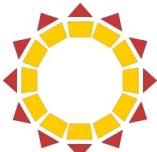


# ANALÝZA DOPADŮ GDPR NA MÍSTNÍ SAMOSPRÁVY



POSLANECKÁ SNĚMOVNA  
PARLAMENTU ČESKÉ REPUBLIKY

Tento materiál vznikl za spolupráce spolků Iuridicum  
Remedium a Otevřená města s podporou kanceláře  
poslance Ondřeje Profanta. Licence: CC BY-SA 4.0



# PŘEDMLUVA

Nařízení Evropského parlamentu a Rady (EU) 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů, zkráceně obecné nařízení o ochraně osobních údajů (General data protection regulation – GDPR), představuje pro zpracovatele osobních údajů nemalou výzvu při jeho naplňování. Vzhledem k blížícímu se datu 25. 5. 2018, kdy GDPR nabývá účinnosti, se množí nejistota úřadů, v jaké míře a v jakých oblastech na ně nařízení dopadá. Jelikož je nařízení nové, neexistuje dostatek výkladových materiálů, které by zpracovatelům osobních údajů přiblížily nové legislativní nároky.

Úřad pro ochranu osobních údajů, který je ve smyslu nařízení dozorovým úřadem pro ČR, popisuje GDPR jako „právní rámec ochrany osobních údajů platný na celém území EU, který hájí práva jejich občanů proti neoprávněnému zacházení s jejich daty a osobními údaji.“

Následující text vznikl se záměrem co nejvíce usnadnit obecním úřadům a jejich organizacím splnění povinností a zřízení opatření vycházející z GDPR. V první části „Analýza dopadů GDPR na organizace územní samosprávy“ naleznete shrnutí nároků GDPR ve vztahu k obcím. Tyto nároky se týkají především zmapování agend a procesů, při kterých dochází ke zpracovávání osobních údajů, a na to navázané povinnosti. Mezi ty se řadí zřízení pozice pověřence pro ochranu osobních údajů, úpravy smluv se zpracovateli dat, tvorba vnitřních předpisů pro nakládání s osobními údaji a řada organizačních a technických opatření.

Druhá část, která tvoří přílohu Analýzy, přistupuje k popsaným povinnostem z praktického hlediska. „Manuál se vzory dokumentů k implementaci GDPR pro obce“ má obecním úřadům poskytnout sroitelnou ná povědu s konkrétními doporučeními zejména pro úpravy smluv s externími zpracovateli osobních údajů.

# ANALÝZA DOPADŮ GDPR NA ORGANIZACE ÚZEMNÍ SAMOSPRÁVY

Je obecně známým a akceptovaným faktem, že stoprocentní implementace GDPR se v termínu do účinnosti u většiny správců a zpracovatelů nedosáhne. Tato analýza se zabývá několika prioritními opatřeními, která k implementaci výrazně pomohou a budou případně dozorovým orgánem zkoumána na prvním místě.

Pojednává-li se o dopadech, lze počítat s jistou pravděpodobností, že horní hranice pokut bude pro orgány veřejné moci či veřejným subjektům stanovena na 10 milionů Kč. Tak je to stanoveno v návrhu zákona o zpracování osobních údajů (dále jen „doprovodný zákon“)<sup>1</sup>, zpracovaného na základě zmocnění v GDPR. Dají se ovšem očekávat pozměňovací návrhy rušící tento „dvojí metr“ ve vztahu k soukromému sektoru<sup>2</sup>, nelze však ani vyloučit

<sup>1</sup> Návrh nařízení o respektování soukromého života a ochraně osobních údajů v elektronických komunikacích a zrušení směrnice č. 2002/58/ES, online:

<http://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX:52017PC0010>

<sup>2</sup> Např. město Černošice:

[http://www.mestocernosice.cz/e\\_download.php?file=data/editor/69cs\\_3.pdf&original=106-evidence\\_osobnich\\_udaj%C5%AF\\_101.pdf](http://www.mestocernosice.cz/e_download.php?file=data/editor/69cs_3.pdf&original=106-evidence_osobnich_udaj%C5%AF_101.pdf)

přijetí rakouského modelu, kde orgány veřejné moci a veřejné subjekty pokutám nepodléhají vůbec<sup>3</sup>.

Nutno zmínit i dopady na poli elektronických komunikací v dlouhodobějším horizontu. V tuto chvíli i v době účinnosti GDPR se toto bude vztahovat i na elektronické komunikace. V legislativním procesu je ovšem tzv. nařízení e-privacy<sup>4</sup>, které bude sloužit jako speciální právní úprava a je možné, že si vyžádá dílčí implementační změny poté, co také na bude účinnosti (odhady jsou na několik měsíců až po dva roky legisvakace, která je některými zájmovými skupinami požadována). S působením územní samosprávy se ovšem sféra elektronických komunikací protíná jen okrajově, takže rozhodně nepůjde o nutnou změnu významnějšího rozsahu.

Možnost zajištění souladu s GDPR pomocí přihlášení se k „oborovým“ kodexům chování (čl. 40 GDPR) anebo prostřednictvím certifikačních schémat (čl. 42 GDPR) se v této analýze pomíjí. V době zpracování analýzy není a ani v době účinnosti GDPR nebude k dispozici ani jeden z těchto nástrojů usnadnění a standardizace implementačních procesů. Z povahy věci se většina analýzy týká automatizovaného zpracování osobních údajů, zejména tedy jejich digitální podoby v informačních systémech; neautomatizované zpracování je zmíněno jako specifická podmnožina zpracování v části B.3. Pokud se dále v textu hovoří o obci, týká se to i kraje.

<sup>3</sup> Stanovisko WP 29 k pověřenci č. 2/2017 Zpracování osobních údajů na pracovišti

([https://www.uouou.cz/assets/File.ashx?id\\_org=200144&id\\_dokumenty=28294](https://www.uouou.cz/assets/File.ashx?id_org=200144&id_dokumenty=28294)), Metodické doporučení MV k pověřenci

(<http://www.mvcr.cz/gdpr/clanek/temp002.aspx>)

<sup>4</sup> obsahuje § 4 odst. 5 zákona o kybernetické bezpečnosti"

# **A. HLAVNÍ AKTIVITY, KTERÉ MUSÍ OBEC PROVÉST – DOPADY ČASOVÉ A NÁKLADOVÉ A TIPY NA JEJICH PROVEDENÍ**

## **I. DATOVÁ ANALÝZA (MAPOVÁNÍ DAT) A PŘÍPRAVA ZÁZNAMŮ O ZPRACOVÁNÍ VČETNĚ OHODNOCENÍ RIZIKOVOSTI**

Část samospráv zahájila první fázi přípravy na GDPR začátkem roku 2018, ojediněle se datovou analýzou zabývaly některé městské části a obce již v roce předchozím.

Dosavadní zkušenosti pomáhají odhadnout časovou i jinou náročnost této přípravy takto: Průměrná městská část nebo obec s rozšířenou působností tj. III. typu má zhruba 160-180 agend v přenesené působnosti. U malých obcí bude počet agend podstatně nižší, navíc může být na základě veřejnoprávní smlouvy domluven výkon některé z agend jinou obcí (v takovémto případě není daná obec ani správcem ani zpracovatelem osobních údajů). V případě obce, která pro jinou obec vykonává působnost dané agendy, nepůjde o vyšší zátěž ve fázi datové analýzy, kterou musí provádět tak jako tak pro „své“ osobní údaje. Projeví se pouze ve vyším počtu osobních údajů jednoho typu v záznamech o zpracování, což eventuálně může zvýšit nepatrně rizikovost zpracování.

Pro samosprávy, které jsou před zahájením této fáze, je velmi dobrou zprávou, že v brzké době budou mít připraveny vzorové materiály pro provádění datové analýzy (resp. terminologí Ministerstva vnitra „systémové analýzy“)<sup>5</sup>. Na základě dohody ÚOOÚ a resortů by se totiž měly jednotlivé resorty věnovat přípravě na účinnost GDPR (tedy zejména metodickému vedení) ve své působnosti. Koordináční roli má plnit Ministerstvo vnitra, které je zároveň gesčním resortem pro územní samosprávu.

Pro obce, které nebudou čekat na vzorové systémové analýzy, lze doporučit sestavit si základ pro analýzy ze svých agend, která bude tvořit základ pro povinné záznamy o zpracování dle čl. 6 GDPR z těchto zdrojů:

Registr práv a povinností, resp. ta jeho část, která je přiřazená dané obci coby orgánu veřejné moci (zákon č. 111/2009 Sb., o základních registrech, a nařízení vlády č. 161/2011 Sb., o stanovení harmonogramu a technického způsobu provedení opatření podle § 64 až 68 zákona o základních registrech). Lze rovněž vycházet z oznámení o vykonávání působnosti v agendě, které všechny orgány veřejné moci povinně podávají Správě základních registrů (§ 6 zákona o základních registrech),

Povinný přehled zákonů, kterými se obec řídí podle zákona č. 106/1999 Sb., o svobodném přístupu k informacím, a jeho prováděcí vyhlášky č. 442/2006 Sb., kterou se stanoví struktura informací zveřejňovaných o povinném subjektu způsobem umožňujícím dálkový přístup, konkrétně položky č. 14.1. Přílohy 1 (Nejdůležitější používané předpisy),

<sup>5</sup> bezprostředně před tiskem MV ČR uveřejnilo tzv. Checklisty pro obce, které nabízí ucelené vodítko zejména pro menší obce; online:

<http://www.mvcr.cz/gdpr/clanek/kontrolni-seznamy-checklisty-pro-obce.aspx>

Web ÚOOÚ, z něhož lze využít základní přehled hlavních předpisů upravujících nakládání s osobními údaji a porovnat jej se svými agendami anebo vlastní dobrovolně zpracovaný přehled evidence osobních údajů zpracovaný v rámci povinně zveřejňovaných informací dle informačního zákona<sup>6</sup>,

Vlastní spisový řád, z něhož lze získat jiný pohled například na problematiku skartačních lhůt, a to podle evidencí, neboť tato součást (vyjmenování všech samostatných evidencí) je dle zákona povinnou položkou spisového řádu.

