláště v případech, kdy zastupitel nemá pravomoc rozhodovat o věci, jíž se informace (osobní údaje) týkají. V takovém případě postačí k tomu, aby mohl dohlížet na dění v obci, pokud je mu poskytnuta pouze anonymizovaná informace.

Když si to shrneme…

Optikou zmíněných požadavků na poskytování informací zastupitelům obce lze dospět k následujícím závěrům.

S informacemi, které se týkají výkonu veřejného opatrovnictví konkrétního člověka (včetně jeho osobních údajů), je starosta obce, případně jiná osoba pověřená výkonem veřejného opatrovnictví, oprávněna seznámit zastupitelstvo obce bez souhlasu opatrovaného, jen pokud je to nezbytné pro splnění povinnosti, která je opatrovníkovi uložena právním předpisem.

Pouze ze skutečnosti, že je opatrovníkem obec, která na základě hlasování zastupitelstva pověřila výkonem opatrovnictví starostu obce, nelze dovodit, že zastupitelstvo má právo na všechny osobní údaje opatrovaných, které starosta obce při výkonu funkce zpracovává. Není proto vhodné, aby starosta obce probíral se zastupiteli obce konkrétní situaci jednotlivých opatrovanců, radil se, jak má vyřídit jejich žádosti, např. o vydání občanského průkazu, o zajištění konkrétní služby, o přidělení kapesného apod. **Členové zastupitelstva by se od starosty obce měli dozvědět pouze obecné informace, které nenarušují soukromí opatrovanců.** Takovou informací může být například informace o tom, že starosta obce zpracoval a podal roční zprávu o činnosti opatrovnické funkce opatrovnickému soudu.

K sdělování osobních údajů souvisejících s výkonem veřejného opatrovnictví členům zastupitelstva by mělo docházet zcela výjimečně a v odůvodněných případech. Například nastane-li situace, kdy opatrovaný požádá, aby zastupitelstvo pověřilo výkonem funkce opatrovníka někoho jiného než starostu (jiného člena zastupitelstva či jiného zaměstnance obecního úřadu), protože ztratil důvěru vůči starostovi obce nebo důvěřuje více jinému zastupiteli, a ten s pověřením souhlasí. V takovém případě je ospravedlnitelné, aby starosta obce, který doposud roli veřejného opatrovníka zastával, informoval zastupitele, jenž tuto roli nově převezme, o situaci opatrovaného a sdělil mu související osobní údaje opatrovaného. Je dále legitimní, informuje-li o nastalé situaci zastupitelstvo, aby změnu ve výkonu veřejného opatrovnictví schválilo. Za této situace má zastupitelstvo právo znát i důvody vedoucí k navržené změně (osobní údaje opatrovaného). I v této souvislosti ale starosta obce pamatuje na dodržení již zmíněné zásady nezbytnosti a přiměřenosti a pečlivě uváží, v jakém rozsahu osobní údaje o opatrovném zastupitelům sdělí.

Veronika Gabrišová
Autorka pracuje v Kanceláři veřejného ochránce práv, je vedoucí odboru veřejného pořádku a místní správy, pověřenkyní pro ochranu osobních údajů a členkou rozkladové komise Úřadu pro ochranu osobních údajů.

21) Srov. § 82 písm. c) zákona o obcích
22) Srov. § 35 a dále také § 84, 85 a 102 zákona o obcích. Blíže také GABRIŠOVÁ, Veronika, ed. Informace. Brno: Kancelář veřejného ochránce práv, [2019]. Stanoviska (Kancelář veřejného ochránce práv). ISBN 978-80-7631-020-9.
23) Srov. rozsudek Městského soudu v Praze ze dne 11. 3. 2019, čj. 14 A 89/2017-47, www.nssoud.cz. Soud hodnotil situaci, kdy bylo zasaženo soukromí nezletilých dětí tím, že zastupitelé na zasedání zastupitelstva byli informováni o jménech útočníků a jménu oběti šikany, k níž došlo ve škole zřizované obcí. Městský soud v Praze dospěl k závěru, že převáží právo na soukromí nad právem zastupitelů, přestože mají za úkol sledovat zájmy obce, dohlížet na ně a být o této záležitosti informováni. Řešení záležitostí školy, jejímž zřizovatelem je obec, je vyhrazeno pouze radě obce a zastupitelé obce nemohou nikterak závazně o problému šikany na škole rozhodovat.

DPO PRO. Ročník II, číslo 3. Vychází každého 28. dne v měsíci v Praze. Cena ročního předplatného činí 1 990 Kč bez DPH. Vydávají SMS-služby s. r. o. se sídlem V Rovinách 40, 140 00 Praha 4-Podolí, IČ: 067 84 771. Adresa redakce: Národní 41, 110 00 Praha 1-Staré Město. Webové stránky: https://www.dpopro.cz. Minimální rozsah 12 stran A4. Evidenční číslo: MK ČR E 24123. ISSN 2695-1363. Šéfredaktorka: JUDr. et Mgr. Eva Janečková, eva.janeckova@sms-sluzby.cz. Redakční rada: JUDr. et Mgr. Eva Janečková, Ing. Mgr. Oldřich Kužílek, Ing. Michal Merta, MBA, MSc., LL.M., JUDr. Adam Furek. Jazyková redakce: Marie Šuláková. Předplatné: Magdalena Komárková, magdalena.komarkova@sms-sluzby.cz, tel.: +420 723 644 867. Grafické práce: Studio Matrix. Redakční uzávěrka: 25. 2. 2022.