**Často kladené dotazy**

**k problematice GDPR**

(aktualizované k 1. 3. 2018)

**Obce, příspěvkové organizace obcí, apod., poskytují různé sociální služby pro seniory. V rámci těchto služeb senioři uvádějí kontaktní údaje na své sousedy, rodinné příslušníky pro případ naléhavých událostí, jak to řeší GDPR?**

Pokud jsou kontaktní údaje osob uvedeny dobrovolně klienty sociální služby pro definované účely, tj. naléhavé situace, není zde rozpor se zákonem pro ochranu osobních údajů či nařízením GDPR, pokud si sociální služba tyto kontakty uschová pro naléhavé případy. Souhlas osob není nutný.

**Prezenční listiny na akcích organizovaných obcemi bývají tištěny do jednoho archu. Podpis účastníka akce je citlivým údajem. Tyto údaje bývají spolu se jménem, příjmením a navzájem se zastupující organizace viditelné pro všechny účastníky akce, kteří se podepisují na jedné listině. Každý z účastníků akcí, bývá viditelně označen (cedulka zavěšená na krku). Je to v souladu s GDPR? Jak má pořadatel akce postupovat? Jaký bude postoj Úřadu pro ochranu osobních údajů k prezenčním listinám a procesu jejich podepisování? Jak má pořadatel postupovat, je-li žádoucí, aby účastníci akci byli označeni visačkou s vlastními osobními údaji?**

Podpis subjektu údajů nespadá do zvláštní kategorie osobních údajů ve smyslu článku 9 obecného nařízení. Je-li účelem obcí pořádané akce, aby se účastníci vzájemně poznali a navázali kontakt, není volně přístupná prezenční kniha problémem. Taktéž označení účastníků z tohoto důvodu je možné, stejně tak může být tímto postupem zajištěno, že se akce budou účastnit jen příslušné osoby. Zpracovávat osobní údaje účastníků akce uvedeným způsobem je tak správce oprávněn bez jejich souhlasu v souladu s již citovaným ustanovením v rámci plnění úkolu prováděného ve veřejném zájmu. Je úkolem obce, aby určila účel a posoudila právní důvod zpracování. Zároveň je třeba dbát na zásadu minimalizace údajů, neboť správce je oprávněn zpracovávat osobní údaje přiměřené, relevantní a omezené na nezbytný rozsah ve vztahu k účelu, pro který jsou zpracovávány.

**Smlouvy s právnickými osobami, ve kterých jsou uvedeny kontakty na fyzické osoby – zaměstnance firem. (např. ve smlouvě s právnickou osobou – dodavatel SW uvedl kontakty (jméno, příjmení, telefon) pro poskytování helpdesku.**

**Jak správně přistupovat k těmto smlouvám? Co když zaměstnanec firmy, jehož údaje jsou obsahem smlouvy, požádá o zapomenutí v souvislosti s ukončením pracovního poměru (anonymizovat údaje zpětně je nereálné).**

Pokud trvá právní důvod zpracování a osobní údaje jsou dále potřebné pro účely, pro které byly shromážděny. Zjednodušeně lze říci, že správce je povinen, pokud obdrží žádost subjektu údajů o výmaz osobních údajů, odstranit osobní údaje zpracovávané na základě souhlasu subjektu údajů, avšak pouze tehdy, pokud zároveň nejsou osobní údaje zpracovávány i na základě jiného právního důvodu (např. pro účely plnění povinnosti apod.). U osobních údajů zpracovávaných na základě jiného právního titulu zreviduje účel a rozsah zpracování, aby mohl případně odstranit nadbytečně zpracovávané osobní údaje. Uzavřené smlouvy včetně osobních údajů je obec povinna uchovat.

**Je jméno samo o sobě s uveřejněním funkce (název pracovní pozice) osobním údajem, který podléhá ochraně (bez další specifikace adresa, telefon)?**

Jméno, příjmení a telefonní e-mailový kontakt zaměstnance obce jsou osobními údaji dle obecného nařízení, neboť na jejich základě lze subjekt údajů identifikovat, resp. jde o údaje vztahující se k identifikovatelné osobě. Předání takovýchto osobních údajů obcí třetí osobě je zpracování dle nařízení GDPR a musí probíhat na základě právního titulu dle článku 6 obecného nařízení GDPR. Pokud půjde typicky o předávání pracovních kontaktů na zaměstnance, tak to se obejde bez souhlasu.

**Jak je to s osobním údajem a žádostí o dotaci?**

Dochází-li ke zpracování osobních údajů v rámci žádosti o dotaci, konkrétně při jejím doložení, není pro takové zpracování nutný souhlas subjektu údajů, neboť jde o zpracování jako důsledek plnění právní povinnosti dle článku 6 odst. 1 písm. c) obecného nařízení GDPR.