Přehled shora uvedených zdrojů je dobrým základem pro určení účelu zpracování osobních údajů a obvykle i pro jejich tituly (v přenesené působnosti půjde o titul dle čl. 6 odst. 1 písmeno e) GDPR, tj. výkon veřejné moci). Je tedy zřejmé, že s těmito pomůckami si obce zmapují především svá zpracování osobních údajů v přenesené působnosti a typická zpracování v oblasti působnosti samostatné.

Atypické agendy obvykle v samostatné působnosti je třeba analyzovat zvlášť pečlivě. Ve fázi mapování je třeba vyčlenit kapacitu i na zmapování různého typu zcela dobrovolného (sms informování, provozování obecních wi-fi a jiných připojení či občanské oslav) nebo o zákon opřeného (kroniky) servisu občanům, kde dochází ke zpracování osobních údajů.

Povinné položky záznamů o zpracování osobních údajů (dále

<sup>6</sup> Enterprise Vault, Data Insight apod.

jen „záznamy“) jsou dle GDPR jasně dané (jméno a kontaktní údaje obce jako správce, včetně kontaktu na pověřence, účely zpracování, kategorie subjektů údajů, kategorie příjemců, informace o ev. předávání do třetí země, ev. lhůty pro výmaz a ev. popis bezpečnostních opatření). Obci však velmi usnadní mapovací fázi i následnou implementaci, pokud zahrne do záznamů i další informace, které pak pomohou s plněním povinností dle GDPR. Mělo by jít o rizikovost zpracování, tj. již zde se předběžně posoudí riziko jednoduchým namodelováním situace, jaké by měla pro osoby důsledky nedostupnost, zveřejnění či pozměnění dat. Vhodné je zde pamatovat na doplňkové kontaktní údaje pro případ nutnosti oznámení incidentu (právním titulem zpracování pak bude plnění právní povinnosti, zde ze samotného GDPR), poznámky o možnostech vyhledání na základě žádosti subjektu údajů apod. Manuál pro obce obsahuje detailní vzor takového obohaceného záznamu, který pak v implementaci výrazně pomůže. Do záznamů je také vhodné doplnit, zda existuje povinnost – a výjimka z ní – informovat subjekty údajů o zpracování dle čl. 13 a 14 GDPR. U obcí, kde je právní titul nejčastěji plnění povinností bude výjimka často naplněna (viz čl. 14 odst. 5 písm. c)).

Výjimky, podle kterých se záznamy o zpracování vést nemusí (zpracování není rizikové, je pouze příležitostné a netýká se citlivých osobních údajů), na obce zpravidla nedopadnou. Nevadí to; pořízení záznamů je však velmi výhodná metoda jak zahájit implementaci GDPR. Proto lze doporučit přípravu záznamů i s dalšími nepovinnými údaji, které však později významně pomohou při naplňování povinností daných GDPR.

Dosavadní zkušenosti naznačují, že jeden záznam o zpracování obnáší 1-3 hodiny práce posuzujícího a pracovníka, který má příslušnou agendu na starost (obvykle vedoucí odboru). Předpokládá se, že vzorové systémové analýzy mohou náročnost snížit. Určitě však nelze počítat s tím, že

by tuto klíčovou fázi zvládly automatizovaně různé softwarové nástroje, které se nabízejí „na klíč“; prvek lidského posuzování je v této fázi skutečně nezbytný.

Nákladově se datová analýza pro městskou část či obec s pověřeným obecním úřadem v případě externích služeb obvykle pohybuje zhruba v rozmezí sto až tři sta tisíc Kč, s výjimkami do obou směrů. Nižší ceny nabízí obvykle velcí poskytovatelé služeb, kteří už pro obce provádí GDPR konzultace delší dobu. Vyšší ceny pak logicky platí kraje, velká města nebo jejich velké příspěvkové organizace. Cenové rozmezí je jen velmi indikativní, protože z dostupných dat je zjevné, že rozsah objednaných služeb se liší, závisí také, zda obec všechny fáze implementace svěří jednomu dodavateli, anebo zakázku rozdělí (i s tím, že část provede vlastními silami). Vhodné bude sdílet zkušenosti s dodavateli služeb s obcemi, které již mají tuto první fázi realizovanou; jde řádově o stovky obcí a rychle přibývají.

## **II. USTAVENÍ POVĚŘENCE PRO OCHRANU OSOBNÍCH ÚDAJŮ**

Obsazení pozice pověřence (DPO) si u obcí žádá zejména kapacitu na rozhodnutí o formě zapojení (externí výkon-/zaměstnanec) a jeho začlenění v rámci organizační struktury a případné provedení výběrového řízení/kontraktaci externího pověřence či jeho výběr z nabízených sdílených služeb pro územní samosprávy. V současnosti je k dispozici dostatek podkladů<sup>7</sup>, které účinně objasně možnosti a podmínky ustanovení a fungování pověřence:

<sup>7</sup> Zejm. § 4b odst. 2 zákona č. 106/1999 Sb., o svobodném přístupu k informacím.

- a) Pověřence je povinna ustavit každá obec bez ohledu na velikost a příspěvková organizace, která rozhoduje o právech a povinnostech (např. školy) nebo která provádí rozsáhlé zpracování citlivých osobních údajů anebo pravidelné systematické monitorování (např. dopravní podniky). Výslově dle Ministerstva vnitra nemusí mít pověřence knihovny či technické správy komunikací<sup>8</sup>. Doprovodný zákon, který je aktuálně v legislativním procesu, definuje v důvodové zprávě příspěvkové organizace (s vyjimkou škol, které rozhodují o právech a povinnostech) jako „pomocné“ subjekty, které pověřence mít nemusí. Definitivní podoba doprovodného zákona však v tuto chvíli jasná není – je navržen do zrychleného projednávání v parlamentu, avšak není jisté, že se mu pozměňovací návrhy vyhnou,
- b) Funkce pověřence může být vykonávána externě, a to i jako společný pověřenec pro několik subjektů; vždy však musí být zajištěna jeho rychlá dostupnost pro ÚOOÚ i veřejnost. Lze využít nabídky komerčních subjektů, ale výhodnější se jeví pověřenci nabízení ze strany asociací územních samospráv. Vhodný je i společný pověřenec pro obec a její příspěvkové organizace, které podléhají povinnosti pověřence mít,
- c) Pověřencem může být i zaměstnanec, a to i na zkrácený úvazek – ve druhé části úvazků může být zaměstnán u stejného zaměstnavatele, ale nikoliv na pozici, která by ohrožovala jeho nezávislost. Pokud bude pověřencem zaměstnanec, bude se jeho náplň práce a odměňování řídit dle nařízení vlády č. 302/2014 Sb., o katalogu správních činností, a nařízení vlády č. 222/2010 Sb., o katalogu prací ve veřejných službách a správě. Tato nařízení již k 1. 1. 2018 obsahují i pozici pověřence pro ochranu osobních ú

<sup>8</sup> tzv. Metodické doporučení k pověřenci, online:

dajú (v obecných úřadech obvykle 11. a 12. platová třída). Další možnosti vhodnout z důvodu nutnosti zachovat nezávislost pověřence může být například dohoda dvou obcí, kdy bude pro jednu obec dělat pověřence zaměstnanec druhé obce a obráceně,

- d) Pověřenec musí ovládat agendu ochrany osobních údajů, a to s přesahy do práva i IT, nemusí však mít žádné formální kvalifikační předpoklady. Jelikož hlavním požadavkem GDPR je jeho nezávislé fungování zaměřené na soulad praxe s GDPR, při výběru (zejména bude-li vykonáván na pozici zaměstnance) by měl být brán v potaz i osobnostní profil, zejména samostatnost, aktivita a přirozená autorita,
- e) Nejsložitější bude vybalancování faktické pozice pověřence s ohledem na zákaz úkolování pověřence v oblasti dozoru nad dodržováním GDPR a jeho faktickou nedotknutelností (zákaz –široce pojatého- sankcionování nebo propuštění za plnění jeho úkolů). Smlouva s pověřencem by se proto měla zaměřit na ošetření situací, kdy naopak sankce na místě jsou – střet zájmů, neplnění svých úkolů ze zákona, nedosažitelnost apod.,
- f) Pověřenec bude pravděpodobně podléhat povinnosti mlčenlivosti (o osobních údajích a k nim přijatým bezpečnostním opatřením), která bude trvat i po skončení jeho působení v pozici. Tato povinnost mlčenlivosti by se pak týkala i jeho případných podřízených. Jde o návrh části českého doprovodného zákona, který není v době dokončení této analýzy schválen, takže není jisté, zda bude zákonem tato právní povinnost stanovena. V rámci příprav se však obcím doporučuje zpracovat povinnost mlčenlivosti pověřence do smluv s ním uzavíraných. Takové ujednání nebude mít vliv na platnost smlouvy, i pokud bude stanoveno nad rámec úpravy v doprovodném zákoně.

Ustavení pověřence lze, a je dokonce vhodné, zajistit co

nejdříve, již před účinností GDPR, tedy ve fázi datových analýz a tvorby záznamů o zpracování, úpravy smluv, ev. souhlasů a ladění interních opatření. Časová náročnost pro ustavení pověřence není vysoká. Je ale nezbytné počítat s lhůtami obvyklými pro výběrové řízení, s přihlédnutím k faktu, že poptávka po pověřencích je vysoká a úroveň uchazečů bude různá. V případě využití pověřence sdíleného, nabízeného jako služba např. Sazem měst a obcí, je proces jednodušší. Je však třeba mít pečlivě připravené požadavky a konkrétní náplň práce s určenými konkrétními povinnostmi (mj. konkrétně určená dostupnost, lhůty pro vyřizování dotazů, dny určené pro konzultace atd). S ohledem na výše uvedené bude časová náročnost na definování způsobu zajištění, kritéria pro výběr, prvky smlouvy s pověřencem, určení eventuálního dalšího úvazku pověřence a provedení výběru zhruba měsíc až měsíc a půl. K počátku dubna by však obce (alespoň II. a III. typu) již měly mít pověřence ustaveného ve funkci.

