

# **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

Na ízení Evropského parlamentu a Rady (EU) 2016/679 o ochran fyzických osob v souvislosti se zpracováním osobních údaj a o volném pohybu t chto údaj , zkrácen obecné na ízení o ochran osobních údaj (General data protection regulation – GDPR), p edstavuje pro zpracovatele osobních údaj nemalou výzvu p i jeho napl ování. Vzhledem k blížícímu se datu 25. 5. 2018, kdy GDPR nabývá ú innosti, se množí nejistota ú ad , v jaké mí e a v jakých oblastech na n na ízení dopadá. Jelikož je na ízení nové, neexistuje dostatek výkladových materiál , které by zpracovatel m osobních údaj p iblížily nové legislativní nároky.

Ú ad pro ochranu osobních údaj , který je ve smyslu na ízení dozorovým ú adem pro R, popisuje GDPR jako „právní rámec ochrany osobních údaj platný na celém území EU, který hájí práva jejich ob an proti neoprávn nému zacházení s jejich daty a osobními údaji.“

Následující text vznikl se zám rem co nejvíce usnadnit obecním ú ad m a jejich organizacím splní povinností a z ízení opat ení vycházející z GDPR. V první ásti „Analýza dopad GDPR na organizace územní samosprávy“ naleznete shrnutí nárok GDPR ve vztahu k obcím. Tyto nároky se týkají p edevším zmapování agend a proces , p i kterých dochází ke zpracovávání osobních údaj , a na to navázané povinnosti. Mezi ty se adí z ízení pozice pov ence pro ochranu osobních údaj , úpravy smluv se zpracovateli dat, tvorba vnit ních p edpis pro nakládání s osobními údaji a ada organiza ních a technických opat ení.

Druhá část, která tvoří podlohu Analýzy, přistupuje k popsaným povinnostem z praktického hlediska. „Manuál se vzory dokument k implementaci GDPR pro obce“ má obecním úvodem poskytnout srozumitelnou náporu důvodu s konkrétními doporučeními zejména pro úpravy smluv s externími zpracovateli osobních údajů.

# **ANALÝZA DOPADŮ GDPR NA ORGANIZACE ÚZEMNÍ SAMOSPRÁVY**

Je obecn známým a akceptovaným faktem, že stoprocentní implementace GDPR se v termínu do ú innosti u v tšiny správc a zpracovatel nedosáhne. Tato analýza se zabývá n kolika prioritními opat eními, která k implementaci výrazn pomohou a budou p ípadn dozorovým orgánem zkoumána na prvním míst .

Pojednává-li se o dopadech, lze po ítat s jistou pravd podobností, že horní hranice pokut bude pro orgány ve ejné moci i ve ejným subjekt m stanovena na 10 milion K . Tak je to stanoveno v návrhu zákona o zpracování osobních údaj (dále jen „doprovodný zákon“)<sup>1</sup>, zpracovaného na základ zmocn ní v GDPR. Dají se ovšem o ekávat pozm ovací návrhy rušící tento „dvojí metr“ ve vztahu k soukromému sektoru<sup>2</sup>, nelze však ani vylou it

<sup>1</sup> Návrh na ízení o respektování soukromého života a ochran osobních údaj v elektronických komunikacích a zrušení sm rnice . 2002/58/ES, online:

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

<sup>2</sup> Nap . m sto ernošice:

[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)

p ijetí rakouského modelu, kde orgány ve ejné moci a vejně subjekty pokutám nepodléhají v bec<sup>3</sup>.

Nutno zmínit i dopady na poli elektronických komunikací v dlouhodob jším horizontu. V tuto chvíli i v dob ú innosti GDPR se toto bude vztahovat i na elektronické komunikace. V legislativním procesu je ovšem tzv. na ízení e-privacy<sup>4</sup>, které bude sloužit jako speciální právní úprava a je možné, že si vyžádá díl í implementa ní zm ny poté, co také na bude ú innosti (odhady jsou na n kolik m síc až po dva roky legisvakace, která je n kterými zájmovými skupinami po žadována). S p sobením územní samosprávy se ovšem sféra elektronických komunikací protíná jen okrajov , takže rozhodn nep jde o nutnou zm nu významn jšího rozsahu.