**Jak je to s činností spolku a osobními údaji?**

Pokud jde o činnost spolku, tak pro vnitřní potřeby spolku se souhlas člena se zpracováním osobních údajů nevyžaduje, zpracování probíhá na základě plnění právní povinnosti dle ustanovení článku 6 odst. 1 písm. c) obecného nařízení. Pokud však jde o zpracování formou zveřejnění seznamu členů, je nutný souhlas člena spolku s takovýmto způsobem zpracování dle ustanovení článku 6 odst. 1 písm. a) obecného nařízení, tak jak to předvídá ustanovení § 236 odst. 3 zákona č. 89/2012 Sb., občanský zákoník.

**Poskytuje SMO ČR pověřence pro ochranu osobních údajů?**

Svaz měst a obcí osoby pověřence pro ochranu osobních údajů neposkytuje. Svaz měst a obcí pomáhá obcím při přípravě nejen pověřence pro ochranu osobních údajů, ale také při revizi osobních údajů, zpracovává vzory dokumentů, které se budou muset předložit při případné kontrole ze strany Úřadu pro ochranu osobních údajů. Na realizaci nařízení připravujeme obce v plném rozsahu, neboť obce nemají pouze povinnost zřídit funkci pověřence pro ochranu osobních údajů, ale také vést záznamy o zpracování osobních údajů.

**Kdo má povinnost zřídit funkci pověřence pro ochranu osobních údajů (kromě orgánu veřejné moci)?**

Jmenovat správce musí za splnění jedné ze tří podmínek. Těmi jsou:

* Zpracování provádí orgán veřejné moci či veřejný subjekt, s výjimkou soudů jednajících v rámci svých soudních pravomocí
* Hlavní činností správce nebo zpracovatele spočívají v operacích zpracování, které kvůli své povaze, svému rozsahu nebo svým účelům vyžadují rozsáhlé pravidelné a systematické monitorování subjektů údajů

(k hlavní činnosti správce uvádíme, že nejdříve se musí vymezit pojem „hlavní činnost“). Hlavní činnost je taková činnost, jež je primární aktivitou správce či zpracovatele činností, kvůli, které byl zřízen nebo která je nedílnou součástí smyslu jeho existence, nikoliv tedy sekundární, pomocná činnost. Hlavní činnost lze tedy chápat jako hlavní cíl správce nebo zpracovatele.

Příklady:

1. Hlavní činností je poskytování zdravotnické péče. Tuto péči by však nemocnice nemohla poskytovat bez toho, aby zpracovávala osobní údaje pacientů, proto bude také toto zpracování hlavní činností správce. Tuto péči ale nelze poskytovat bez zpracování osobních údajů pacientů, v tomto případě, bude zpracování hlavní činností správce.
2. Běžné aktivity organizace, kde jsou zpracovány osobní údaje, které jsou vzhledem k povaze sekundární. Pro zajištění hlavní činnosti můžou být nezbytné, nicméně jsou od ní jasně oddělitelné (např. oddělení financí ve firmě).

* Hlavní činnosti správce nebo zpracovatele spočívají v rozsáhlém zpracování zvláštních kategorií údajů a osobních údajů týkajících se rozsudků v trestních věcech a trestných čin

**Proč je Úřad kompetentní ke kontrole GDPR?**

Na základě čl. 51 Nařízení GDPR se stanoví, že každý členský stát stanoví, že jeden nebo více orgánů veřejné moci jsou pověřeny monitorováním uplatnění tohoto nařízení. Činnost úřadu je vymezena zákonem č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů.

Úřad na základě tohoto zákona:

* Provádí dozor nad dodržováním zákonem stanovených povinností při zpracování osobních údajů.
* Vede registr povolených zpracování osobních údajů.
* Přijímá podněty a stížnosti občanů na porušení zákona.
* Poskytuje konzultace v oblasti ochrany osobních údajů

Jelikož Česká republika vstoupila na základě referenda do Evropské unie, stala se tak i součástí evropského právního prostoru. GDPR je přijato formou nařízení, tedy má přímý účinek. Dozor nad dodržováním zákonem stanovených povinností v tomto případě jsou aplikovatelné i na nařízení.

**Kolik je běžná cena za implementaci GDPR pro obce?**

Svaz měst a obcí České republiky nedisponuje informacemi ohledně nabídek za služby, které musí město/obec zaplatit při zavádění GDPR (vstupní audit).

Ceny za služby nemůžeme specifikovat, ale pro základní orientaci uvádíme, že specializovaný software na GDPR pro obec sčítající cca 20 000 obyvatel vyjde na 18 500 Kč/rok, případně další servisované služby na základě informací našich členů.