Náplň práce pověřence je ponejvíce konzultační, školicí, poradenská a monitorovací (auditní). Dle GDPR a vodítek k pověřenci je jeho konkrétní náplní práce:

- poskytování informací a poradenství o povinnostech v celém rozsahu GDPR - správcům nebo zpracovatelům a zaměstnancům,
- poskytování poradenství, pokud jde o posouzení vlivu na ochranu osobních údajů (u obcí spíše nebude nutné),
- monitorování souladu s GDPR, tj. průběžná činnost dle koncepce a ad hoc potřeb,
- zvyšování povědomí a odborné přípravy pracovníků zapojených do operací zpracování a souvisejících auditů,
- spolupráce s Úřadem pro ochranu osobních údajů; má

být kontaktním místem pro pracovníky ÚOOÚ,

- fungování jako kontaktní místo pro subjekty údajů ve všem, co se týká zpracování osobních údajů a s výkonem práv subjektů údajů (na přístup, pozastavení, změnu, výmaz, přenositelnost atd.).

Náklady na činnost pověřence je třeba zahrnout do rozpočtů, jsou trvalé, nicméně pohybují se od několika set Kč měsíčně za externího pověřence od sdružení samospráv, po řádově desetisíce při zajištění formou zaměstnání pracovníka v této pozici či externí službu s vysokou přidanou hodnotou. Ustálilo se, že ceny pod deset tisíc Kč měsíčně u větších obcí a městských částí lze u externích poskytovatelů bez problémů dosáhnout.

Lze shrnout, že zajištění pověřence nepatří k nejnáročnějším povinnostem nutným pro dodržení GDPR a tuto povinnost lze do účinnosti GDPR pohodlně stihnout, přičemž náklady nemusí být vysoké, jsou však trvalé. Určitě je ale nutné věnovat kapacity pečlivému vyladění povinností pověřence i jeho výběru, vzhledem k tomu, že je jeho ustavení povinné a pozice silná. Určitě se vyplatí, aby byla supervize nakládání s osobními údaji zajištěna na vysoké úrovni.

### **III. ÚPRAVA SMLUV SE ZPRACOVATELI**

V oblasti kontraktace zpracování osobních údajů je situace různých obcí a to stejného typu, rozličná. Liší se jak co do velikosti zpracovatelů (má vliv na vyjednávací pozici podmínek smlouvy i jejich schopnost dosáhnout souladu s GDPR), tak co do rozsahu zpracovávaných agend, resp. osobních údajů. Potřebné kapacity a čas na úpravu smluv se tedy nedají všeobecně odhadovat, závisí na počtu upra-

vovaných smluv, stávající podobě smluv (zejména klauzule o garanci souladu řešení s aktuální legislativou v průběhu trvání kontraktu) i vyjednávací proceduře. V úvahu se musí vzít i časové hledisko s ohledem na nutnost výběrových řízení, pokud by obec dospěla k závěru, že bude třeba zpracování osobních údajů zajistit novým zpracovatelem a hledisko nejbližší účinnosti smlouvy až jejím zveřejněním v registru smluv. Nemálo zpracovatelů bude objektivně potřebovat čas na technické úpravy svých systémů k zajištění provádění povinností dle GDPR, což bude danost vyjednávání o dodacích smluv.

Ačkoliv by měla úprava smluv se zpracovateli následovat po provedení první fáze implementace GDPR, tj. datové analýzy a přípravy záznamů o zpracování, v době dokončení této analýzy, je třeba si uvědomit, že do účinnosti GDPR zbývají už jen čtyři měsíce, což není mnoho. Lze proto doporučit, aby obce, které ještě s úpravou smluv se svými zpracovateli nezačaly, zahájily současně s prováděním datové analýzy jednání se svými dodavateli, kteří zpracovávají osobní údaje. Výzva k předložení dodatku prvně zpracovatelem ostatně také napoví ohledně jeho připravenosti na GDPR. Smluvní zajištění je tvrdá povinnost daná GDPR (čl. 28 GDPR), formálně velmi dobře prokazatelnou, takže lze očekávat, že při případné kontrole budou ÚOOÚ zajímat smlouvy se zpracovateli na jednom z čelných míst.

Uvedení všech smluv do souladu s požadavky GDPR bude trvat řádově měsíce, pokud se budou povinnosti dané GDPR specifikovat podle druhu zpracování. U složitějších zpracování to bude nutné. Obcím lze doporučit (a na náročnost dopadů bude mít vliv):

- a) Využití pomocných materiálů jako je Příloha k této Analýze se vzory dokumentace, kde jsou obsaženy i potřebné povinné smluvní klauzule v univerzální podobě,

- b) Společný postup v rámci uskupení obcí na jakékoliv úrovni ve vztahu k velkým poskytovatelům, např. elektronické spisové služby,
- c) Zda může zpracovatel do úvah zahrnout i eventuální požadavky jiných právních předpisů, na prvním místě zákona o kybernetické bezpečnosti, pokud mu daná územní samospráva podléhá – tento zákon obsahuje požadavky na povinné smluvní klauzule s poskytovateli cloudových služeb<sup>9</sup>,
- d) U velkých poskytovatelů IT a zejména cloudových služeb, využívá-li je obec, lze využít připravenosti veskrze rychle pokrýt nejen technicky, ale i smluvně GDPR compliance,
- e) U stejných subjektů lze využít též podpory v GDPR poradenství, kterou někteří nabízí (většinou zdarma coby součást marketingu) či se inspirovat jejich smluvním řešením i pro smlouvy s jinými zpracovateli,
- f) Pamatovat na možnosti, které dává zatím nepřijatá legislativa a ošetřit je ve smlouvě pomocí podmínek, opcí, apod. (např. možnost zpracovatele zprostít pověřence povinnosti mlčenlivosti namísto správce (možnost v návrhu, jak obsahuje návrh zákona o zpracování osobních údajů)),
- g) Obdobně jako se zpracovateli bude třeba upravit i smlouvy s eventuálními společnými správci.

Dopad v podobě nákladů se odhaduje obtížněji, tuto fázi zatím většina obcí nerealizuje. Indikativně lze vycházet z kalkulace nákladů na kapacity vlastních zaměstnanců při zajištěním vlastním personálem a z hodinových sazeb služeb

<sup>9</sup> Vhodnou pomůckou pro naplánovaní procesů může být materiál Svazu měst a obcí pro implementaci GDPR nazvaný Karta procesu (online ke stažení pro členy SMO na [www.smo.cz](http://www.smo.cz))

poradenských společností, protože nejobvyklejší bude zřejmě zajištění kombinací jejich vstupu (příprava smluv externě, dojednávání a organizace kontraktace interně). Počítat s vytížením nemalé části kapacit svých právníků a obvykle i IT zaměstnanců a podpůrné administrativy je vhodné na dva až pět měsíců.

Obce by měly rovněž věnovat pozornost tomu, zda úpravu smluvní dokumentace, softwaru apod. nemají právo požadovat od svých dodavatelů zdarma v rámci tzv. legislativního maintenance, které je častou součástí smluv.

## **IV. ORGANIZAČNÍ OPATŘENÍ**

### **1. ŠKOLENÍ**

Proškolení by se mělo týkat všech zaměstnanců přicházejících do styku s osobními údaji, což je převážná část pracovníků úřadů územních samospráv. Bylo zjištěno, že k lednu 2018 absolvovala nějaký typ školení ke GDPR většina tajemníků obecních úřadů.

V rámci posledního čtvrtroku příprav by se měli proškolit nejlépe na počátku datové analýzy vedoucí odborů, aby mohli účinně spolupracovat při mapování agend. V dalším průběhu implementace je vhodné proškolit zaměstnance IT oddělení, aby měli představu o zásadách GDPR a potřebných opatřeních. Součástí tohoto školení by už nicméně měly být i konkrétní kroky, které bude nutné v IT oblasti provést. Na konci implementace GDPR, resp. před začátkem účinnosti GDPR, by měli absolvovat školení referenti a všichni, kdo zpracování osobních údajů vykonávají. Lze jim tak již předat více návodné postupy řešení.

Školení by mělo být prováděno někým nikoli zcela externím - ideální by bylo již angažování pověřence, velmi vhodné je školení od sdružení samospráv, výborná je samozřejmě i forma workshopů, kde se může vyměnit mnoho zkušeností s dobrou praxí tam, kde se provádí. Pokud je na implementaci GDPR najat externí dodavatel, měl by i školení provádět on a je vhodné smluvně zajistit, aby část školení věnoval odpovědím na dotazy na míru.

Není však problém provést jedno velké úvodní školení pro všechny zainteresované zaměstnance bez rozdílu pozic na počátku datové analýzy a poté know-how distribuovat více na míru podle průběhu implementace.

Nutná je dokumentace pro školení u všech pracovníků i s detaily školícího modulu – doložení přijatých opatření je součástí principu odpovědnosti dle čl. 5 odst. 2 GDPR. Některí školitelé na GDPR bývají akreditováni coby školitelé ministerstvem vnitra (osvědčuje jistou odbornost, minimálně díky povinným dobrozdáním od dalších odborníků v tématu), je to možné kritérium zakázky.

Vzhledem k výše uvedeném nejsou školící aktivity zvlášť časově náročné, je třeba je však začlenit do poptávkovo-vého/smluvního balíku při zajišťování pověřence/výběru externího implementátora/modelu spolupráce v rámci sdružení samospráv. Náklady se podle formy školení, lektorů, počtu účastníků či dalších požadavků mohou pohybovat v rozmezí tří až sedmi tisíc Kč za hodinu. Nemusí jít o zcela jednorázový náklad, GDPR požaduje pravidelné ověřování opatření na zajištění bezpečnosti osobních údajů (čl. 31 odst. 1 písm. d)) a v prvním období účinnosti je školení formou rozboru případů z praxe vhodné coby jeden z nástrojů plnění této povinnosti, zaměstnancům tak (při vhodné formě) nové povinnosti lépe utkví v paměti.