Možnost zajišt ní souladu s GDPR pomocí p ihlášení se k „oborovým“ kodex m chování ( l. 40 GDPR) anebo prost ednictvím certifika ních schémat ( l. 42 GDPR) se v této analýze pomíjí. V dob zpracování analýzy není a ani v dob ú innosti GDPR nebude k dispozici ani jeden z t chto nástroj usnadn ní a standardizace implementa ních proces . Z povahy v ci se v třína analýzy týká automatizovaného zpracování osobních údaj , zejména tedy jejich digitální po doby v informa ních systémech; neautomatizované zpracování je zmín no jako specifická podmnožina zpracování v ásti B.3. Pokud se dále v textu hovo í o obci, týká se to i kraje.

<sup>3</sup> Stanovisko WP 29 k pov enci . 2/2017 Zpracování osobních údaj na pracovišti

([https://www.uouu.cz/assets/File.ashx?id\\_org=200144&id\\_dokumenty=28294](https://www.uouu.cz/assets/File.ashx?id_org=200144&id_dokumenty=28294)), Metodické doporu ení MV k pov enci

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

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

# **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**

ást samospráv zahájila první fázi p ípravy na GDPR za- átkem roku 2018, ojedin le se datovou analýzou zabývaly n které m stské ásti a obce již v roce p edchozím.

Dosavadní zkušenosti pomáhají odhadnout asovou i jinou náro nost této p ípravy takto: Pr m rná m stská ást nebo obec s rozší enou p sobností tj. III. typu má zhruba 160-180 agend v p enesené p sobnosti. U malých obcí bude po et agend podstatn nižší, navíc m že být na základ ve ejnoprávní smlouvy domluven výkon n které z agend jinou obcí (v takovémto p ípad není daná obec ani správcem ani zpracovatelem osobních údaj ). V p ípad obce, která pro jinou obec vykonává p sobnost dané agendy, nep jde o vyšší zát ž ve fázi datové analýzy, kterou musí provád t tak jako tak pro „své“ osobní údaje. Projeví se pouze ve vyš- ším po tu osobních údaj jednoho typu v záznamech o zpracování, což eventuáln m že zvýšit nepatrn rizi-kovost 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. terminologií Ministerstva vnitra „systémové analýzy“)<sup>5</sup>. Na základě dohody ÚOOÚ a resort by se totiž mohly jednotlivé resorty v novat připravit na úřinnost GDPR (tedy zejména metodickému vedení) ve své práci o sobnosti. Koordinální roli má plnit Ministerstvo vnitra, které je zároveň ním resortem pro územní samosprávu.

Pro obce, které nebudou ekvat na vzorové systémové analýzy, lze doporučit sestavit si základ pro analýzy ze svých agend, která bude tvořit základ pro povinné záznamy o zpracování dle I. 6 GDPR z toho zdroje :

Registr práv a povinností, resp. ta jeho část, která je příslušná dané obci coby orgánu ve ejmě 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 základníchregistrech). Lze rovněž vycházet z oznámení o vykonávání práci o sobnosti v agendě, které všechny orgány ve ejmě moci povinně podávají Správě základních registrů (§ 6 zákona o základníchregistrech),

Povinný přehled zákona, 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, konkrétní položky č. 14.1. Pílohy 1 (Nejdéležitější používané předpisy),

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

Web ÚOOÚ, z n hož lze využít základní p ehled hlavních p edpis upravujících nakládání s osobními údaji a porovnat jej se svými agendami anebo vlastní dobrovoln zpracovaný p ehled evidence osobních údaj zpracovaný v rámci povinn zve ej ovaných informací dle informa ního zákona<sup>6</sup>,

Vlastní spisový ád, z n hož lze získat jiný pohled nap íkla na problematiku skarta níh lh t, a to podle evidencí, nebo tato sou ást (vyjmenování všech samostatných evidencí) je dle zákona povinnou položkou spisového ádu.