Tento program je koncipován tak, že po naplnění daty vytvoří audit osobních údajů, včetně zhodnocení rizik a návrhu opatření.

Školení zaměstnanců provádíme i my jako SMO ČR, dlouhodobě se také budeme zabývat pomoci pověřencům pro ochranu osobních údajů pro členské obce zdarma.

**Musí domov pro seniory jmenovat pověřence pro ochranu osobních údajů?**

Domov pro seniory pověřence zřizovat nemusí, může si ho však zřídit dobrovolně na základě čl. 39 obecného nařízení. Pokud si pověřence nestanoví, je vítané mít v organizaci určenou osobu, která se bude ochraně osobních údajů věnovat.

**Budou muset společenství vlastníků jednotek jmenovat pověřence pro ochranu?**

Pokud pouze provádí zpracování osobních údajů v souvislosti s činnostmi spočívajícími v zajišťování výkonu bytových spoluvlastnických práv a povinností tak, jak je upravuje zákon č. 89/2012 Sb. pověřence jmenovat nemusejí.

**Co se rozumí pod pojmem „rozsáhlé zpracování a rozsáhlé systematické monitorování“? Je možno tyto pojmy vyjádřit?**

Obecné nařízení o ochraně osobních údajů pojem pravidelného a systematického monitorování subjektů údajů nedefinuje, ale koncept „monitorování chování subjektů údajů“ zahrnuje veškeré formy sledování a profilování na internetu, a to i pro účely behaviorální reklamy. Pojem monitorování však není omezen na on-line prostředí a on-line sledování by mělo být považováno pouze za příklad monitorování chování subjektů údajů. Pracovní skupina WP29 vykládá pojem „pravidelné“ v tom smyslu, že znamená jedno nebo více z níže uvedeného:

• probíhající nebo vyskytující se po určité období v určitých intervalech,

• opakovaně se vyskytující nebo opakovaný ve stanovených časech,

• odehrávající se nepřetržitě nebo pravidelně. Pracovní skupina WP29 vykládá pojem „systematické“ v tom smyslu, že znamená jedno nebo více z níže uvedeného:

• vyskytující se v souladu se systémem,

• předem naplánované, organizované nebo metodické

**Podléhá požadavkům GDPR účetnictví (prodejní doklady, mzdová a personální agenda) a co je třeba posoudit při zabezpečení této agendy?**

Obecné nařízení o ochraně osobních údajů (GDPR) se týká všech subjektů, které zpracovávají osobní údaje fyzických osob, například zaměstnanců či klientů. V rámci účetnictví se jedná o zpracování podle zvláštního zákona, kterým je zákon č.  563/1991 Sb., o účetnictví, a je tedy nezbytné pro splnění právní povinnosti, která se na správce vztahuje ve smyslu článku 6 odst. 1 písm. c) obecného nařízení.

Úřad pro ochranu osobních údajů doporučuje přihlédnout, v jakém stavu se nachází technika zvolená pro účel zpracování, provádět pravidelné testování a hodnocení účinnosti zavedených technických a organizačních opatření pro bezpečnost zpracování. Při posuzování vhodné úrovně bezpečnosti je třeba zohlednit zejména rizika, která představuje zpracování, zejména náhodné nebo protiprávní zničení, ztráta, pozměňování, neoprávněné zpřístupnění předávaných, uložených či jinak zpracovávaných osobních údajů, nebo neoprávněný přístup k nim.

**Jaký je právní titul pro zpracování osobních údajů v rámci podnětů a podání občanů vůči veřejné správě? Je to zákon č. 500/2004 Sb., správní řád, tedy je možno použít právní titul dle čl. 6 odst. 1 písm. c) GDPR?**

Přijímání podnětů a stížností lze řadit pod právní důvody zpracování nezbytné pro plnění zákonem stanovené povinnosti.

**Lze nahrávat zasedání obecního zastupitelstva?**

Zasedání obecního zastupitelstva lze považovat za věc veřejného zájmu. Ve věci veřejného zájmu nahrání podobizny člověka lze podřadit pod tzv. jednu ze zákonných licencí. Samotné nahrání v tomto případě je možné. Problém může nastat v případě, kdy zastupitelstvo obce bude projednávat věci, které se týkají 3. osob. V této otázce je třeba každou věc řešit individuálně.