## 2. IT OPATŘENÍ

Opatření v oblasti IT lze považovat za nejnáročnější, jak časově, tak i finančně. Bude nutné posoudit, zda je níže uvedené IT opatření potřeba zavést v rámci stávajících produktů a systémů, které má úřad k dispozici, anebo je třeba pořízení zcela nového softwarového vybavení či rozšíření stávajících produktů o licence k dalším funkcionalitám či kombinací obou možností.

I zde se ke snížení náročnosti této obtížné fáze implementace velmi doporučuje sdílení informací s dalšími obcemi rámci sítí tajemníků obecních úřadů, obcí samotných apod., vhodná jsou společná jednání s velkými a zavedenými dodavateli, sdílení dobré praxe, benchmarking a podobně.

Pozor, je třeba dát na to, aby zavedená IT řešení nezpracovávala osobní údaje nadbytečně, nad rámec nutného, protože jakékoli zpracování osobních údajů, i to, které slouží k plnění povinností na poli ochrany osobních údajů dle GDPR, podléhá beze zbytku povinnostem z GDPR plynoucích.

Z právně-organizačního pohledu je třeba definovat, které nástroje a opatření na poli IT budou pro implementaci nezbytné. Následně bude nezbytné vypracovat ve spolupráci s IT odborem a zároveň ideálně již s pověřencem varianty řešení, dostupné produkty a řešení včetně různých možností zajištění. Po rozhodnutí vedení obce o volbě varianty řešení je třeba již se specialistou na veřejné zakázky připravit poptávku, bude-li řešení v pořízení IT zadáno externě. Základními požadavky GDPR ve vztahu k IT jsou zejména

- omezení účelem zpracování

- minimalizace zpracovávaných osobních údajů
- omezení jejich uložení jen na nezbytně nutnou dobu

Z uvedeného vyplývají hlavní obvyklé IT nástroje v následujícím výčtu:

- Zmapování nestrukturovaných dat (zejména e-maily, souborové servery, soubory v cloudových řešeních jako SharePoint či interní komunikační kanály) není neobvyklé (v instituci to bývá více než 50% dat) a týká se alespoň zjištění povahy osobních údajů v nich, zejména zda se tam nachází citlivé osobní údaje, a posuzuje se vhodnost nasazení speciálních softwarových nástrojů pro jejich mapování (obvykle výhledově, jsou dost nákladné), hlídá se indexování či i korekce<sup>10</sup> anebo řešení interními jednoduchými opatřeními (viz dále část pojednávající o možnostech u nejčastějšího typu těchto dat - e-mailů),
- Zmapování stávajících přístupů ke strukturovaným i nestrukturovaným datům (posouzení dotazovacích nástrojů u obou typů dat, jejich náročnosti a kompatibility zejména s ohledem na možnost práva na přístup k údajům – nutnost dotazování nad desítkami agend),
- Součástí dvou shora uvedených otázek je i posouzení vhodnosti zavedení omezení možnosti vyhledávání v agentách a hlavně nestrukturovaných datech,
- Nástrojem u strukturovaných dat (zjednodušeně řečeno dat v databázích), který doporučuje i GDPR, je i pseudonymizace osobních údajů – obec by měla posoudit, kde je třeba zavést. Mělo by se brát v potaz, že dle GDPR je

<sup>10</sup> Stanovisko WP 29 č. 2/2017 ke zpracování osobních údajů v zaměstnání

pseudonymizace standardní nástroj, takže rozhodně není vyhrazena jen pro citlivá data apod. Vhodná je všude, kde k některým operacím nebo po část doby zpracování není nutné jednoznačné určení osoby,

- Posouzení vhodnosti šifrování osobních údajů by se mělo provést zejména u citlivých osobních údajů, údajů na přenosných zařízeních (zejména notebooky, tablety) a podobně,
- Rychlosť a uživatelský komfort nástrojů pro řízení přístupů (přístupová práva budou vyplývat z datové analýzy a interních směrnic),
- Možnosti stávajících nástrojů dobře rozpoznávat a zveřejňovat data určená ke zveřejnění, ať již v rámci úředních desek nebo povinností v oblasti otevřených dat, a také je převádět do strojově čitelného formátu dle požadavků zákona i standardů pro otevřená data,
- U přenosných zařízení posouzení nastavení z hlediska bezpečnosti (zejm. prevence a řešení ztráty dat nebo zařízení) a oddělení oblasti soukromých/služebních dat v souladu s doporučeními WP29, ať již jde o možnosti užívání služebních mobilů, notebooků apod. k soukromým účelům či koncept využívání vlastních zařízení zaměstnanců pro služební účely (BYOD),
- Nezbytné je i zhodnotit stávající řešení zálohování, neboť právo být zapomenut (právo na výmaz osobních údajů) se vztahuje i na osobní údaje v zálohách.

Je zřejmé, že opatření v IT jsou náročná jak na mapování možností pro nejvhodnějším řešení, na samotné jejich zavedení včetně testování a nebude ojedinělá i nezbytnost

pořídit nový softwarový produkt nebo rozšířit stávající. Náklady na licence k software mohou být až vyšší statisíce, i když obvykle spíše menší částky. Odhad člověkohodin IT pracovníků se pohybuje rozhodně také ve stovkách. V této oblasti je zejména zřejmé, že do účinnosti GDPR nebude vše stoprocentně zajištěno. Nutná bude často prioritizace opatření, základními opatřeními bude řízení přístupu a správa zařízení. Doporučit lze určitě též prověřit plnění povinnosti logování (i nahlížecích) přístupů k osobním údajům – plyne už z dnešní legislativy, ale nebývá vždy plněna stoprocentně. ÚOOÚ s touto povinností pravidelně pracuje. Nebude neobvyklé, že navržené postupy v IT se budou realizovat postupně a až po účinnosti GDPR.

## **4. ÚPRAVA ČI TVORBA INTERNÍCH SMĚRNIC PRO NAKLÁDÁNÍ S OSOBNÍMI ÚDAJI**

Stanovení odpovědností za zpracování osobních údajů je prvním krokem před tvorbou směrnic. Vyplýne z mapování dat a stávajících přiřazení odpovědností v rámci organizační struktury. V interních směrnicích lze doporučit upravit

- procesy v případech nových institutů GDPR resp. i staronových, kde se právní úprava neplnila dokonale: co, kdo, kdy koná v případě realizace práv subjektů údajů na přístup, výmaz, opravu<sup>11</sup>,
- proceduru pro situace tzv. incidentů, zejména pak zajištění informování ÚOOÚ eventuálně i subjektů údajů (část odpovědnosti a role zpracovatelů a pověřence by měla být vtělena ve smlouvách s nimi),

<sup>11</sup> čl. 13 - 17 GDPR, případně též práva na omezení zpracování dle čl. 18 GDPR (práva na přenositelnost, námitka proti zpracování či proti automatizovanému zpracování nebudou u obcí ve většině případů relevantní).

- modelový souhlas se zpracováním osobních údajů, je-li u obce relevantní,
- modelové poučení subjektů údajů o zpracování dle čl. 13 a 14 GDPR, pro relevantní situace (situace by měly být začleněny do procesů),
- nutná jsou stanovení odpovědností konkrétních pozic a povinností zaměstnanců obecně (zde pak musí následovat skutečné, nejen formální seznámení, daných osob, a samozřejmě prokazatelné),
- praktičnosti směrnice pomůže i odkaz na interní předpisy související (spisový řád, bezpečnostní politika obecně, provozní řád IT), pomůže tak i souladu předpisů a vnitřní logice systému (typicky u skartace).

Není vhodné opisovat do směrnic text GDPR, zejména ne obecné zásady apod., mělo by jít o praktický dokument s konkrétními informacemi „kdo, kdy, jak“. Počítat je třeba i s dalšími úpravami v souvisejících vnitřních dokumentech včetně organizačního řádu.

Vzhledem k poměrně volným pravidlům pro vydávání a schvalování interních směrnic lze případně dopady na obce dávkovat a to příjetím směrnice upravující základní a nutné

záležitosti s tím, že její doplnění lze očekávat na základě zkušeností s realizací nových institutů a práv po účinnosti GDPR. I dozorový úřad počítá s postupným naplňováním GDPR a náplň směrnice lze na základě zkušeností rozvíjet o větší detaily.

Náročnost na kapacity je nižší, je však třeba počítat s průběžnou prací na směrnici, jak je popsáno výše, a obvykle i nutností prověřit ostatní stávající vnitřní přespisy na poli bezpečnosti, obsluhy informačních systémů, ale třeba i spisový řád (zejména skartační lhůty), jak je uvedeno výše. Nebude obvykle třeba zajistit tvorbu interních směrnic externí službou.

## **B. VYBRANÁ ČASTÁ A NEJEDNOZNAČNÁ ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ**

### **1. SPISOVÁ SLUŽBA**

Vedení spisové služby (rozuměj elektronické), na které již Ministerstvo vnitra vydalo metodiku, a zajištění, aby spisová služba fungovala v souladu s požadavky GDPR, se opírá o několik stěžejních doporučení:

- Provést revizi spisového a skartačního plánu, zejména skartačních lhůt, které by měly být v souladu se zásadou minimalizace stanoveny jen po nezbytně dlouhou dobu k uchovávání osobních údajů, případně je dát do souladu s GDPR,
- Pokud je výsledkem této revize závěr o tom, že některé typy osobních údajů, resp. dokumentů s nimi, nebude

možné dále uchovávat, je třeba pamatovat na povinnosti na úseku archivnictví a kontaktovat příslušný archiv pro umožnění výběru archiválií,

- Minimalizovat osobní údaje v obecně dostupných informacích (tj. informacích bez logování nahlížení),
- Zavést klasická technická opatření jako je pseudonymizace, omezení vyhledávání, úprava smluv se zpracovateli či řízení přístupů i v systému spisové služby pro naplnění požadavků GDPR,
- Využití práv osob na přístup k údajům do systému zaznamenávat, pamatovat na ochranu osobních údajů třetích osob (anonymizace) při poskytování,

Výslovné shrnutí právní situace: využití práva na výmaz osobních údajů nemůže obstát na neskartovaný dokument a na dokument po skartační lhůtě vybraný v následném procesu jako archiválie,

Doporučení k likvidaci dokumentů s osobními údaji (uplatní se i pro dokumenty mimo spisovou službu): odstranit se musí i metadata a záznamy ze záloh, pokud je záloha ne-digitální, musí se zajistit, že obnova neobnoví vyřazené osobní údaje a je ve speciálním důvěrném režimu.

