ELEKTRONICKÝ ZPRAVODAJ PRO POVĚŘENCE

HLÍDACÍ PES PRO OSOBY ZODPOVĚDNÉ ZA GDPR | 3. ročník | číslo 4 | únor 2021

Jak a kdy zveřejnit kontakty na zaměstnance obce

Jaké údaje o zaměstnancích můžou, či dokonce musejí obce a další veřejné instituce zveřejňovat na svých webových stránkách? Lze zveřejnit soukromé číslo, životopis nebo údaj o platu zaměstnance? Kdy jde ještě o veřejný zájem a kdy už o zásah do soukromí?

Častým problémem veřejných institucí, zejména pak menších obcí, je otázka, **zda mohou, či dokonce musejí na svých webových stránkách zveřejňovat kontaktní údaje zaměstnanců**, a to i pokud někteří z nich fakticky nevstupují do kontaktu se širší veřejností. Typicky se může jednat například o zaměstnance IT oddělení. V tomto článku se pokusíme problematiku zveřejňování osobních údajů zaměstnanců veřejných institucí na webových stránkách osvětlit.

Právní základ

Pro určení, zda zaměstnanci správního orgánu či jiné veřejné instituce a jejich kontaktní údaje mohou být uvedeny na webových stránkách obce, je nezbytné **vymezit, které z právních předpisů jsou v tomto směru relevantní**.

Ústavním základem zveřejňování některých informací ze strany obcí a obecních úřadů, a to včetně kontaktů na vybrané zaměstnance, je čl. 17 odst. 5 Listiny základních práv a svobod, dle kterého: „*Státní orgány a orgány územní samosprávy jsou povinny přiměřeným způsobem poskytovat informace o své činnosti. Podmínky a provedení stanoví zákon.*“ Předmětný článek Listiny základních práv a svobod tak sice stanovuje, že **správní orgány a samosprávné celky musí zveřejňovat určité informace**, ale již neříká, jaké tyto informace mají být, a nechává toto na zákonném právním předpisu.

Tímto prováděcím zákonem je přitom zákon č. 106/1999 Sb., o svobodném přístupu k informacím (dále jen „InfoZ“), který v sobě obsahuje úpravu **zpřístupňování informací ze strany správních orgánů, samosprávných celků a dalších veřejných institucí** veřejnosti. V souvislosti s InfoZ pak nesmíme zapomenout ani na jeho podzákonný prováděcí předpis, jímž je vyhláška Ministerstva vnitra č. 515/2020 Sb., o struktuře informací zveřejňovaných o povinném subjektu a o osnově popisu úkonů vykonávaných v rámci agendy (dále jen „vyhláška“).

S ohledem na skutečnost, že se ovšem rovněž nacházíme v oblasti osobních údajů (neboť informace o úředních osobách a zaměstnancích

představují osobní údaje), **nesmíme zapomenout ani na předpisy týkající se právě ochrany osobních údajů**. Těmi jsou zejména nařízení Evropského parlamentu a Rady EU ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů (dále jen „nařízení"), které je přímo použitelným právním předpisem Evropské unie, a dále zákon č. 110/2019 Sb., o zpracování osobních údajů (dále jen „ZZOÚ"), jenž toto nařízení v rámci České republiky provádí.

Povinnost zveřejňovat informace

Dle § 2 odst. 1 InfoZ patří mezi povinné subjekty k poskytování informací ohledně své působnosti samozřejmě nejen správní orgány a územně samosprávné celky, tedy **obce a kraje, ale i jejich orgány a další veřejné instituce** (například státní podniky, státní fondy a podobně). Pod poskytováním informací dle InfoZ si ovšem nelze představit pouze pasivní poskytování informací ze strany povinného subjektu – tedy zveřejňování informací na základě žádosti podané fyzickou nebo právnickou osobou. Povinné subjekty naopak **musejí zveřejňovat některé specifické informace aktivně a bez podnětu** (žádosti). Tyto informace jsou pak obecně upraveny v § 5 InfoZ a v ustanovení § 5 odst. 1 písm. b) InfoZ, kde je mimo jiné stanovena i povinnost zveřejnění organizační struktury povinného subjektu.