P ehled shora uvedených zdruj je dobrým základem pro ur ení úelu zpracování osobních údaj a obvykle i pro jejich tituly (v p enesené p sobnosti p jde o titul dle l. 6 odst. 1 písmeno e) GDPR, tj. výkon ve ejné moci). Je tedy z ejmé, že s t mito pom ckami si obce zmapují p edevším svá zpracování osobních údaj v p enesené p sobnosti a typická zpracování v oblasti p sobnosti samostatné.

Atypické agendy obvykle v samostatné p sobnosti je t eba analyzovat zvláš pe liv . Ve fázi mapování je t eba vy lenit kapacitu i na zmapování r zného typu zcela dobrovolného (sms informování, provozování obecních wi-fi a jiných p i- pojení i ob anské oslav) nebo o zákon op eného (kroniky) servisu ob an m, kde dochází ke zpracování osobních údaj .

Povinné položky záznam o zpracování osobních údaj (dále

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

jen „záznamy“) jsou dle GDPR jasně dané (jméno a kontaktní údaje obce jako správce, v etn kontaktu na pověnce, údely zpracování, kategorie subjektu údaj, kategorie příjemce, 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 záznamu i další informace, které pak pomohou s plněním povinností dle GDPR. Mohlo by jít o rizikovost zpracování, tj. již zde se představí posoudit riziko jednoduchým namodelováním situace, jaké by mohlo pro osoby sledky nedostupnost, zveřejnění i poznámky dat. Vhodné je zde pamatovat na doprovodné kontaktní údaje pro případ nutnosti oznamení 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 pomáhá. Do záznamu 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 nejáštěji plnění povinností bude výjimka asto 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 záznamu je však velmi výhodná metoda jak zahájit implementaci GDPR. Proto lze doporučit přípravu záznamu i s dalšími nepovinnými údaji, které však později významně pomohou při naplnění 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 klíovou fázi zvládly automatizované různé softwarové nástroje, které se nabízejí „na klíč“; prvek lidského posuzování je v této fázi skutečně nezbytný.

Nákladová datová analýza pro místní obec s povoleným obecním úřadem v případě externích služeb obvykle pohybuje zhruba v rozmezí sto až tisíc Kč, s výjimkami do obou stran. Nižší ceny nabízí obvykle velcí poskytovatelé služeb, kteří už pro obce provádí GDPR konzultace delší dobu. Vyšší ceny pak logicky platí kraje, velká místní 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 svého jednomu dodavateli, anebo zakázku rozdělí (i s tím, že místní provede vlastními silami). Vhodné bude sdílet zkušenosti s dodavateli služeb s obcemi, které již mají tuto první fázi realizovanou; jde o stovky obcí a rychle probíhají.

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

Obsazení pozice pověřence (DPO) si u obcí žádá zejména kapacitu na rozhodnutí o formu zapojení (externí výkon/zaměstnanec) a jeho zařazení v rámci organizační struktury a případné provedení výběrového řízení/kontraktace externího pověřence i jeho výběru z nabízených sdílených služeb pro územní samosprávy. V současnosti je k dispozici dostatek podkladů<sup>7</sup>, které umožňují objasnění 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) Pov ence je povinna ustavit každá obec bez ohledu na velikost a p ísp vková organizace, která rozhoduje o právech a povinnostech (nap . školy) nebo která provádí rozsáhlé zpracování citlivých osobních údaj anebo pravidelné systematické monitorování (nap . dopravní podniky). Výslovn dle Ministerstva vnitra nemusí mít pov ence knihovny i technické správy komunikaci<sup>8</sup>. Doprovodný zákon, který je aktuáln v legislativním procesu, definuje v d - vodové zpráv p ísp vkové organizace (s vyjimkou škol, které rozhodují o právech a povinnostech) jako „pomocné“ subjekty, které pov ence 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 pozemkovací návrhy vyhnou,

b) Funkce pov ence m že být vykonávána extern , a to i jako spole ný pov enec pro n kolik subjekt ; vždy však musí být zajist na jeho rychlá dostupnost pro ÚOOÚ i ve ejnost. Lze využít nabídky komer ních subjekt , ale výhodn jší se jeví pov enci nabízení ze strany asociací územních samospráv. Vhodný je i spole ný pov enec pro obec a její p ísp vkové organizace, které podléhají povinnosti pov ence mít,

c) Pov encem m že být i zam stnanec, a to i na zkrácený úvazek – ve druhé ásti úvazk m že být zam stnán u stejného zam stnavatele, ale nikoliv na pozici, která by ohro žovala jeho nezávislost. Pokud bude pov encem zam stnanec, bude se jeho nápl práce a odm ování ídit dle na ízení vlády . 302/2014 Sb., o katalogu správních inností, a na ízení vlády . 222/2010 Sb., o katalogu prací ve ve ejných službách a správ . Tato na ízení již k 1. 1. 2018 obsahují i pozici pov ence pro ochranu osobních ú