Obecně zákonná dovolení u podobizen a záznamů (zvukových i obrazových) dle zákona č. 89/2012 Sb., jsou tyto:

* výkon či ochrana práv nebo oprávněných zájmů jiných osob (např. před domácím násilím) děje-li se tak za účelem jeho uplatnění či obrany některou z přípustných forem soudního, správního či jiného úředního řízení
* úřední účel na základě zákona (ospravedlněno veřejným zájmem na veřejném pořádku v úředních věcech)
* o veřejné vystoupení ve věcech veřejného zájmu (např. právě na zasedání obecního zastupitelstva)
* vědecký či umělecký účel (např. obrazový záznam zákroku k lékařskému výzkumu) o zpravodajský účel (např. i internetem)
* **ani při využití zákonné licence nesmí dojít k použití nepřiměřeným způsobem proti oprávněným zájmům člověka**

**Musí kulturní příspěvkové organizace kraje (muzea a galerie) zřizovat funkci DPO ve svých organizacích, když nedochází v dané organizaci k rozsáhlému zpracování osobních údajů (dle čl. 37 obecného nařízení)?**

Neplatí, že by jen pouze z důvodu, že organizace byla založena subjektem, který musí mít pověřence, měla mít též pověřence. Jinými slovy u takto založených organizací je nutné zkoumat, zdali nemusí mít pověřence především dle článku 37 odst. 1 písm. b), c) obecného nařízení. Důležité je věnovat pozornost podmínkám, které musí nastat pro vznik této povinnosti (např. musí jít o hlavní činnost spočívající v rozsáhlém zpracování zvláštních kategorií osobních údajů či jít o hlavní činnost spočívající v rozsáhlém monitorování subjektů údajů).

Muzeum, galerie, knihovna – jejich činnost nespadá do vymezení v článku 37 odst. 1 písm. b) a c) obecného nařízení – zatímco například nemocnice, zřízená městem, bude muset mít pověřence, ale ne z důvodu, že ji založilo město, ale proto, že je její hlavní činností rozsáhlé zpracování zvláštních kategorií osobních údajů (o zdravotním stavu), tedy dle písmena c).

Krajské knihovny lze postavit na úroveň ostatním knihovnám, tj. nemusí mít pověřence, a to ani tehdy, pokud budou rozesílat pozvánky na jimi pořádané akce. Muzea, galerie či knihovny nemusí mít pověřence, pokud zpracovávají nezbytné osobní údaje v souvislosti s jejich oprávněnou činností, včetně osobních údajů zaměstnanců pro pracovněprávní účely či uspokojování potřeb členů nebo mají kamerový systém.

**Musí mít pověřenec pro ochranu osobních údajů nějakou certifikaci? Spousta firem certifikaci na DPO nabízí.**

Nařízení Evropského parlamentu a Rady (EU) 2016/679 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) nestanovuje certifikaci pověřence jako předpoklad výkonu funkce pověřence. Pověřenec tak certifikát mít nemusí a správce může jako pověřence vybrat i „necertifikovanou“ osobu, která disponuje dostatečným právním povědomím o ochraně osobních údajů a citovaném Obecném nařízení.

Není vyloučeno, že některé firmy „certifikaci“ pověřenců nabízejí, nicméně využití certifikace pověřence bude na dobrovolné bázi, a to jak ze strany pověřence, tak ze strany správce, který nemá povinnost vybírat certifikovaného pověřence.

**Kdo bude kontrolovat pověřence pro ochranu osobních údajů, že vykonávají svou činnost řádně a s péčí odborníka? Bude to ÚOOÚ?**

Obecné nařízení o ochraně osobních údajů stanovuje povinnost jmenovat pověřence vymezenému okruhu organizací. Primárně tak bude Úřad pro ochranu osobních údajů kontrolovat, zdali organizace, která má podle článku 37 odst. 1 obecného nařízení povinnost jej jmenovat, tak učinila. K institutu pověřence se však váží i další povinnosti, mimo jiné povinnost jmenovat pověřence na základě jeho profesních kvalit, zejména na základě jeho odborných znalostí práva a praxe v oblasti ochrany údajů a schopnosti plnit úkoly stanovené v článku 39 obecného nařízení. Součástí kontroly tak může být i kontrola plnění povinnosti dle článku 37 odst. 5 obecného nařízení. Ta by byla na místě především tehdy, pokud by zpracování, které provádí organizace se jmenovaným pověřencem, vykazovalo závažná pochybení a vznikaly by tak pochyby o odborné úrovni jmenovaného pověřence.

**Nařízení operuje s pojmem veřejný zájem, co je to?**

Veřejný zájem platí mezi tzv. „neurčité právní pojmy“, výklad je různý. Obecně ale jde o takový zájem, resp. zájmy, jež by bylo možno označit za obecné či veřejné, resp. obecně prospěšné zájmy, jejichž nositeli jsou blíže neurčené, nicméně alespoň rámcově určené determinovatelné okruhy označené jako „veřejnost“.