Organizační struktura

Co všechno se pod pojmem organizační struktura skrývá? V prvé řadě se samozřejmě jedná o **zveřejnění formální struktury povinného subjektu**, a to včetně vztahů nadřízenosti a podřízenosti. Formální strukturou se rozumí zejména popis jednotlivých organizačních útvarů povinného subjektu, kterými mohou být například **oddělení či odbory konkrétního povinného subjektu**. Dále se ale pod organizační strukturou rozumí i osobnostní substrát daného povinného subjektu.

Dříve bylo oprávnění zpracovávat osobní údaje zaměstnanců na webových stránkách povinného subjektu uvedeno přímo v § 5 odst. 2 písm. f) zákona č. 101/2000 Sb., o ochraně osobních údajů (dále jen „ZOOÚ"): *„Bez tohoto souhlasu je (osobní údaje) může správce zpracovávat […], pokud poskytuje osobní údaje o veřejně činné osobě, funkcionáři či zaměstnanci veřejné správy, které vypovídají o jeho veřejné anebo úřední činnosti, o jeho funkčním nebo pracovním zařazení…"* ZOOÚ byl ovšem nahrazen výše zmíněným nařízením a ZZOÚ ani nařízení podobné ustanovení jako ZOOÚ již neobsahuje.

Výkladem je ovšem možné dovodit, že zveřejnění jména a kontaktu na konkrétního zaměstnance správního orgánu, samosprávného celku či veřejné instituce je nadále právními předpisy požadováno a toto zpracování je možné podřadit pod **titul zpracování osobních údajů nezbytných pro splnění úkolu prováděného ve veřejném zájmu** nebo při výkonu veřejné moci dle čl. 6 odst. 1 písm. e) nařízení. Alternativně by bylo ještě možné uvažovat o zpracování dle čl. 6 odst. 1 písm. c) nařízení, tedy o zpracování nezbytném pro splnění právní povinnosti, která se na správce osobních údajů vztahuje.

Nezveřejňujte na stránkách soukromá telefonní čísla či e-maily

Je vhodné ještě poznamenat, že velmi podobné ustanovení jako to v ZOOÚ v sobě obsahuje i ZZOÚ, a to ve svém § 43 odst. 3 písm. f). Toto ustanovení se ovšem nachází v hlavě IV, jež se týká ochrany osobních údajů při zajišťování obranných a bezpečnostních zájmů České republiky. Z uvedeného důvodu se tak toto ustanovení nedá použít v podobném rozsahu jako v ZOOÚ.

Jaké údaje a o kom lze zveřejnit?

Lze tedy shrnout, že osobní údaje o úředních osobách, které se vztahují k jejich veřejné nebo úřední činnosti, mohou nebo by spíše měly být zveřejněny na stránkách daného povinného subjektu. Otázkou ovšem je, **jaké osobní údaje se považují za vztahující se k veřejné nebo úřední činnosti** a k funkčnímu nebo pracovnímu zařazení.

Zaměstnanci a úředníci

Typicky se bude samozřejmě jednat o jména a příjmení dané osoby a označení její **funkce či pracovního místa** (například referent, rada…). Dále se může jednat o osobní údaje, jako jsou služební telefonní číslo nebo e-mail. Rovněž může jít o dosažený titul, jenž tímto způsobem vypovídá o odbornosti daného úředníka či zaměstnance k vykonávané působnosti.

Toto ostatně potvrdil i Nejvyšší správní soud ve svém rozsudku ze dne 25. 3. 2015, sp. zn. 8 As 12/2015, kde se ovšem jednalo o žádost o poskytnutí **informace o dosaženém vzdělání a odborné praxi konkrétní úřední osoby**. Na druhou stranu ale Nejvyšší správní soud ve stejném rozsudku dovodil, že informace nesmí být poskytnuta na základě šikanózní žádosti, která má za cíl konkrétní osobu poškodit. V tomto směru je tak nutné při zveřejňování informací o dosaženém vzdělání a odborné praxi postupovat relativně opatrně a zveřejňovat tyto informace spíše jen u osob na vedoucích pozicích, případně se souhlasem dotčených zaměstnanců či úředníků.