Nad rámec metodiky Ministerstva vnitra lze doporučit zajistit u spisové služby také elektronickou skartaci.

## 2. E-MAILY

E-mailsy obsahují velké množství osobních údajů včetně citlivých, zároveň splňují podmínu automatizovaného vedení a nejsou tedy z působnosti GDPR vyňaty (GDPR nedopadá pouze na neautomatizované evidence, kde nejsou osobní

údaje přístupné podle zvláštních kritérií). Navíc samotné e-mailové adresy, zejména pokud jsou tvořeny jménem a příjmením (a to i pracovní), bývají často samy o sobě osobním údajem.

Stanoví-li se účel zpracování osobních údajů v e-mailech, je to vedení korespondence, které vyplývá z mnoha výslovných či implicitních povinností územních samospráv. Pro provedení zásady minimalizace osobních údajů (čl. 5 písm. c) pověřenec GDPR) bude nevhodnějším postupem zaměřit se na přílohy coby zdroj mnoha osobních údajů, často i citlivých a komplexních (např. CV).

Obec si může interní procesy nastavit tak, že

- a) interním předpisem uloží každou relevantní přílohu „zpracovat“ tj. zejména uložit do příslušné složky agendy,
- b) nastaví automatické odstranění (nevratné smazání) příloh po určité době, např. 6 měsících,
- c) úpravu metodik u e-mailů v úřadě lze využít i pro přenastavení politik, které dělají na poli ochrany osobních údajů také problém – a to e-mailové adresy zaměstnanců. Pokud jsou tvořeny jménem a příjmením, půjde o osobní údaj spadající pod pravidla GDPR. V případě adresy tvořené nikoli jménem, ale např. pozicí (poverenec@urad.cz) se vyřeší jak problém se zbytnou kategorií osobních údajů tvořících e-mailové adresy, tak se zastupitelností pracovníků,
- d) s tím souvisí doporučení WP 29 týkající se zpracování osobních údajů v zaměstnání<sup>12</sup>, kde se u různých typů

<sup>12</sup> stanovisko WP 29 č. 2/2017 ke zpracování osobních údajů na pracovišti, online:

[https://www.uouou.cz/assets/File.ashx?id\\_org=200144&id\\_dokumenty=28680](https://www.uouou.cz/assets/File.ashx?id_org=200144&id_dokumenty=28680)

zpracování a technologií opakovaně zdůrazňuje právo zaměstnanců na zachování ochrany soukromého života i v zaměstnání. Kontrola zaměstnavatele, co do obsahu korespondence, aktivit online apod. je i na zařízeních zaměstnavatele nutně omezená. Zájmy zaměstnavatele doporučuje WP29 zohlednit řešením, které se jeví velmi praktické a lze doporučit zavést i u zaměstnavatelů - územních samospráv, a to vyhradit zaměstnancům určitý prostor (na pevném disku, ve složce pošty apod.) pro soukromé aktivity, kam je přístup zaměstnavatele omezený, zatímco v ostatním bude právo zaměstnavatele na kontrolu vyšší.

Uvedená doporučení ohledně nastavení e-mailové politiky je třeba realizovat nejen pomocí organizačních opatření (směrnice), ale je nutné provést změny v informačních systémech a zejména pak průběžně kontrolovat a trvat na jejich zařízení. Je možné se domnívat, že v době účinnosti GDPR by již mohlo být reálné mít připravenou novou směrnici a běžící nebo dokončené úpravy v nastavení v IT systémech. Zásadní bude proškolení a pevné zavedení v rámci úřadu. Dá se předpokládat, že ÚOOÚ nebude v první fázi kontrol požadovat stoprocentní zajištění souladu s GDPR i v nestrukturovaných datech typu e-mailů, mj. i proto, že vodítka WP29 nebyla a nejsou k dispozici v dostatečném předstihu před účinností GDPR. Vyhledově do budoucna se však změny doporučují.

### **3. NEAUTOMATIZOVANÉ ZPRACOVÁNÍ**

Celá analýza pojednává o automatizovaném zpracování osobních údajů, které je dnes převažující realitou ve většině agend u většiny obcí. V plánování příprav na GDPR je však třeba myslet i na opatření v oblasti zpracování tzv. pa-

pírového či obecněji analogového (např. osobní údaje na magnetických páskách).

Nejnáročnější částí bude zřejmě zmapování těchto přetravajících agend u větších obcí, zavedení odpovídajících organizačních opatření (např. řízení přístupu, bezpečnost), která jsou oproti digitální podobě osobních údajů většinou snazší.

Lze spíše očekávat, že pravidla pro skartaci, umisťování analogových dokumentů jsou historicky vžitá a obvykle nebude třeba zásadních změn.

## **C. NOVÉ MÉNĚ RELEVANTNÍ INSTITUTY GDPR – ČEMU SE OBCE VYHNOU:**

Potřebná je i rekapitulace nových povinností daných GDPR, která naopak pro naprostou většinu obcí relevantní nebude (nemusí to však platit o organizacích jimi zřizovaných, viz informace níže v textu), a proto není potřeba je poptávat do školení, implementaci nebo je jinak významněji zahrnovat do plánů implementace.

### **1. PORTABILITY**

Dobrou zprávou pro územní samosprávu je, že nový institut

přenositelnosti osobních údajů (čl. 20 GDPR) se jich z 99 % nebude týkat. Samotné nařízení totiž vylučuje z této povinnosti (čl. 20 odst. 3) zpracování nezbytné pro splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci.

Zajištění povinnosti přenositelnosti osobních údajů se tak bude týkat buď atypických činností v rámci samostatné působnosti anebo v příspěvkových organizacích. Musí jít o osobní údaje poskytnuté samotným subjektem údajů na základě souhlasu anebo pro plnění smlouvy a jde-li zároveň o automatizované zpracování. Portabilita tak tedy dopadne určitě na větší knihovny.

## **2. ZVLÁŠTNÍ PODMÍNKY TÝKAJÍCÍ SE OSOBNÍCH ÚDAJŮ DĚTÍ**

Samotné obce nebudou muset řešit také speciální povinnost získat namísto dítěte mladšího 13 let (jak určuje věkovou hranici český návrh doprovodného zákona) souhlas jejich zákonného zástupce. Týká se totiž jen nabídky služeb informační společnosti (přenos dat, připojení, ale i různé sociální sítě, aplikace apod.), což je v kombinaci s cílením na děti u obce i v samostatné působnosti nepravděpodobné.

Je však třeba mít na paměti, že pokud by v rámci podpory své činnosti nabízeli různé online aplikace příspěvkové or-

ganizace jako je sportovní či kulturní zařízení obce, školy a podobně, je nezbytné si obstarat prokazatelným způsobem souhlas zákonného zástupce. Výjimkou jsou dle GDPR jen preventivně poradenské online služby pro děti, aby byl zachován jejich smysl.

Pro jakékoli jiné zpracování platí u dětí dvě zásady, a to že právní titul zpracování z důvodu zájmu správce či třetí osoby je u dětí posuzován ještě přísněji vůči zásahu do jeho práv a že případné zpracování osobních údajů dětí musí plnit řadu informačních povinností dle čl. 13 a 14 GDPR formou dětem přístupnou (i zde je však vyňato zpracování ze zákoněho titulu a další situace).

### **3. ANALÝZY HODNOCENÍ DOPADŮ ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ (DPIA)**

Tento nový resp. nově formalizovaný institut dle čl. 35 GDPR nastupuje pouze v případě, že určitý druh zpracování bude mít za následek vysoké riziko pro práva a svobody fyzických osob. Ač se doporučuje začlenit rizikovost zpracování, která vyplývá zejména z kategorie osobních údajů či závěrů, kterých se zpracováním dosáhne, již do fáze datové analýzy a tvorby záznamů o zpracování, nemusí být povaha vysokého rizika vždy jasná. GDPR také svěřuje národním zákonodárcům možnost prohlásit určité druhy zpracování za jednoznačně vysoce rizikové a tedy podléhající DPIA anebo naopak výčtem určit druhy zpracování, které DPIA vylučují. V aktuálně známé podobě návrhu doprovodného zákona se tyto výčty neobjevují. Pro územní samosprávu u většina zpracování probíhá na základě zákona a vychází se z toho, že zákonodárce si již před přijetím rizika zanalyzoval (u nás je od roku 2012 součástí důvodové zprávy dopad na ochranu soukromí). Pozornost je třeba u obce spíš zaměřit dovnitř – na systémy kontroly či automatizovaného hodnocení

zaměstnanců – kritéria lze celkem návodně najít v Pokynech WP29 pro DPIA.

V posuzování dopadů je třeba vzít v potaz i doporučení WP 29, aby byla DPIA či alespoň její závěry obsahující doporučení zveřejněna (naplňuje se tak princip transparentnosti daný čl. 5 i dalšími částmi GDPR). Tuto povinnost by měla obec mít na paměti, nepředstavuje téměř žádnou zátěž časovou či jinou.

Pokud se týká organizací spadajících pod obec, nejčastěji bude DPIA podléhat kamerový systém městské policie a jeho parametry. Spadá pod pojem systematického monitorování veřejných prostorů, často již i s moduly pro automatizované rozpoznávání osob, nestandardního chování apod. Tyto činnosti obvykle budou spadat pod povinnost DPIA a bude tak nutné posoudit rizika. Ani zde by neměla být DPIA formální výrobou nějakého dokumentu, ale pozitivním posouzením, např. zda rizikovost tohoto zpracování nepovede i k přehodnocení nasazení technologie oproti „neautomatizovanému“ řešení návratu více policistů nebo strážníků do ulic apod.