<sup>8</sup> tzv. Metodické doporu ení k pov enci, online:

daj (v obecních úadech obvykle 11. a 12. platová t ída). Další možnosti vzhodnout z d vodu nutnosti zachovat nezávislost pov ence m že být nap íklad dohoda dvou obcí, kdy bude pro jednu obec d lat pov ence zam stnanec druhé obce a obrácen ,

d) Pov enec musí ovládat agendu ochrany osobních údaj , a to s p esahy do práva i IT, nemusí však mít žádné formální kvalifikaci p edpoklady. Jelikož hlavním požadavkem GDPR je jeho nezávislé fungování zam ené na soulad praxe s GDPR, p i výb ru (zejména bude-li vykonáván na pozici zam stnance) by m l být brán v potaz i osobnostní profil, zejména samostatnost, aktivita a p irozená autorita,

e) Nejsložit jší bude vybalancování faktické pozice pov ence s ohledem na zákaz úkolování pov ence v oblasti dozoru nad dodržováním GDPR a jeho faktickou nedotknutelností (zákaz –široce pojatého- sankcionování nebo propušt ní za pln ní jeho úkol ). Smlouva s pov encem by se proto m la zam it na ošet ení situací, kdy naopak sankce na míst jsou – st et zájm , nepln ní svých úkol ze zákona, nedosažitelnost apod..

f) Pov enec bude pravd podobn podléhat povinnosti ml enlivosti (o osobních údajích a k nim p ijjatým bezpe - nostním opat ením), která bude trvat i po skon ení jeho p sobení v pozici. Tato povinnost ml enlivosti by se pak týkala i jeho p ípadných pod ízených. Jde o návrh ásti es kého doprovodného zákona, který není v dob dokon ení této analýzy schválen, takže není jisté, zda bude zákonem tato právní povinnost stanovena. V rámci p íprav se však obcím doporu uje zpracovat povinnost ml enlivosti pov ence do smluv s ním uzavíraných. Takové ujednání nebude mít vliv na platnost smlouvy, i pokud bude stanoveno nad rámec úpravy v doprovodném zákon .

Ustavení pov ence lze, a je dokonce vhodné, zajistit co

nejd íve, již p ed ú inností GDPR, tedy ve fázi datových analýz a tvorby záznam o zpracování, úpravy smluv, ev. souhlas a lad ní interních opat ení. asová náro nost pro ustavení pov ence není vysoká. Je ale nezbytné po ítat s lh tami obvyklými pro výb rově ízení, s p ihlédnutím k faktu, že poptávka po pov encích je vysoká a úrove uchaze bude r zná. V p ípad využití pov ence sdíleného, nabízeného jako služba nap . Svazem m st a obcí, je proces jednodušší. Je však t eba mít pe liv p ipravené požadavky a konkrétní nápl práce s ur enými konkrétními povinnostmi (mj. konkrétn ur ená dostupnost, lh ty pro vy izování dotaz , dny ur ené pro konzultace atd). S ohledem na výše uvedené bude asová náro nost na definování zp sobu za-jišt ní, kritéria pro výb r, prvky smlouvy s pov encem, ur- ení eventuálního dalšího úvazku pov ence a provedení výb ru zhruba m síc až m síc a p l. K po átku dubna by však obce (alespo II. a III. typu) již m ly mít pov ence ustaveného ve funkci.