Rozhodně by se na webových stránkách povinných osob **neměly objevovat soukromá telefonní čísla či e-mailové adresy**, pokud k tomu

není povinná osoba oprávněna na základě výslovného souhlasu ze strany subjektu údajů (tedy samotného úředníka). Rovněž fotografie úředníků, a to i vedoucích, by měly být zveřejňovány pouze s jejich souhlasem.

Dalším typickým osobním údajem, či spíše dokumentem, jenž obsahuje velké množství osobních údajů a někdy se na webových stránkách správních orgánů či jiných veřejných institucí objevuje, je životopis. I ten by měl být na webových stánkách povinného subjektu **publikován pouze se souhlasem dotčené osoby**, neboť bude zpravidla obsahovat poměrně velké množství informací včetně takových, které se vykonávané veřejné nebo úřední činnosti vůbec netýkají.

Poměrně zajímavě se k okruhu zveřejňovaných informací vyjádřil Nejvyšší správní soud ve svém rozsudku ze dne 27. 5. 2011, sp. zn. 5 As 57/2010, kde poukázal na to, že mezi údaje, které nevypovídají o veřejné a úřední činnosti ani o funkčním či pracovním zařazení, jsou **informace o platu či odměně úřední osoby** (bez ohledu na to nicméně platí, že informace o odměně a platu zaměstnance, jenž je příjemcem veřejných prostředků podle § 8b odst. 1 InfoZ, má povinný subjekt povinnost poskytnout v rozsahu vymezeném § 8b odst. 3 InfoZ). Na druhou stranu Nejvyšší správní soud dovozuje, že mezi údaje vypovídající o pracovním nebo funkčním zařazení patří i informace o tom, **do kterého útvaru je zaměstnanec nebo úředník zařazen, kdo je jeho nadřízeným a kdo podřízeným**. Tomu ostatně odpovídá i výše popsané zveřejnění formální struktury úřadu či veřejné instituce.

Jak ale dovozuje i komentářová literatura, možnost poskytnutí informace (osobního údaje) automaticky neznamená, že tento údaj může být zároveň i zveřejněn, neboť **zveřejnění určitého údaje má poněkud širší rozsah než pouze jeho poskytnutí** konkrétnímu žadateli. Z tohoto důvodu by měly být zveřejňovány výše uvedené osobní údaje (a to se týká i údajů jako e-mail či přímý telefonní kontakt) **pouze u zaměstnanců, u kterých je veřejný zájem na tom, aby tyto informace byly dostupné širokému okruhu osob**. Jedná se tak zejména o pracovníky, kteří skutečně přicházejí do kontaktu s osobami „z vnějšku" veřejné instituce, s nimiž budou muset komunikovat. V případě oddělení, které do přímého kontaktu se žadateli nebo dalšími osobami nepřicházejí (typicky IT oddělení či úklidové služby), je tak namístě doporučit spíše zveřejnění kontaktu například pouze na vedoucího oddělení či sekretariát.

Další osoby

Kromě úředníků a zaměstnanců ovšem ve veřejných institucích pracují i další osoby, které mohou také působit ve veřejné funkci. Jedná se přitom nejen o **členy zastupitelstev samosprávných celků, ale třeba i o členy pracovních skupin**, jež jsou rovněž zřizovány samosprávnými celky. V daném případě by pro zveřejňování údajů o členech těchto skupin měla platit podobná pravidla jako u zaměstnanců a úředníků. Zejména by tak měly být kontaktní údaje zveřejňovány pouze v případech, kdy se jedná o **služební kontaktní údaje spojené s jejich veřejnou funkcí nebo činností**. V případě pracovních skupin by pak mělo dojít i ke zvážení, čeho se daná pracovní skupina týká, zda jde například o posouzení projektu, který zásadním způsobem ovlivní budoucí vzhled obce, nebo zda jde pouze o mimoškolní vzdělávání. Je tedy nutné posoudit váhu veřejného zájmu na zveřejnění osobních údajů v porovnání se zájmem na ochranu osobních údajů.

