KONTROLY ÚOOÚ VE STÁTNÍ SPRÁVĚ A OBCÍCH
POKUTA 6 MILIONŮ EUR PRO BANKU
POVINNÉ TESTOVÁNÍ ZAMĚSTNANCŮ VS. GDPR
PORADNA: OTÁZKY K TESTOVÁNÍ NA COVID-19

ELEKTRONICKÝ ZPRAVODAJ PRO POVĚŘENCE

HLÍDACÍ PES PRO OSOBY ZODPOVĚDNÉ ZA GDPR | 3. ročník | číslo 6 | březen 2021

Kontroly ÚOOÚ ve státní správě a obcích

Co odhalily kontroly Úřadu pro ochranu osobních údajů v oblasti státní správy a obcí? Úřad si posvítil na rezervační i kamerové systémy. V čem obce nejčastěji chybují?

V předchozím čísle jsme rozebrali poznatky z kontrolní činnosti ÚOOÚ za druhé pololetí roku 2020 v oblasti poskytování finančních služeb a pojišťovnictví a narazili jsme na některé problematické body týkající se zpracování osobních údajů zejména v rámci biometrie. V tomto článku se podíváme na dvě další oblasti – **IT technologie a zpracování osobních údajů v rámci obcí a státní správy**.

IT technologie

V rámci této oblasti se ÚOOÚ věnoval cookies a kamerovému systému. O **zpracování osobních údajů při používání cookies** jsme informovali již v předchozích číslech, kde jsme rozebírali jednotlivé protokoly z provedených kontrol a leckdy došli k poměrně zajímavým závěrům (jako jsou nevydané tiskové zprávy o zrušení návrhu doporučení k používání cookies a podobně).

Co se druhé oblasti týče, v rámci kontrolního plánu pro rok 2020 si ÚOOÚ stanovil úkol zkontrolovat **provozování kamerového systému na fotbalovém stadionu**. Kontrolovanou

ÚOOÚ kontroluje i orgány státní správy, přestože jim nelze udělit pokutu

osobou byl prvoligový fotbalový klub, který za účely stanovenými jako *„ochrana majetku správce a ochrana života a zdraví osob pohybujících se ve sledovaném prostoru pomocí kamerového systému, určení, výkon nebo obhajoba právních nároků správce, předcházení a odhalování protiprávní činnosti, porušování uděleného zákazu vstupu a porušování návštěvního řádu, doložení výše uvedených závadných jednání subjektu údajů“* provozuje prostřednictvím zpracovatele dva kamerové systémy.

Dlužno dodat, že ani v jednom z nich **nedocházelo ke zpracování biometrických osobních údajů** a kontrolovaný subjekt plnil všechny povinnosti dle GDPR (včetně provedené DPIA), a kontrola tudíž neodhalila žádný problém, který by správci vytkla.

Obce a státní správa

V rámci této oblasti ÚOOÚ provedl celkem tři kontroly. Pokud nahlédnete do souvislostí, mohlo by vás překvapit, proč ÚOOÚ **věnoval pozornost kontrole subjektů státní správy**, kterým nelze za stávajícího znění ustanovení § 61 odst. 2, respektive § 62 odst. 5

zákona o zpracování osobních údajů uložit správní trest.

Ačkoliv takové subjekty trestat skutečně nelze, **neznamená to, že je nelze kontrolovat** a ověřovat, zda splňují všechny povinnosti dle GDPR. V tomto duchu tak lze kvitovat postup ÚOOÚ, že se kontrolám věnuje, neboť každý **subjekt údajů má stále potenciální nárok domáhat se náhrady** utrpěné újmy dle čl. 82 odst. 1 GDPR. Orgány státní správy by tak neměly rezignovat na svoje povinnosti jen proto, že jim aktuálně není možno uložit sankci.

Dlužno dodat, že všechny tři kontroly se týkají obcí, které lze za orgány veřejné moci ve smyslu čl. 83 odst. 7 GDPR považovat bez ohledu na to, v jaké působnosti jednají. To však neznamená, že by se ÚOOÚ nevěnoval i „jiným" správním orgánům (například oznámení o zahájení kontroly ve věci rezervačního systému na očkování proti covidu-19 a podobně). Nyní už ale k proběhlým kontrolám.