## **ZDROJE:**

- Materiály MV; [www.mvcr.cz/gdpr](http://www.mvcr.cz/gdpr)
- Materiály WP 29;  
[http://ec.europa.eu/newsroom/just/item-detail.cfm?item\\_id=50083](http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083).
- V češtině jsou dokumenty WP 29 dostupné zde:  
<https://www.uouou.cz/pracovni-skupina-wp29-vydala-tri-dokumenty-k-obecnemu-narizeni-o-ochrane-osobnich->

udaju/d-21750

- Hlavní dopady GDPR na obce, z výzkumného projektu VŠE IGS F5/65/2017 „Změny v úkolech obcí v důsledku změn českých a evropských právních předpisů“,

<http://denik.obce.cz/clanek.asp?id=6736785>

- Materiál

[https://ictrevue.ihned.cz/c3-65720560-0ICT00\\_d-65720560-aby-mohly-byt-udaje-zapomenuty-musi-byt-nejprve-nalezeny](https://ictrevue.ihned.cz/c3-65720560-0ICT00_d-65720560-aby-mohly-byt-udaje-zapomenuty-musi-byt-nejprve-nalezeny)

- Materiály ÚOOÚ; [www.uouu.cz](http://www.uouu.cz)

## **ZKRATKY:**

- GDPR – Obecné nařízení o ochraně osobních údajů - Nařízení (EU) 2016/679
  - WP 29 – Pracovní skupina zřízená Evropskou komisí, která vydává dokumenty, které mají poskytnout výklad novinek zaváděných obecným nařízením o ochraně osobních údajů.
  - DPIA – Data Protection Impact Assessment neboli česky Posouzení vlivu na ochranu osobních údajů. Jde o nástroj, který napomáhá správcům a zpracovatelům uvést zpracování osobních údajů do souladu s GDPR.

# **MANUÁL SE VZORY DOKUMENTŮ K IMPLEMENTACI GDPR PRO OBCE**

Tento manuál je určen zejména pro menší obce. Ty, které se rozhodnou zajistit si přípravu na GDPR samy, ale i ty, které využijí externích služeb a rády by měly podklady pro sestavení poptávky, kontrolu a srovnání nabídek.

Manuál je pojat prakticky - poskytuje konkrétní vzory a shrnuje postupy ve třech resp. čtyřech nejdůležitějších krocích přípravy: tvorba záznamů o zpracování, resp. v případě „obohacených záznamů o zpracování“ provedení datové analýzy, úpravu smluv se zpracovateli a nové instituty souhlasu.

# **VZOR OBOHACENÉHO ZÁZNAMU O ZPRACOVÁNÍ**

Proti povinnému záznamu o zpracování dle GDPR je počet informací zásadně rozšířen, má to však smysl – při jednom mapování dat se nashromáždí další údaje, které velmi pomohou při plnění dalších povinností. Záznamy o zpracování v této podobě znamenají provedení velké části mapování dat. Hvězdičkou jsou označeny informace, které mají návaznost na nějakou z povinností dle GDPR, ve vedlejším sloupci je tato povinnost odkázána.

Základ – informaci o všech zpracováváních (resp. zjednodušeně agendách) obec může získat ze stávajících přehledů, které má k dispozici: organizační řád, spisový a skartační řád, oznámení o vykonávání působnosti v agendě pro registr práv a povinností.

**Název zpracování**  
Název a popis informačního systému

**Hl.povinnost**

\*Forma zpracování:  
listinná/elektronická/elektronická – smlouva dle § 4 odst. 5  
á v clodu/obrazová (L/E/C/O) zákona o kybernské bezpečnosti

O jakou jde skupinu subjektů  
údajů (např. zaměstnanci)

Vyjmenování osobních údajů,  
které se zpracovávají (konkrétní  
položky)

Druh zpracování (např.  
shromažďování, vyhledávání,  
uchovávání, zveřejňování,  
profilování)

\*Je externí zpracovatelem? (A/N)  
Pokud ano, jeho identifikace

Pracovní pozice odpovědná za  
dané zpracování (návaznost na  
vnitřní směrnici)

\*Jde o společné zpracování více  
správci? (A, N) Pokud ano,  
identifikace společného správce.

\*Účel zpracování (popis, oč jde)

\*Právní titul (čl. 6+9)

\*Pokud je titulem souhlas, kde a  
jak je uchováváno jeho  
prokázání

\*Je přítomna nabídka online  
služeb dětem pod 13 let? Pokud  
ano, jak je zajištěn a uchován  
souhlas zákonného zástupce, jak  
je ověřen?

A – zejm. smlouva dle čl. 28  
GDPR

Brát v potaz omezení při přidání  
jiného účelu (čl. 6 odst. 4)  
Zejm. dopady souhlasu, smlouvy  
na portability, odvolání souhlasu,  
plnění zákonné povinnosti vede  
k odpadnutí povinnosti DPPA  
apod.

Čl. 8

Fyzické umístění osobních údajů  
Doba uchovávání a čím je daná

*Dochází k automatizovanému rozhodování či profilování? (A/N)	Čl. 21 a 22 Odmítnutí subjektem znamená ukončení platnosti titulu opráv. zájmu
*Dochází k přímému marketingu? (A/N) Průměrné počty zpracovávaných subjektů Kdo má k osobním údajům přístup? (přístupové skupiny) Popis zabezpečení (fyzické – např. Ochrana budovy, ale i organizační – hesla, pseudonymizace, šifrování)	dopad zejm. na posuzování rizika
*Jak se zajistí právo na přístup? (popsat tj. náročnost + možnost hledat NAD systémy) (možná návaznost na interní směrnici)	Čl. 15, zavést proces Dopad hl. na DPIA čl. 35 a info při incidentu čl. 34
*Rizikovost zpracování (N/S/V) *Původ osobních údajů – od subjektů samotných/jinde (SUBJ/JIN) Zajištění práva na přístup, opravu, výmaz (popis procesu, ev. návaznost na směrnice) Jak bude ověřena totožnost žadatele při žádosti o přístup atd.? Chceme kontakt/autentizaci dopředu? Dochází k předávání 3.osobě? Pokud ano, vyjasnit roli, titul atd.	Rozdílné informování subjekt dle čl. 14 a 15
*Dochází k předávání do zahraničí? Pokud ano, kam a jak je OOU zajištěna?	též dopad na povinnost komunikacev případě odvolání souhlasu, incidentu (zejm. čl. 19) HI. čl. 44 an. u třetích zemí
*Posouzení, zda poskytnutí kopie neovlivní práva 3. osob (A/N) a ev. zda účtovat poplatek Čl. 14 odst. 4 Další poznámky	

# **VZORY SMLUVNÍCH KLAUZULÍ A TIPY PRO TVORBU SMLUV/DODATKŮ SMLUV SE ZPRACOVATELI**

Tyto smluvní klauzule jsou připraveny pro modelovou smlouvu realizovanou v ČR, bez zahraničního prvku; odkazy na „právní předpisy“ se tedy myslí zejména zákon o zpracování osobních údajů (aktuálně ve stadiu návrhu) či jiné speciální předpisy českého právního rádu. Odkaz na konkrétní ustanovení GDPR v této smlouvě jen v případech, kdy je „didakticky“ vhodné nebo poprvé zmíněn určitý institut dle GDPR. Smluvní vzor počítá s automatizovaným zpracováním osobních údajů (ale lze jej využít s malými úpravami i pro manuální zpracování).

Bez znalosti konkrétního smluvního vztahu jsou zde uvedené klauzule nutně obecnější a některé se nemusí uplatnit (např. povinnost informovat subjekt údajů v případě incidentu, který nepředstavuje riziko pro práva a svobody subjektu údajů). V případě různých druhů zpracování resp. i různých kategorií osobních údajů je vhodné příslušné povinnosti správce/zpracovatele upravit na míru každému konkrétnímu zpracování v oddělených částech smlouvy.

Varianty úpravy smluvních vztahů jsou označeny buďto označením VAR A/B atd. anebo kurzívou v textu, kde jsou varianty odděleny lomítkem (eventuálně doprovázeny vyšvětlujícím textem kurzívou v závorce).

Ze zde uvedených klauzulí lze zkonstruovat i zcela novou smlouvu, nahrazující předešlou. Výběr postupu závisí především na obsahu původní smlouvy a náročnosti definování ustanovení, které se mění/nemění). Označení „subjekt

údajů“ lze nahradit označením „klient“ apod. dle původní smlouvy, úzu vztahů mezi správcem a zpracovatelem či jejich dalšími smluvními vztahy se subjekty údajů.

Zavedené zkratky:

- „správce“
- „zpracovatel“
- „osobní údaje“ (rozuměj údaje upravené touto smlouvou definované v úvodních ustanoveních)
- „smlouva“ (původní smlouva)
- „dodatek“ (aktuální dodatek, kterým se případně mění původní smlouva)
- „strany smlouvy“ (správce i zpracovatel)

## **Účel**

Účelem tohoto dodatku/této smlouvy je stanovit resp. doplnit podmínky, za kterých zpracovatel bude provádět pro správce zpracování osobních údajů tak, aby obě strany smlouvy dodržely všechny povinnosti plynoucí každé z nich z nařízení EU č. 2016/679 (dále jen GDPR) a z příslušných právních předpisů.

## **Popis zpracování osobních údajů**

(1) Zpracovatel je oprávněn zpracovávat jménem správce nezbytné osobní údaje pro poskytování následujících služeb:

(2) Účelem zpracování je \_\_\_\_\_

(3) Zpracovávané osobní údaje zahrnují (detailní popis, lze i pseudonymizovaná ukázka datasetu apod.) (dále jen „osobní údaje“).