Závěr

Lze tedy shrnout, že osobní údaje týkající se pracovního zařazení zaměstnance veřejné instituce a jeho **služební kontaktní údaje lze ve většině případů veřejnosti nejen sdělit, ale i zveřejnit**. Veřejný zájem na zveřejnění těchto osobních údajů přitom zpravidla narůstá s tím, jak je daná osoba zařazena v hierarchickém žebříčku dané veřejné instituce, a to i s ohledem na její případný kontakt s osobami mimo tuto instituci.

Na druhou stranu není většinou nezbytné zveřejňovat kontaktní údaje na zaměstnance, kteří běžně do styku s veřejností nepřicházejí. Rovněž by se mělo jednat o **zveřejnění pouze těch údajů, které mají souvislost s danou institucí** – tedy skutečně pouze e-mailu nebo telefonního čísla přiděleného institucí zaměstnanci. Další osobní údaje pak mohou být zveřejněny pouze s jeho výslovným souhlasem a při jeho odvolání musejí být zase následně odstraněny.

▪▪▪

Mgr. Adam Novák
Advokátní kancelář Rada & Partner

Vymáhání GDPR – jak jsme na tom v ČR?

Věděli jste, že Úřad pro ochranu osobních údajů obdrží v průměru 7,5 stížností každý den? Počet stížností i výše pokut přitom roste v celé Evropě. Jak si ve vymáhání GDPR stojíme v porovnání s ostatními členskými státy? A za co byly uděleny tři nejvyšší pokuty v minulém roce?

Dne 28. 1. jsme oslavili Den ochrany osobních údajů. Svátek byl na tento den stanoven z důvodu přijetí Úmluvy o ochraně osob se zřetelem na automatizované zpracování osobních dat, což se stalo roku 1981. Za oněch 40 let ušla ochrana osobních údajů poměrně zásadní cestu, která změnila a stále mění fungování trhu – **velcí technologičtí giganti jsou nuceni fakticky upravovat parametry svých služeb** (ačkoliv je to pro ně nevýhodné), stěhují svá datacentra do jiných zemí (ve snaze vyhnout se odpovědnosti) či **vyhrožují, že své služby pro celou Evropu jednoduše vypnou** (viz například prohlášení Facebooku).

Velkou zásluhu na tom má samozřejmě i přijetí GDPR, které minimálně v rámci naší české kotliny zvýšilo o této problematice povědomí. Dopady GDPR na podnikání jsou tak všudypřítomné, a to hlavně z důvodu vysokých sankcí. Využijme proto tohoto jubilea a pojďme si krátce zrekapitulovat, **jak jsme na tom v rámci vymáhání sankcí a jak GDPR zasahuje do fungování ekosystémů společností** fungujících na území EU.

Základní statistiky

Právě v lednu tohoto roku vydala společnost DLA Piper, respektive její tým, který se zabývá kybernetickou bezpečností a ochranou osobních údajů, **zprávu týkající se uložených pokut podle GDPR**. V rámci této zprávy se zaměřili na statistiky ukládání pokut, počtu stížností a dalších zajímavých informací, a to zejména za období od 28. 1. 2020 do 27. 1. 2021.

Co se týče statistiky stížností a podnětů, oproti předchozímu období, kdy takových oznámení bylo v průměru 278 denně, **došlo v období minulého roku k 19% nárůstu** (na 331 denně). To skutečně není málo. S ohledem na čím dál **častější přechod procesů a podnikatelů do online prostředí**, mimo jiné z důvodu současné pandemické situace, lze předpokládat, že bude přibývat i počet oznámení.

Ohromný je také objem sankcí, které za uplynulý rok dozorové orgány udělily. V součtu totiž celková suma

> **V minulém roce udělily dozorové úřady pokuty za 4 miliardy korun**

udělených (nikoliv však vždy pravomocných a konečných) pokut činila celkem **158,5 milionů eur, tedy něco okolo čtyř miliard korun**. Přitom v předchozím období, tedy od účinnosti GDPR, dozorové orgány udělily něco okolo 114 milionů eur, v celkové výši tedy od účinnosti GDPR něco okolo 272 milionů eur (v přepočtu cca sedm miliard korun).