Mobilní rozhlas

Hned první kontrola v této oblasti je poměrně zajímavá, neboť byla **zahájena v důsledku ohlášení porušení zabezpečení** osobních údajů – důležité je to, že osobou, která ohlášení provedla, byl pověřenec pro ochranu osobních údajů daného města.

Ústředním motivem ohlášení porušení zabezpečení a následné kontroly byl postup starosty, který si vyžádal od ředitele místní základní školy **seznam zaměstnanců a zákonných zástupců žáků** včetně jejich kontaktních údajů. Těmto osobám pak starosta na vlastní pokyn prostřednictvím importu **provedl registraci do aplikace Mobilní rozhlas** (tu si běžně subjekt údajů provádí sám registrací a udělením souhlasu se zpracováním osobních údajů), kterou provozuje soukromá společnost. Z textu poskytnutého ÚOOÚ neznáme bližší podrobnosti než to, že se vše událo v době vyhlášeného nouzového stavu v souvislosti s výskytem covidu-19.

Pověřenec a správce spolu musejí pravidelně komunikovat

ÚOOÚ v daném případě konstatoval několik porušení ustanovení GDPR – od ustanovení týkajících se právních titulů po informování o zpracování osobních údajů a dodržení zásady transparentnosti. Pro nás je však zajímavé to, že ÚOOÚ konstatoval, že **předmětný incident nelze považovat za porušení zabezpečení** osobních údajů. Úřad k tomu totiž dodal: *„Zároveň zjištěný stav týkající se spolupráce mezi kontrolovanou osobou a pověřencem pro ochranu osobních údajů kontrolující vyhodnotili jako stav mající značné rezervy z hlediska nastavení efektivní spolupráce, a hraničící s porušením povinností stanovených čl. 39 obecného nařízení."*

ÚOOÚ k tomu následně v rámci informování veřejnosti poskytl i doplňující informace: *„Při výběru a jmenování pověřence pro ochranu osobních údajů dle čl. 37 obecného nařízení je nutno pamatovat nejen na to, aby tento byl jmenován na základě svých profesních kvalit, odborných znalostí práva a praxe v oblasti ochrany osobních údajů, ale také na základě schopnosti plnit úkoly stanovené čl. 39 obecného nařízení. Uvedené však musí být též podpořeno postavením pověřence pro ochranu osobních údajů ve smyslu čl. 38 obecného nařízení a správce či zpracovatel musí zajistit, aby byl pověřenec pro ochranu osobních údajů náležitě a včas zapojen do veškerých záležitostí souvisejících s ochranou osobních údajů."*

Když to převedeme do lidské řeči, můžeme daný text chápat také jako vyčinění správci i jeho DPO za to, že spolu nekomunikují a že **DPO pravděpodobně nemá dostatečné kvality** k tomu, aby správně vyhodnotil všechny okolnosti týkající se zpracování GDPR, a tím pádem může docházet k porušení GDPR ze strany správce, neboť jím jmenovaný DPO nemusí splňovat podmínky čl. 37 odst. 5 GDPR.

K této kontrole na závěr ještě jednu poznámku – ÚOOÚ v daném případě pravděpodobně **posuzoval i možnost využití jiného právního titulu**, než je souhlas, a to s přihlédnutím k dané situaci. Ačkoliv neznáme bližší

podrobnosti, ÚOOÚ k tomu uvedl následující: *„Aplikaci právního titulu ochrany životně důležitých zájmů subjektů údajů nebo jiné fyzické osoby ve smyslu čl. 6 odst. 1 písm. d) obecného nařízení nebylo v tomto případě možné akceptovat.“*