(4) Kategorie subjektů údajů jsou (detailní popis, zejména mající vliv na posouzení rizika – např. dětští klienti do 15 let, jejich zákonné zástupci, pacienti, kterým jsou poskytovány zdravotnické služby v oblasti ....).

(5) Zpracovávání osobních údajů dle této smlouvy zahrnuje tyto operace a postupy (detailně popsat, je možné odkázat na přílohu, kde bude přehledně a detailně, ev. provázáno s povinnostmi správy a údržby systému apod.).

(6) Doba trvání zpracování osobních údajů je vymezena (definovat časový úsek, jde-li o jednorázové, či nepravidelné či formulovat jako dobu neurčitou - "po dobu účinnosti této smlouvy" apod.)

(7) K zajištění shora uvedených služeb bude správce poskytovat zpracovateli následující informace (detailní popis procesů) jednorázově/pravidelně v intervalech/na vyžádání.

### **Základní povinnosti zpracovatele**

(1) Zpracovatel se zavazuje

- a) zpracovávat osobní údaje pouze pro účely této smlouvy,
- b) zpracovávat osobní údaje v souladu se závazky v této smlouvě a s instrukcemi správce,
- c) bez odkladu informovat správce, pokud má za to, že jeho instrukce je v rozporu s GDPR nebo právními předpisy upravujícími ochranu osobních údajů,
- d) (VAR) pokud je zpracovatel povinen zasílat osobní údaje mimo EU nebo mezinárodní organizaci, musí zpracovatel informovat správce o právním základě této povinnosti před zahájením zpracování osobních údajů,
- e) zajistit důvěrnost zpracovávaných osobních údajů

ve smyslu čl. 5 odst. 1 písm.f) GDPR,

(2) Zpracovatel je dále povinen zajistit, aby zaměstnanci či jiné osoby pověřené zpracovatelem k nakládání s osobními údaji

a) byli zavázáni k mlčenlivosti, nemají-li povinnost mlčenlivosti ze zákona

b) byli odpovídajícím způsobem proškoleni

c) měli přístup k osobním údajům jen ve zcela nezbytném rozsahu.

(3) Zpracovatel je dále povinen zajistit v maximální možné míře standardní ochranu osobních údajů dle čl. 25 GDPR, zejména pak VAR: např. minimalizaci zpracovávaných osobních údajů a pseudonymizaci, šifrování (konkrétně rozepsat opatření odpovídající vyhodnocenému riziku).

(4) Zpracovatel je povinen kdykoli správci doložit, že splňuje požadavky dané touto smlouvou a požadavky právní úpravy účinné k danému okamžiku. Doložení může prokázat na pokyn správce i jiné další osobě, úřadu nebo instituci v rámci dozoru, provádění auditů apod.

(5) Zpracovatel se zavazuje k součinnosti při provádění auditů zpracování osobních údajů (VAR: lze upravit minimální lhůty oznamení předem apod.).

## **Možnosti subkontraktace**

### **VAR A**

Zpracovatel může pověřit určitými operacemi zpracování/zpracováním jiného dalšího zpracovatele (subkontraktovat). V tomto případě je povinen předem správce písemně informovat o zamýšlených detailech svěření zpracování dalšímu zpracovateli. Toto oznámení musí zejména zahrnovat

informace, jaké operace zpracování jsou subkontraktovány, jméno a účinné kontaktní údaje dalšího zpracovatele a časové podmínky subkontraktu. Správce může ve lhůtě \_\_\_\_\_ týdnů od doručení tohoto oznámení zakázat zamýšlené subkontraktování; pokud se nevyjádří, předpokládá se, že souhlas k subkontraktování udělil/neudělil.

## **VAR B**

- (1) Zpracovatel je oprávněn zapojit \_\_\_\_\_ (jméno, kontakty, identifikace) coby dalšího zpracovatele ve smyslu čl. 28 GDPR k zajištění těchto operací zpracování: \_\_\_\_\_
- (2) Zpracovatel může zapojit do zpracování dalšího zpracovatele jen s předchozím písemným schválením správce pro konkrétního dalšího zpracovatele.

Následné ustanovení, platné pro obě varianty:

- (1) Další zpracovatel bude zavázán ke stejným povinnostem jako zpracovatel dle této smlouvy, GDPR a dalších právních předpisů.
- (2) Další zpracovatel bude zavázán řídit se instrukcemi správce.
- (3) Zpracovatel je odpovědný za to, že další zpracovatel poskytne stejné záruky v podobě technických a organizačních opatření tak, aby zpracování splňovalo požadavky GDPR a dalších právních předpisů. Pokud další zpracovatel poruší tyto požadavky, trvá odpovědnost včetně smluvních sankcí zpracovatele vůči správci, který je oprávněn ji po zpracovateli vyjmáhat.

Práva subjektu údajů na informace a přístup k osobním údajům

## **VAR A (získání osobních údajů přímo od subjektů údajů)**

Zpracovatel se zavazuje informovat subjekty údajů podle čl. 13

GDPR v okamžiku získání osobních údajů. Znění a podoba této informace musí být předem schváleny správcem.

### **VAR B (získání osobních údajů jinde než u subjektů údajů a neplatí výjimky čl. 14 odst. 5)**

Zpracovatel se zavazuje informovat subjekty údajů podle čl. 14 GDPR nejdéle do \_\_\_\_ (max. 30 dnů od získání OU) od získání osobních údajů/nejpozději při první komunikaci se subjektem údajů/nejpozději při prvním zpřístupnění osobních údajů jinému příjemci.

### **Výkon oprávnění subjektů údajů**

Zpracovatel se zavazuje k maximální součinnosti správci při plnění povinnosti správce zajistit subjektu údajů na žádost realizaci práv:

- a) práva na přístup ke svým osobním údajům dle čl. 15 GDPR,
- b) práva na opravu svých osobních údajů dle čl. 16 GDPR,
- c) práva na výmaz osobních údajů dle čl. 17 GDPR,
- d) práva na omezení zpracování dle čl. 18 GDPR,
- e) práva namítat zpracování osobních údajů dle čl. 21 GDPR,
- f) práva namítat zpracování dle čl. 21 GDPR,
- g) práva na přenositelnost údajů dle čl. 20 GDPR,
- h) práva namítat automatizované rozhodování včetně profilování dle čl. 22 GDPR.

### **VAR A**

Pokud subjekt údajů zašle požadavek na využití některého z práv shora uvedených zpracovateli, zpracovatel jej zašle bez zkoumání oprávněnosti bez prodlení/do \_\_\_ správci na kontaktní e-mail/jiný prostředek komunikace \_\_\_\_\_.

## **VAR B**

Pokud subjekt údajů zašle požadavek na využití některého z práv shora uvedených zpracovateli, zavazuje se zpracovatel ve lhůtách a za podmínek stanovených GDPR vyřídit požadavek subjektu údajů. Tato povinnost platí i v případě subkontraktace zpracování osobních údajů.

Ohlašování případů porušení zabezpečení osobních údajů

## **VAR A**

Zpracovatel se zavazuje oznámit správci jakékoli porušení zabezpečení osobních údajů (dále jen „incident“) nejpozději do \_\_\_ hodin (max. 72 hodin pro správce od jeho informování) na kontaktní e-mail/jiný prostředek komunikace \_\_\_\_\_. K tomuto oznámení je zpracovatel povinen připojít veškerou dokumentaci ev. jí jinak zpřístupnit správci.

## **VAR B**

(1) Zpracovatel se zavazuje po předchozím souhlasu správce splnit povinnost ohlásit jménem správce incident údajů Úřadu na ochranu osobních údajů bez zbytečného odkladu, nejdéle však do 72 hodin od zjištění incidentu. Zpracovatel je povinen správce informovat i o incidentech, u kterých je nepravděpodobné, že by představovaly rizika pro práva a svobody subjektu údajů.

(2) Oznámení incidentu musí

- popsat povahu incidentu včetně kategorií a přibližného počtu subjektu údajů, kterých se incident týká, a přibližný počet

dotčených záznamů,

- obsahovat jméno a kontaktní údaje pověřence pro ochranu osobních údajů nebo jiné kontaktní osoby, která může poskytnout více informací,
- popsat možné následky incidentu,
- popsat přijatá protiopatření včetně opatření na zmírnění nepříznivých následků.

(3) Pokud není možné všechny shora uvedené informace poskytnout najednou, musí zpracovatel poskytnout dané informace postupně bez zbytečného odkladu od jejich získání.

(4) Po souhlasu správce/ zpracovatel uvědomí jménem správce dotčené subjekty údajů o incidentu v případě, že incident představuje pro subjekty údajů vysoké riziko pro jejich práva a svobody.

(5) Informace subjektu údajů podle odstavce výše musí srozumitelným způsobem minimálně:

- popsat povahu incidentu včetně kategorií a přibližného počtu subjektu údajů, kterých se incident týká a kategorií a přibližný počet dotčených záznamů,
  - obsahovat jméno a kontaktní údaje pověřence pro ochranu osobních údajů nebo jiné kontaktní osoby, která může poskytnout více informací,
  - popsat možné následky incidentu,
  - popsat přijatá protiopatření včetně opatření na zmírnění nepříznivých následků.
- Povinná součinnost zpracovatele správci

(1) Zpracovatel se zavazuje k nutné součinnosti

- a) při zpracování DPIA,
- b) při předběžné konzultaci s Úřadem na ochranu osobních údajů dle čl. 36 GDPR,
- c) (není povinné dle GDPR, může být vhodné u běžících zpracování) při přípravě či změnách záznamů o zpracování osobních údajů dle čl. 30 GDPR, zejména je povinen
  - i) písemně vést jméno a kontaktní údaje správce, případných dalších zpracovatelů a případného pověřence ochrany osobních údajů,
  - ii) kategorie zpracování osobních údajů,
  - iii) případné poskytování osobních údajů do zemí mimo EU s dokumentací přijetí odpovídajících záruk,
  - iv) je-li to možné, popis technických a organizačních bezpečnostních opatření.