Český podíl

Určitě si kladete otázku, jak se na částce sedmi miliard korun podílel český Úřad pro ochranu osobních údajů. Bez velkého napínání můžeme rovnou uvést, že **ÚOOÚ od účinnosti GDPR rozdal pokuty v celkové výši 2 889 000 korun**. Ze sedmi miliard, připadajících na všechny členské státy, to skutečně netvoří významný poměr, neboť **Česká republika se podílí na sankcích cca v 0,04 %**.

Dle informací serveru o českém internetu Lupa.cz, který informace ze zprávy DLA Piper ověřoval, **ÚOOÚ obdržel od účinnosti GDPR celkem 7 179 podnětů a stížností**. Ze statistik tak vyplývá, že dostane okolo 7,5 stížností denně. Kolik z těchto podnětů skutečně vedlo k zahájení kontrol, se můžeme pouze domnívat, neboť z výše uvedeného článku nevyplývá, zda údaj o počtu kontrol zahrnuje i kontroly zahájené podle kontrolního plánu, či nikoliv. Tak či tak ÚOOÚ poskytl Lupě vyjádření, že za **účinnosti GDPR zahájil celkem 144 kontrol**, což i v případě, že by se jednalo o kontroly zahájené jako důsledek stížnosti, není mnoho.

Rekordmani

Jistě se pro zajímavost sluší zmínit **tři rekordmany, co se uložených pokut týče**, které DLA Piper v evropském kontextu vyzdvihla.

Porušování GDPR se určitě nevyplácí ve Francii: tamní dozorový or-

gán uložil v lednu roku 2019 společnosti Google **pokutu ve výši 50 milionů eur, a to za porušení zásady transparentnosti** ve vztahu k personalizované reklamě, stejně tak jako porušení ustanovení týkajícího se právního základu. O tomto případu jsme informovali v předchozích číslech Zpravodaje, více se dočtete například **zde**.

O něco menší pokuta byla udělena dozorovým orgánem v Hamburku, a to **ve výši 35,26 milionů eur společnosti H&M**. Německo se tak v celkovém žebříčku zařadilo na druhé místo. Důvod měl spočívat v **neoprávněném uchovávání a užívání osobních údajů zaměstnanců**, respektive údajů o jejich soukromém životě. Například pokud se zaměstnanec vrátil z „nemocenské" (respektive ze sick day), jeho nadřízený s ním vedl takzvaný „welcome back talk" (česky „uvítací pohovor"), v rámci něhož s ním **probral příznaky nemoci, diagnózu a podobně**. Tyto informace spolu s dalšími údaji z jiných rozhovorů (včetně informace o soukromém a rodinném životě nebo o náboženském přesvědčení) byly následně **sdíleny až s padesáti manažery celé společnosti.** Data měla být sbírána už od roku 2014, přičemž nebýt technické chyby, jež v roce 2019 zapříčinila, že byla najednou zpřístupněna celé společnosti, by se na to možná ani nepřišlo. Bližší informace najdete v tiskové zprávě **EDPB**.

Třetí příčku obsadila Itálie. Tamní dozorový úřad **udělil telekomunikačnímu operátorovi TIM SpA pokutu ve výši 27,8 milionů eur** (viz tisková zpráva **EDPB**). Dozorový orgán obdržel v minulosti **stovky stížností na nevyžádané marketingové hovory**, což odstartovalo kontrolu ve spolupráci se specializovaným útvarem policie. Došlo tak k odhalování dalších a dalších porušení, z nichž výše uvedená sankce vyplynula. Dozorový orgán odhalil přehršel porušení od vynucování souhlasu (respektive nerespektování neposkytnutí souhlasu) v rámci marketingových aktivit přes **chybné informování a zajištění zabezpečení po špatné vedení seznamu osob, které si nepřejí být kontaktovány**. Italský dozorový úřad mimo výše uvedenou sankci uložil společnosti TIM celkem dvacet opravných opatření, což svědčí o závažnosti jednotlivých porušení nebo minimálně o jejich počtu.

ÚOOÚ už dostal více než 7 000 stížností

Období bez pokut skončilo

Čísla nelžou a poukazují na to, že **počet stížností, počet uložených pokut i jejich objem roste**. S konečnou platností tak můžeme říct, že „zkušební období", kdy se dozorové úřady snažily spíše pomáhat s implementací než ukládat tvrdé sankce, pravděpodobně skončilo.