Rezervační systém obce

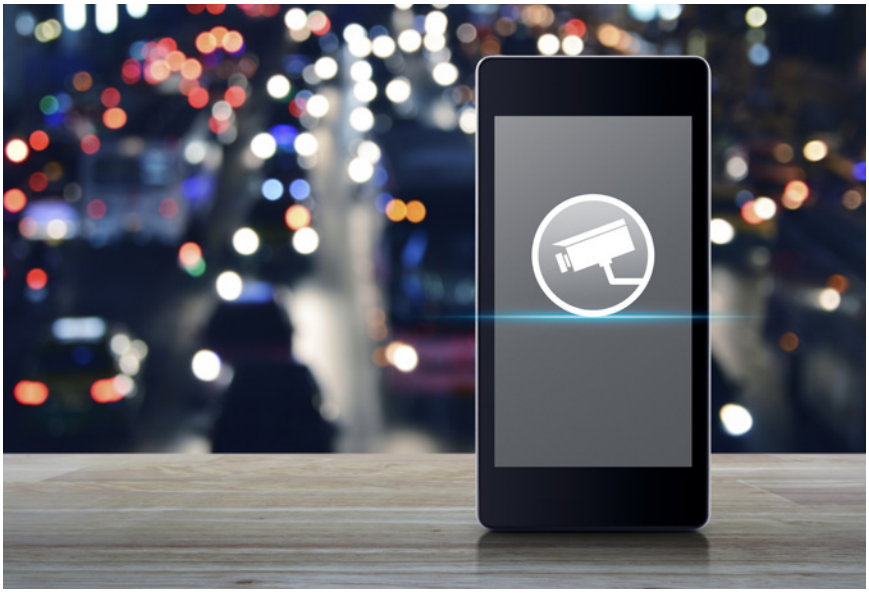
Druhá kontrola v této oblasti se týkala podnětu stěžovatele, jemuž se nelíbil způsob **zpracování osobních údajů v rámci rezervačních systémů obce**, tedy něco, co ÚOOÚ naposled komentoval ve svém vyjádření **zde**. Stěžovatel se totiž chtěl objednat na úřad kvůli novému občanskému průkazu, přičemž po kliknutí na odkaz byl **přesměrován na internetové stránky soukromého subjektu** (který tuto službu poskytuje vícero subjektům) a ty po něm pro provedení registrace bez dalšího bližšího poučení vyžadovaly uvedení osobních údajů.

ÚOOÚ se v rámci dané kontroly neomezil pouze na konstatování **porušení zásady transparentnosti, ale i zásady minimalizace** (viz zmíněné vyjádření výše). V rámci zpracování osobních údajů obcí se často setkáváme s poměrně zajímavým způsobem informování, a to prostřednictvím pouhého odkazu na záznamy o činnostech zpracování. Subjektu údajů je pak poskytnut pouze **odkaz na stránku se všemi záznamy o činnostech zpracování**, které bývají často velmi obecné – subjekt údajů v nich musí dále hledat svoji konkrétní situaci.

Tato praxe je velmi často kritizována, neboť v takovém případě **nelze hovořit o správném poskytnutí informací** o zpracování osobních údajů. Můžeme se však jen domnívat, jestli se tak dělo i v tomto případě, každopádně ÚOOÚ k tomu konstatoval, že *„poskytnuté informace ve smyslu čl. 13 obecného nařízení jsou natolik zobecněny, že nelze považovat za splněnou zásadu dle čl. 5 odst. 1 písm. a) obecného nařízení ve smyslu transparentnosti, a taktéž uvedené nelze považovat za transparentní poskytnutí informací ve smyslu čl. 12 odst. 1 obecného nařízení“*.

Odkázat uživatele na stránku se záznamy o činnostech nestačí

Pokud byste si z toho měli vzít ponaučení, mělo by to být zejména to, abyste **správně informovali subjekt údajů** a plnili svoji povinnost v souladu s Pokyny WP29 k transparentnosti. Nelze se spoléhat jen na to, jak k dané otázce přistupuje dodavatel technologie, neboť jak správně podotýká ÚOOÚ, **odpovědnost je vždy na správci**.



Městský kamerový systém

Kontrolou provedenou na základě kontrolního plánu prošlo bez ztráty květinky jedno ze sedmadvaceti statutárních měst. Kontrolováno bylo **zpracování osobních údajů prostřednictvím kamerových systémů městské policie**, jmenovitě městský dohledový systém, dohled nad světelnými křižovatkami, mobilní kamery na klopách strážníků a kamery umístěné ve služebních vozidlech. Mimoto se kontrola věnovala i kamerám, které využívá přímo město **za účelem ochrany podzemních garáží**, a taktéž kamerovým systémům dvou městských obvodů.