(2) Zpracovatel se dále zavazuje správce bez odkladu informovat o každém

- a) požadavku na zpřístupnění osobních údajů od orgánů veřejné moci včetně orgánů činných v trestním řízení,
- b) dotazu či šetření Úřadu na ochranu osobních údajů týkající se osobních údajů dle této smlouvy.

### **Bezpečnostní opatření**

Zde uvedené povinnosti je vhodné specifikovat blíže (pokud již není v původní smlouvě) např. podle standardních SLA (service-level agreement) klauzulí smluv o poskytnutí software, software as a service apod. – např. minimální dostupnost helpdesku,

doba odezvy, úroveň zabezpečení dle zavedené klasifikace. Dané povinnosti je velmi vhodné specifikovat časově a navázat na snížení odměny či smluvní sankce.

Zpracovatel se zavazuje zajistit minimálně tato bezpečnostní opatření vůči zpracovávaným osobním údajům:

- a) pseudonymizace a šifrování osobních údajů,
- b) zajištění trvalé důvěrnosti, integrity, dostupnosti a odolnosti systémů pro zpracování osobních údajů,
- c) v případě technických či fyzických problémů obnovit dostupnost osobních údajů,
- d) zavést pravidelné testování a hodnocení účinnosti technických a organizačních bezpečnostních opatření a prokázat je na vyžádání správci.

### **Povinnosti zpracovatele při ukončení zpracování**

(1) Zpracovatel se zavazuje při ukončení zpracování z důvodu \_\_\_\_ zlikvidovat osobní údaje/vrátit všechny osobní údaje správci/předat osobní údaje jinému zpracovateli určenému správcem.

(2) Zároveň je zpracovatel povinen zlikvidovat všechny kopie osobních údajů v informačních systémech zpracovatele/osobní údaje v záložních kopiích až po potvrzení správce/jiného zpracovatele o úspěšném ukončení migraci dat.

### **Povinnosti správce**

#### **Správce se zavazuje**

- a) Poskytovat zpracovateli osobní údaje ke zpracování,
- b) Zpracovatele instruovat výhradně písemně,

- c) Zajistit splnění svých povinností vyplývajících z GDPR,
- d) Dohlížet na zpracování včetně provádění auditů a kontrol u zpracovatele.

### **DOPORUČENÍ K DALŠÍM USTANOVENÍM SMLOUVY:**

V případě zpracování osobních údajů (nejen jich) v cloudu, nastává relativně nová povinnost dle § 4 odst. 5 zákona č. 181/2014 Sb., o kybernetické bezpečnosti a smlouva s poskytovatelem cloudu musí povinně obsahovat:

zakotvení povinnosti poskytovatele cloudu zohlednit bezpečnostní politiky obce,

stanovení úrovně poskytovaných služeb, tj. SLA klauzule,

systém schvalování subdodavatelů služby cloud computingu obcí,

podmínky ukončení smluvního vztahu z pohledu bezpečnosti,

řízení kontinuity činností v souvislosti s poskytovanou službou cloud computingu,

určení vlastníka uchovávaných dat,

dohoda o důvěrnosti smluvního vztahu (NDA klauzule, nebude tedy zveřejněno ani v registru smluv),

stanovení úrovně ochrany dat z pohledu důvěrnosti, dostupnosti a integrity,

pravidla zákaznického auditu,

stanovení povinnosti poskytovatele cloudu informovat obec o kybernetických bezpečnostních incidentech.

## **Komunikace stran, dokumentace**

určení osob na každé straně smlouvy, včetně rychlých kontaktních údajů (v případě existence pozice pověřence pro ochranu osobních údajů u správce bude na straně správce pověřenec)

kontaktní údaje musí umožňovat velmi rychlou, pokud ne nepřetržitou dostupnost (zejména s ohledem na oznamovací povinnosti u incidentů)

## **Následky neplnění povinností zpracovatele**

zvážit doplnění, zvýšení smluvních pokut

v tomto případě výslovně umožnit započitatelnost pokut vči odměně za zpracování

zavedení prokázaného porušení povinností zpracovatele coby výpovědního důvodu smlouvy/důvodu odstoupení od smlouvy

upravit, pokud již není, porušení povinností i do výše odměny (např. model SLA ohledně dostupnosti dat, služeb apod.)

## **Ustanovení o odměně zpracovatele**

doplnit o možnosti snížení odměny při porušení SLA apod.

předmětem vyjednávání bude zřejmě i navýšení celkové odměny proti původní smlouvě v důsledku nových povinností (paušálně/podle hodin práce na součinnosti v méně obvyklých případech nezaviněných zpracovatelem apod.)

předpokládáme i jednání o tom, kdo hradí náklady na provedení různých povinností dle této smlouvy (jedna z variant je paušalizování v odměně a výslovné vyloučení dalších nákladů k tíži správce)

## **Účinnost a trvání dodatku/smlouvy**

účinnost dodatku nemusí být 28.5.2018, ale klidně i dříve

prakticky jediná povinnost, která zanikne k 28.5.2018, je povinnost registrace zpracování osobních údajů u UOOÚ, doporučujeme tuto povinnost v původní smlouvě, je-li, ošetřit rozvazovací podmírkou/zánikem účinnosti této části smlouvy k 28.5.2018

dodatek/resp. celou smlouvu zvolit na dobu neurčitou/určitou/automatická prolongace v závislosti na podmírkách plnění povinností/opce na prolongaci apod.

nezapomenout na klauzuli o přetrvání určitých povinností i po ukončení smlouvy (např. mlčenlivost), nejlépe obecnou formulací o povinnostech z povahy věci přežívajících trvání smlouvy

## **Ostatní vhodné klauzule**

zvážit, zda jsou dobré ošetřena práva duševního vlastnictví, např. výslovné vyloučení přechodu práv duševního vlastnictví (zde zejména práva k databázi ze strany správce) a naopak udělení nezbytné bezplatné licence k databázi, software apod. pro provádění smlouvy a eventuálně v tomto dodatku doplnit

pokud není, vložit klauzuli vylučující předsmluvní odpovědnost

pamatovat u veřejných institucí (knihovny apod.) na nutnost zveřejnění v registru smluv a to i v případě dodatku smlouvy uzavřené před účinností zákona o registru smluv (je nutné doplnit z důvodu navázání na účinnost i z důvodu informace zpracovatele, pokud by chtěl některé části označit za obchodní tajemství, vhodné je např. u detailní specifikace zabezpečení osobních údajů apod.)

## **Vzor souhlasu**

Vzor pro situaci obecní ankety (předpoklad, že obec potřebuje z nějakého důvodu znát totožnost tazatelů a anketu i sběr souhlasů a osobních údajů provádí online):

Online formát umožňuje i uživatelsky přátelštější poučení, které je GDPR velmi doporučováno. Daný text tak lze upravit podle těchto doporučení - dvěma vděčnými nástroji jsou

a) vrstvené informace (hlavní informace shrnutý v krátkém výstižné zkratce, po rozkliku vede link na detailnější informace)

b) užití grafiky, ikonek pro hlavní instituty nebo informace (např. pro poskytování třetím stranám apod.)

Po vyplnění ankety se vygeneruje SMS/e-mail s jedinečným kódem pro pozdější případné odvolání souhlasu.

Účast v této anketě je zcela dobrovolná.

Pokud se pro účast rozhodnete, budeme zpracovávat Vaše osobní údaje v rozsahu: jméno, adresa, věk, povolání, kontakt v podobě e-mailu nebo telefonního čísla, názory na zajišťování bydlení obcí a bytovou politiku. Budeme je uchovávat jen na základě Vašeho souhlasu, který můžete kdykoli odvolut. Pak odstraníme Vaše jméno, adresu a kontakt a anonymně budeme mít jen Váš názor, věk a povolání.

Účelem zpracování Vašich osobních údajů je získání informací o preferencích občanů v závislosti na jejich věku, povolání a bydlišti v obci v oblasti bytové politiky a následné tvorby této politiky.

Na základě těchto osobních údajů nedochází k automatizovanému rozhodování ani profilování.

Vaše osobní údaje nebudou poskytnuty žádné třetí straně. Na

základě speciálních zákonných podmínek by k těmto údajům mohly mít přístup policie a soudy, eventuálně Úřad na ochranu osobních údajů.

## **Máte právo**

kdykoli odvolat souhlas se zpracováním těchto svých osobních údajů a to zadáním kódu, který Vám po vyplnění této ankety přijde na mobil/e-mail na této stránce a následně odkliknutím volby Odvolávám souhlas s účastí v anketě

požadovat přístup ke svým osobním údajům a poskytnutí jejich kopie

na opravu svých osobních údajů, jsou-li nepřesné nebo neúplné

výmaz svých osobních údajů, jsou-li zpracovávány bez platného právního titulu

podat stížnost u Úřadu na ochranu osobních údajů, pokud máte za to, že zpracování osobních údajů porušuje právní předpisy

## **Jak dlohu budeme Vaše údaje zpracovávat?**

Jeden měsíc po ukončení ankety, aby se s podklady výsledků ankety mohlo seznámit nejbližší zasedání zastupitelstva anebo do odvolání souhlasu.

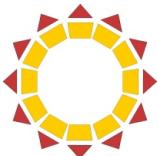
## **Kde se budou Vaše údaje zpracovávat?**

Vaše osobní údaje budeme zpracovávat v našich interních počítačových systémech na vlastním serveru (ev. fyzické umístění; cloud).

## **Správcem Vašich osobních údajů tedy bude:**

Obec XY, kontaktní údaje: Obecní úřad XY, adresa, PSČ, vyřizuje: pan/í YZ, odbor tel.: , e-mail.: , kontakt na pověřence obce pro ochranu osobních údajů:





POSLANECKÁ SNĚMOVNA  
PARLAMENTU ČESKÉ REPUBLIKY

Tento materiál vznikl za spolupráce spolků Iuridicum  
Remedium a Otevřená města s podporou kanceláře  
poslance Ondřeje Profanta. Licence: CC BY-SA 4.0

<https://www.profant.eu>

<http://www.iure.org>

<http://www.otevrenamesta.cz/>