Jak vyplývá z pokuty udělené v Hamburku (a také z předešlých článků ve Zpravodaji, kde jsme upozorňovali na kontroly ÚOOÚ v rámci zaměstnanecké agendy), již také spíše **neplatí, že důležité je mít vyřešenou ochranu osobních údajů „navenek"**, protože se jedná o nejrizikovější agendu, přičemž otázky zpracování osobních údajů našich zaměstnanců můžeme prozatím nechat na jindy. Ke čtyřicátinám Dne ochrany osobních údajů si tak můžeme se slzami rozbalit dárek ve formě utvrzení se, že „prázdninové období" bez pokut skončilo a ochranu osobních údajů musíme brát skutečně vážně.

▪▪▪

Mgr. Josef Bátrla
advokát v oblasti IT
www.josefbatrla.cz

ÚOOÚ prošetřuje předávání osobních údajů o lidech v karanténě policii

Úřad pro ochranu osobních údajů prošetřuje předávání strukturovaných dat o osobách, kterým byla nařízena karanténa, Policii ČR. Podle informací Deníku N předávaly policii data všechny krajské hygienické stanice a Česká správa sociálního zabezpečení. Mělo se jednat jak o informace o nařízení karantény, tak o další osobní údaje – například datum narození, adresu trvalého bydliště a místo současného pobytu. Za 11 měsíců epidemie v Česku šlo přitom do karantény kvůli koronaviru více než 421 tisíc lidí, z toho téměř pětina letos v lednu. Policie zatím neuvedla, jakým způsobem s daty nakládala. K věci se vyjádřil předseda ÚOOÚ Jiří Kaucký: *„Státní orgány musí zacházet s osobními údaji občanů vždy přesně v intencích zákona a zákonným způsobem, účelně a přiměřeně."* V současné době Úřad zjišťuje, jak k předávání údajů docházelo, a zkoumá okolnosti, za nichž Policie ČR údaje dále uchovávala a používala.

Zdroj: ČTK

Klikněte a stáhněte si checklist

CHECKLIST: Jak na reaudit krok za krokem

1. KROK: KONTROLA ÚPLNOSTI	
Ověřte, zda jsou vaše záznamy o činnostech zpracování úplné a zda nepřibyla žádná nová operace zpracování, zpracovatel či důvod výmazu, který by nebyl zanesen ve vaší dokumentaci.	☐
Můžete si například vyžádat seznam uzavřených smluv s dodavateli za uplynulý rok. Díky tomu zjistíte, jaké nové služby byly poptány a proč, to vás může navést na stopu novým či jinak pojatým operacím zpracování.	☐
Vaše zjištění poznamenejte do nových záznamů o činnostech zpracování v režimu sledování změn.	☐
2. KROK: PRÁVNÍ AUDIT	
Ověřte, zda splňujete všechny podmínky GDPR k daným operacím.	☐
Vytvořte si checklist přímo pro svou organizaci a ve vztahu k jednotlivým operacím zpracování zkontrolujte, že:	☐
• o všech účelech byly subjekty údajů informovány;	☐
• se všemi zpracovateli je uzavřena zpracovatelská smlouva;	☐
• kde je oprávněný zájem, disponujete posouzením takového oprávněného zájmu a podobně.	☐
Všechna zjištěná porušení GDPR zaznamenejte do pracovní verze auditní zprávy.	☐
Posuďte, zda je vaše dokumentace právně úplná a bezvadná, na základě aktuálních vodítek, pokynů, stanovisek, rozhodovací praxe, a podobně.	☐
Zkontrolujte, že máte správně nastaveny účely, právní tituly, že zpracovatelské smlouvy obsahují, co mají.	☐
3. KROK – BEZPEČNOSTNÍ AUDIT	
Ověřte, zda jsou stanovená bezpečnostní opatření přiléhavá a také jestli jsou dodržována.	☐
V této fázi může být přínosné zapojit do ověření třetí nestrannou osobu, která v tomto oboru podniká.	☐
4. KROK - MÍRA RIZIK A JEJICH ODSTRANĚNÍ	
Ke každému zjištění přidejte odůvodnění a své hodnocení, o jak velké riziko se jedná.	☐
Připojte svůj návrh k odstranění rizika.	☐

Rezervační systémy úřadů často porušují GDPR

Objednávat se na úřady prostřednictvím online rezervačních systémů je ve státní správě a samosprávě stále častější. Ochrana osobních údajů jde přitom však často stranou! Jakých chyb se veřejné instituce nejčastěji dopouštějí?