Ani v tomto případě **nedošlo ke konstatování žádného porušení**, přesto si povšimněte jedné věci, která je poměrně důležitá, ale přesto stále opomíjená a často se v ní chybuje – **kdo vlastně může provozovat jaké kamerové systémy?** Tomuto tématu jsme se již na stránkách Zpravodaje věnovali, pokud by vás tedy zajímaly podrobnosti, nahlédněte do archivu.

Závěr

Vždy byste měli pamatovat na povinnosti týkající se zejména **transparentnosti a správného stanovení zákonného titulu**. Jako pověřenci máte také za úkol správně vyhodnocovat situace a postupovat v souladu s nařízením. V dalším díle se můžete těšit na závěry z kontrol, které se týkají prodeje či školství.

▪▪▪

Mgr. Josef Bátrla,
advokát v oblasti ICT
www.josefbatrla.cz

Pokuta 6 milionů eur pro CaixaBank

Španělský dozorový úřad nedávno udělil nejvyšší pokutu ve své historii. Banka CaixaBank bude muset za porušení GDPR zaplatit 6 milionů eur. O co v případu šlo?

Španělský dozorový úřad (*Agencia Española de Protección de Datos*) uložil **pokutu v celkové výši 6 milionů eur bance CaixaBank**, jednomu z největších finančních ústavů ve Španělsku. Jedná se o nejvyšší uloženou pokutu v historii španělského dozorového úřadu. Jaká porušení byla zjištěna? Úřad uložil CaixaBank pokutu za **neplnění informační povinnosti** vůči subjektům údajů (ve výši 2 milionů eur) a za **protiprávní zpracování osobních údajů** (ve výši 4 milionů eur).

Španělský dozorový úřad dospěl k závěru, že dokumenty, které měly zajistit splnění informační povinnosti vůči subjektům údajů, neobsahovaly dostatečné informace, konkrétně ohledně **kategorií zpracovávaných osobních údajů, účelech zpracování a právním základu** jejich zpracování, a to zejména u zpracování, která byla opřena o čl. 6 odst. 1 písm. f) GDPR (tedy u zpracování prováděných na základě oprávněného zájmu). Při rozhodování o výši pokuty za toto pochybení (2 miliony eur) vzal úřad v úvahu **povahu, závažnost a dobu trvání protiprávního jednání**, nedbalostní charakter daného jednání, skutečnost, že CaixaBank je velkou společností, a obrat banky.

Banka podcenila informační povinnost

Španělský dozorový úřad dále dospěl k závěru, že souhlas se zpracováním osobních údajů, jejž banka používala, **nesplňoval podstatné náležitosti stanovené GDPR**. Podle úřadu jej tedy nebylo možné považovat za platný. Úřad dále zjistil, že oprávněný zájem nebyl u činností, které na něm byly založené, dostatečně odůvodněn. Podle něj tedy došlo k porušení čl. 6 GDPR. Úřad přistoupil k uložení pokuty ve výši 4 milionů eur. Vzal v úvahu stejné skutečnosti, k jakým přihlížel při uložení pokuty za nesplnění informační povinnosti vůči subjektům údajů (viz výše), a **navíc přihlédl i k charakteru osobních údajů**, jichž se předmětná zpracování týkala, a k výhodám, které banka tímto protiprávním postupem získala. Rozhodnutí dozorového úřadu je k dispozici na webových stránkách úřadu **zde** (ve španělském jazyce).

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

Povinné testování zaměstnanců vs. GDPR

Testovat zaměstnance musí nově i každý zaměstnavatel s více než 10 zaměstnanci! Co je třeba si pohlídat z hlediska ochrany osobních údajů?

Jak jsme vás již informovali v mimořádném čísle, podle **aktuálně platných mimořádných opatření Ministerstva zdravotnictví** smějí zaměstnavatelé umožnit svým zaměstnancům osobní přítomnost na pracovišti jen za podmínky, že **zaměstnanec podstoupí některou z forem testu** na přítomnost viru SARS-CoV-2 a výsledek tohoto testu je negativní. S povinným testováním souvisí i povinnosti v oblasti zpracování a zabezpečení osobních údajů. Připomínáme proto, co je třeba si pohlídat.

Údaj o zdravotním stavu

Při zajišťování testů pro zaměstnance dochází k tomu, že zaměstnavatel musí jako správce osobních údajů **zpracovat i údaje o výsledku provedeného testu**. Je-li výsledek pozitivní, zpracovává tím údaj o zaměstnancově zdravotním stavu, což je nejen osobní údaj, nýbrž podle čl. 9 obecného nařízení o ochraně osobních údajů (GDPR) **údaj zvláštní kategorie** (podle dřívější terminologie citlivý osobní údaj).

Ke zpracování tohoto typu osobního údaje může dojít i v souvislosti s povinností zaměstnance, který si provedl nebo mu byl laickou osobou proveden test na přítomnost antigenu viru SARS-CoV-2 a výsledek byl pozitivní, **oznámit tuto skutečnost zaměstnavateli**.

Zpracování bez souhlasu

Každé zpracování osobních údajů musí být podle čl. 6 GDPR zákonné. Jedním z přípustných právních titulů pro zpracování je i plnění právní povinnosti, která se na správce osobních údajů vztahuje. Mimořádná opatření ministerstva zdravotnictví patří mezi opatření obecné povahy, a **musí být tudíž považována za právní předpisy**. Osobní údaje zvláštní kategorie lze zpracovávat pouze v případech uvedených v čl. 9 odst. 2 GDPR. Patří mezi ně i nezbytnost zpracování z důvodu významného veřejného zájmu. Vzhledem ke všem okolnostem platí, že **testování zaměstnanců významnému veřejnému zájmu odpovídá**.

K zpracování údajů o provedeném testu nepotřebujete souhlas

Z uvedeného lze bezpečně dovodit, že pokud zaměstnavatel ve vztahu ke svému zaměstnanci zpracuje údaj zvláštní kategorie, tedy informaci o tom, že byl pozitivně testován, a bylo mu tím pádem diagnostikováno onemocnění covid-19, **jde o zpracování prováděné ve veřejném zájmu** a současně slouží ke splnění právní povinnosti, která je zaměstnavateli jako správci osobních údajů uložena. Samotná skutečnost, že ke zpracování dochází, nenarušuje GDPR. Vzhledem k existenci právního titulu je toto

zpracování zákonné, aniž k němu zaměstnavatel musí od dotčeného zaměstnance vyžadovat souhlas.

Povinnosti při zpracování

Zaměstnavatel jako správce osobních údajů si musí být vždy vědom svých povinností, které při zpracování osobních údajů podle GDPR má. Údaj o výsledku testu smí použít **výhradně v souvislosti s plněním svých povinností** podle platných mimořádných opatření. Současně platí, že smí zpracovávat pouze ty osobní údaje, které jsou pro splnění těchto povinností nezbytné. Údaje může zpracovávat pouze po dobu, během níž to bude podle okolností a vzhledem k dalším právům a povinnostem zaměstnavatele nezbytné.

S údajem o výsledku provedeného testu musí zaměstnavatel nakládat v souladu se základními zásadami zpracování osobních údajů, mezi něž patří i **povinnost zajistit náležité zabezpečení**. V prvé řadě musí zaměstnavatelé věnovat pozornost tomu, aby zajistili, že k tomuto osobnímu údaji budou mít přístup pouze osoby, u nichž je to nezbytné (ty, které mají u zaměstnavatele na starosti zajišťování agendy spojené s povinnostmi vyplývajícími z mimořádných opatření).

K výsledkům testů musí mít přístup jen nezbytné množství osob

Rozhodně není přípustné, aby byly výsledky testů zveřejňovány či **nekontrolovaně zpřístupňovány dalším osobám**. Při uplatnění nástrojů zabezpečení zpracování, stanovených v obecné rovině v čl. 32 GDPR a konkretizovaných se zřetelem k možnostem jednotlivých zaměstnavatelů jejich vnitropodnikovou dokumentací, musí zaměstnavatelé **zabezpečit údaje o výsledku provedených testů** před neoprávněným či protiprávním zpracováním, náhodnou ztrátou, zničením nebo poškozením.

Při zpracovávání údajů o výsledcích testů musí mít zaměstnavatelé na paměti i **zásadu transparentnosti**. V souladu s povinnostmi vyplývajícími z čl. 12 a následujících GDPR jsou povinni zaměstnance informovat zejména o tom, jaké údaje zpracovávají, za jakým účelem, po jakou dobu a zda a komu jsou předávány.

▪▪▪

JUDr. Jaroslav Stránský, Ph.D.