Úřad pro ochranu osobních údajů vykonal v minulém roce několik šetření, která se zaměřovala na rezervační systémy provozované správci osobních údajů z oblasti státní správy a samosprávy. Na **základě poznatků z provedených šetření vydal Úřad koncem loňského roku doporučení**, v němž upozornil veřejné instituce na to, že musí při nabízení služeb klientům (kteří jsou v postavení subjektů údajů) **vysvětlit, k čemu potřebují jejich konkrétní osobní údaje** a proč je zpracovávají předmětným způsobem. Veřejné instituce zároveň musí být schopny popsat a transparentně a srozumitelně **odůvodnit, proč si vybraly ke zpracování osobních údajů soukromé dodavatele** (zpracovatele), a také musí zajistit a průběžně sledovat ochranu osobních údajů v systémech těchto externích dodavatelů (zpracovatelů).

Rezervační systémy

Řada úřadů v současné době **využívá pro objednávání klientů různé druhy online rezervačních systémů**. Klienti, kteří jsou v postavení subjektů údajů, se pomocí těchto rezervačních systémů mohou objednat na konkrétní den a čas a vyřídit všechny potřebné záležitosti (například podat žádost o nový občanský nebo řidičský průkaz, o povolení k dlouhodobému pobytu a podobně). Proces **objednávání probíhá obvykle s využitím e-mailo-**

vé adresy subjektu údajů, jejímž prostřednictvím se rezervace termínu potvrdí a subjekt údajů získá PIN, který následně zadá do vyvolávacího zařízení v budově předmětného úřadu.

Rezervační systémy shromažďují nadbytečné údaje

Jaké chyby ÚOOÚ odhalil?

Úřad pro ochranu osobních údajů zjistil během svých šetření rezervačních systémů provozovaných správci osobních údajů z oblasti státní správy a samosprávy, včetně řady obcí, že **nejčastěji dochází k porušení zásady transparentnosti** (čl. 5 odst. 1 písm. a) GDPR), **zásady účelového omezení údajů** (čl. 5 odst. 1 písm. b) GDPR) a **minimalizace údajů** (čl. 5 odst. 1 písm. c) GDPR).

Úřad se konkrétně během svých šetření rezervačních systémů setkal nejčastěji s následujícími pochybeními:

- jsou **shromažďovány nadbytečné osobní údaje**, které nejsou pro účely rezervace termínu nezbytné (příkladem mohou být situace, kdy jsou povinně vyžadovány další kontaktní osobní údaje, jako je třeba telefonní číslo, a nadto není subjekt údajů informován o účelu zpracování tohoto osobního údaje);
- subjekt údajů **není transparentně a srozumitelně informován o zpracování osobních údajů**, zejména není upozorněn na zpracování osobních údajů soukromým zpracovatelem;
- subjekt údajů je při přesměrování na soukromý web **nesprávně, neúplně nebo chybně informován** o důvodu, proč se tak děje;
- **nejsou plněny podmínky vyjádření souhlasu subjektu údajů**, kdy zejména subjekt údajů není před udělením souhlasu informován o právu svůj souhlas kdykoliv odvolat;
- získávaný **souhlas subjektu údajů není možné považovat za souhlas „informovaný“**, tedy není možné říct, že jej subjekt údajů udělil po řádném poučení o zpracování osobních údajů od správce.

Doporučení Úřadu pro ochranu osobních údajů je dostupné z jeho webových stránek **zde**.