Stane se VB zemí s dostatečnou úrovní ochrany osobních údajů?

Evropská komise zveřejnila 19. února 2021 návrh rozhodnutí o odpovídající úrovni ochrany osobních údajů Spojeným královstvím. Dle daného rozhodnutí by Spojené království mělo být z pohledu předávání osobních údajů považováno za takzvanou bezpečnou třetí zemi (neboli třetí zemi s dostatečnou úrovní ochrany osobních údajů). Předávání osobních údajů do Spojeného království by tak nevyžadovalo ze strany předávajícího správce, respektive zpracovatele osobních údajů přijetí žádných dodatečných opatření (jako jsou například závazná vnitropodniková pravidla – Binding Corporate Rules, standardní smluvní doložky – Standard Contractual Clauses nebo schválený kodex chování podle čl. 40 GDPR spolu se závaznými a vymahatelnými závazky správce nebo zpracovatele ve třetí zemi uplatňovat vhodné záruky).

Podrobněji jsme se oběma variantám, tedy jak postupovat v případě, že rozhodnutí o odpovídající úrovni ochrany osobních údajů bude vydáno do konce června 2021, a jak postupovat v případě, že vydáno nebude, věnovali v **článku** Předávání osobních údajů do VB po brexitu – co se změní? Nyní se jeví, že pravděpodobnější bude první, pro všechny správce a zpracovatele osobních údajů určitě pozitivnější scénář, tedy že k vydání rozhodnutí dojde včas (do konce června 2021). Návrh rozhodnutí je dostupný z webových stránek Evropské komise **zde** (v anglickém jazyce).

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

Poradna

V případě, kdy testování zaměstnanců na nemoc covid-19 bude prováděno prostřednictvím poskytovatele zdravotnických služeb, bude třeba s tímto poskytovatelem uzavřít s ohledem na GDPR zpracovatelskou smlouvu? Vystupuje zaměstnavatel, kterému vyplývá povinnost testovat své zaměstnance, v roli správce osobních údajů a lékař, který provádí testování a vykazuje úkony zdravotní pojišťovně, v roli zpracovatele? Jak správně písemně ošetřit danou skutečnost?

V tomto případě se s ohledem na účely zpracování osobních údajů nepředpokládá povinnost uzavření zpracovatelské smlouvy, neboť v tomto vztahu se jedná o vztah dvou samostatných správců. Toto pravidlo platí obecně na každý vztah mezi zaměstnavatelem a závodním lékařem, respektive spolupracujícím poskytovatelem zdravotních služeb (viz například vyjádření ÚOOÚ **zde**).

V konečném důsledku jsou tak zaměstnavatel i lékař v pozici samostatných správců, jejichž povinnosti, které jim plynou ze strany GDPR, nejsou tímto nijak dotčeny. Oba subjekty mají povinnost informovat o možných příjemcích osobních údajů a celkově plnit svou informační povinnost.

V mimořádném čísle Zpravodaje pro pověřence v článku *Ochrana osobních údajů versus testování zaměstnanců na covid-19* uvádíte, že pokud se zaměstnanec nedostaví nebo odmítne testování na covid-19, jedná se o neomluvenou absenci a hrubé porušení pracovních povinností. Jak postupovat ve funkci starosty, který nemá uzavřenou pracovní smlouvu? Starosta tedy není zaměstnanec ve smyslu zákoníku práce, je veřejný funkcionář, člen zastupitelstva obce zvolený zastupitelstvem obce, aby ji zastupoval navenek, nemá uzavřen pracovní poměr, proto se na něj zákoník práce nevztahuje. Pokud by tedy odmítl nebo se nedostavil na testování na covid-19, jak v tomto případě postupovat?

Zodpovědět tuto otázku není zcela jednoduché, neboť i samotné pracovněprávní postihy spojené s testováním (respektive jeho odmítnutím) jsou aktuálně předmětem přezkumu ze strany soudní soustavy, přičemž vyřešení této oblasti bude mít pravděpodobně i dopad na následující odpověď.

Jak správně uvádíte, starosta není zaměstnancem obce, ale jeho orgánem. Na jeho působení tak zásadně nedopadá právní úprava uvedená v zákoníku práce a případné postihy tak v tomto duchu nelze ukládat (zjednodušeně řečeno). Funkce starosty je totiž v prvé řadě politická, neboť starosta (bez ohledu na to, zda jako uvolněný, či neuvolněný) vykonává veřejnou funkci.