JUDr. Andrej Lobotka, Ph.D.
www.smart-law.cz

Poradna

Nájemníci bytů v domě vlastněném městem mají v poslední době problém s opakovanými krádežemi kol a podobně. I když tuší, kdo za tím je, a obrátili se na policii, nikoho se zatím nepodařilo prokazatelně obvinit. Proto se obrátili na majetkový odbor s dotazem, zda by mohli se souhlasem města ve společných prostorách, kde ke krádežím dochází, nainstalovat kameru za účelem ochrany svého majetku. Je to možné? Případně za jakých podmínek? Jak správně postupovat? Domnívám se, že město by nebylo správcem ani zpracovatelem osobních údajů, pokud by k instalaci a provozování kamery pouze dalo souhlas. Nájemníci by se asi museli dohodnout, kdo z nich na sebe vezme roli provozovatele kamery a správce osobních údajů, anebo se za tímto účelem nějakou formou sdružit.

Co se týče provozování kamerového systému, Úřad pro ochranu osobních údajů k němu v minulosti vydal stanovisko, jež po účinnosti GDPR aktualizoval a které se touto otázkou široce zabývá. Co se týče samotného užití kamerového systému, klíčové je, co myslíte „prostorami, kde ke krádežím dochází“. V obecné rovině totiž je nutno kamerový systém nastavit tak, aby byl způsobilý splnit svůj účel (tedy ochránit majetek či zdraví osob), ale zároveň tak, aby nepřiměřeně nezasahoval do práva na soukromí některých osob. Zjednodušeně řečeno, pokud by kamerový systém byl namířen na dveře nájemníků a sledoval tak jejich příchod a odchod, pravděpodobně by bylo nepřiměřeně zasaženo do jejich práv na soukromí. S tím totiž souvisí i právní titul, na základě kterého by celá operace zpracování osobních údajů měla probíhat, neboť v úvahu přichází prakticky jen nezbytnost pro splnění oprávněných zájmů správce či třetích osob. Takový zájem pak musí mít s přihlédnutím k okolnostem přednost před právy subjektů údajů, jinak takové osobní údaje ani nelze zpracovávat. Co se pak týče ostatních podmínek, jako je doba zpracování a související otázky, doporučuji nahlédnout do zmíněného stanoviska.

Poslední bod, nejproblematičtější, je správcovství. Je totiž otázkou, zda v případě, kdy je bytový dům vlastněn městem, přičemž město jako vlastník má již z principu (řádného hospodáře) zájem na tom, aby život a majetek nájemníků byl chráněn, může být správcem osobních údajů někdo jiný, popřípadě zda by analogicky takové správcovství městu nepřipadlo stejně jako v případě přičitatelnosti zpracování osobních údajů zaměstnancem zaměstnavateli. Dle aktuálního právního názoru už jen ze samotného faktu, že pro instalaci potřebujete souhlas města, je právě město (respektive příslušný orgán) v pozici správce, proto doporučuji obrátit se s dotazem na DPO města a zjistit, jak se na danou problematiku tváří oni. Je totiž dost možné, že by pověřenec neakceptoval řešení, kdy de iure by správcem mělo být město, ale to by se vzdalo své odpovědnosti a přesunulo ji na jednoho z nájemníků (který nota bene může kdykoliv podat výpověď).

Nevíte si s něčím rady? Pošlete nám svůj dotaz a my vám zprostředkujeme odpověď! Dotazy pokládejte e-mailem na:
zpravodaj.poverenec@forum-media.cz

V příštím čísle Zpravodaje se dozvíte:
- **Kontroly ÚOOÚ za druhé pololetí 2020**
- **Nová vodítka k rozpoznávání obličejů**

Elektronický zpravodaj pro pověřence | Vydavatel: Nakladatelství FORUM, s. r. o. | Adresa redakce: Střelničná 1861/8a, 182 00 Praha 8 | Šéfredaktorka: Mgr. Anna Zavadilová | Editorka: Anna Pěkná | Zákaznický servis: Petra Pokojová, office@forum-media.cz, tel.: +420 251 115 576, fax: +420 251 512 422 Jazyková redakce: Bc. Vendula Pazderová | Fotografie: www.bigstockphoto.com | Zlom časopisu: Renata Brtnická | Roční předplatné: 2 490 Kč bez DPH Objednávka předplatného: office@forum-media.cz, fax: +420 251 512 422, informace o předplatném: +420 251 115 576 | Redakční uzávěrka: 11. 2. 2021 Elektronický zpravodaj vychází jako čtrnáctideník, celobarevný, 8 stran A4, ISSN 2571-1504.