Z výše uvedených důvodů je tak nutno nad různými sankcemi přemýšlet jako nad politickým postihem. Starosta se totiž za svoje činy a výkon funkce zodpovídá

v prvé řadě zastupitelstvu obce. V zákoně o obcích je taktéž stanoveno, že starostu volí z řad jejich členů samo zastupitelstvo – tentýž orgán má ale i možnost starostu odvolat, a to i bez udání důvodu usnesením, které bylo přijato nadpoloviční většinou všech členů zastupitelstva. Mohli bychom polemizovat o tom, zda oprávnění zastupitelstva úkolovat starostu lze vykládat jako oprávnění uložit povinnost starostovi, aby se podrobil testům, nicméně nakonec bychom (pokud vůbec) došli ke stejnému závěru – výkon funkce starosty je politickou funkcí, za jejíž výkon starosta nese odpovědnost, totéž pak lze říct i přeneseně o zastupitelstvu, která má svého starostu s trochou nadsázky „na svědomí".

Zpracováváme záznamy o zpracování za správce a stále nám není jasné, kdo všechno patří mezi příjemce, které v tabulce uvádíme – máme zde uvádět i zaměstnance správce, kteří dané osobní údaje zpracovávají? Nebo pouze příjemce, kteří jsou „externí" a jimž předáváme osobní údaje pro splnění právní povinnosti – například ČSSZ, finanční úřady, soudy a podobně?

Povinnost uvádět příjemce se objevuje na několika místech GDPR, zejména u záznamů o činnostech zpracování, ale také v rámci informování subjektů údajů o zpracování osobních údajů. Samotnou definici „příjemce" nalezneme přímo v čl. 4 odst. 9 GDPR, kdy za příjemce je považována „fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, kterým jsou osobní údaje poskytnuty, ať už se jedná o třetí stranu, či nikoliv. Avšak orgány veřejné moci, které mohou získávat osobní údaje v rámci zvláštního šetření v souladu s právem členského státu, se za příjemce nepovažují; zpracování těchto osobních údajů těmito orgány veřejné moci musí být v souladu s použitelnými pravidly ochrany údajů pro dané účely zpracování".

Co se týče zaměstnanců správce, ti se do tohoto výčtu nepočítají z toho důvodu, že prostřednictvím jejich úkonů vlastně dochází ke zpracování osobních údajů samotným správcem. Velmi zjednodušeně řečeno je totiž právnická osoba konstrukt, který sám o sobě žádný úkon provést neumí – činí tak prostřednictvím svých zástupců, tedy prostřednictvím statutárního orgánu či zaměstnanců. Pokud však tuto informaci uvádíte, nemělo by to samo o sobě být porušením GDPR, jedná se jen o nadbytečnou informaci.

Na základě jakého právního důvodu má správce zpracovávat osobní údaje zaměstnanců získané z GPS lokátorů ve firemních vozidlech? Na základě oprávněného zájmu, nebo uděleného souhlasu?

Obecně v zaměstnanecké agendě platí pravidlo, že když nemůžeme využít pro zpracování osobních údajů jiný právní titul než souhlas, pravděpodobně bychom za takovým účelem neměli zpracovávat osobní údaje vůbec. To platí i pro zpracování osobních údajů prostřednictvím GPS lokátorů ve firemních vozidlech. Vždy však záleží na účelu zpracování osobních údajů (není tedy vyloučeno, že takové zpracování může probíhat i na základě souhlasu, je to však velmi nepravděpodobné), ale ve většině případů se zejména pro účely ochrany majetku bude zpracování odehrávat na základě oprávněného zájmu.

Toto téma je však mnohem složitější, proto se mu budeme věnovat i v dalších číslech našeho Zpravodaje.

JOSEF BÁTRLA ADVOKÁT

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:
- **Monitoring zaměstnanců vs. GDPR**
- **Kontroly ÚOOÚ ve školství a obchodech**

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. 3. 2021 Elektronický zpravodaj vychází jako čtrnáctideník, celobarevný, 8 stran A4, ISSN 2571-1504.