Nápl práce pov ence je ponejvíce konzulta ní, školicí, po- radenská a monitorovací (auditní). Dle GDPR a vodítek k pov enci je jeho konkrétní náplní práce:

- poskytování informací a poradenství o povinnostech v celém rozsahu GDPR - správc m nebo zpracovatel m a zam stnanc m,
- poskytování poradenství, pokud jde o posouzení vlivu na ochranu osobních údaj (u obcí spíše nebude nutné),
- monitorování souladu s GDPR, tj. pr b žná innost dle koncepce a ad hoc pot eb,
- zvyšování pov domí a odborné p ípravy pracovník zapojených do operací zpracování a souvisejících audit ,
- spolupráce s Ú adem pro ochranu osobních údaj ; má

být kontaktním místem pro pracovníky ÚOOÚ,

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

Náklady na inost povolenec je třeba zahrnout do rozpočtu, jsou trvalé, nicméně pohybují se od několika set Kč méně za externího povolence od sdružení samospráv, po náklady desetitisíce při zajištění formou zaměstnání pracovníka v této pozici i externí službu s vysokou přidanou hodnotou. Ustálilo se, že ceny pod deset tisíc Kč méně nejsou v těch obcích a městských částech lze u externích poskytovatelů bez problém dosáhnout.

Lze shrnout, že zajištění povolenec nepatří k nejnáročnějším povinnostem nutným pro dodržení GDPR a tuto povinnost lze do únosti GDPR pohodlně stihnout, přinejmeněž náklady nemusí být vysoké, jsou však trvalé. Určitě je ale nutné vnovat kapacity pro plné využití povolenec 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 údaj je situace různých obcí a to stejného typu, rozdílná. Liší se jak co do velikosti zpracovatele (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 asistence na úpravu smluv se tedy nedají všeobecně odhadovat, závisí na počtu uprava-

vovaných smluv, stávající podob smluv (zejména klauzule o garanci souladu ešení s aktuální legislativou v pr b hu trvání kontraktu) i vyjednávací procedu e. V úvahu se musí vzít i asové hledisko s ohledem na nutnost výb rových ízení, pokud by obec dosp la k záv ru, že bude t eba zpracován osobních údaj zajistit novým zpracovatelem a hledisko nejbližší ú innosti smlouvy až jejím zve ejn ním v registru smluv. Nemálo zpracovatel bude objektivn pot ebovat as na technické úpravy svých systém k zajist ní provád ní povinností dle GDPR, což bude danost vyjednávání o dodatcích smluv.

A koliv by m la úprava smluv se zpracovateli následovat po provedení první fáze implementace GDPR, tj. datové analýzy a p ípravy záznam o zpracování, v dob dokon ení této analýzy, je t eba si uv domit, že do ú innosti GDPR zbývají už jen ty i m síce, což není mnoho. Lze proto doporu it, aby obce, které ješt s úpravou smluv se svými zpracovateli neza aly, zahájily souasn s provád ním datové analýzy jednání se svými dodavateli, kte í zpracovávají osobní údaje. Výzva k p edložení dodatku prvn zpracovatelem ostatn také napoví ohledn jeho p ipravenosti na GDPR. Smluvní zajist ní je tvrdá povinnost daná GDPR ( l. 28 GDPR), formáln velmi dob e prokazatelnou, takže lze o ekávat, že p i p ípadné kontrole budou ÚOOÚ zajímat smlouvy se zpracovateli na jednom z elných míst.

Uvedení všech smluv do souladu s požadavky GDPR bude trvat ádov m síce, pokud se budou povinnosti dané GDPR specifikovat podle druhu zpracování. U složit jších zpracování to bude nutné. Obcím lze doporu it (a na náro nost dopad bude mít vliv):

- a) Využití pomocných materiál jako je P íloha k této Analýze se vzory dokumentace, kde jsou obsaženy i pot eb né povinné smluvní klauzule v univerzální podob ,

- 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 pokryt nejen technicky, ale i smluvní GDPR compliance,
- e) U stejných subjektů lze využít též podpory v GDPR poradenství, kterou některou nabízí (v těsnou čidlova coby součást marketingu) i se inspirovat jejich smluvním řešením i pro smlouvy s jinými zpracovateli,
- f) Pamatovat na možnosti, které dává zatím nepřijatá legislativa a ošetřit je ve smlouvách pomocí podmínek, opcí, apod. (např. možnost zpracovatele zprostít povinenec povinnosti mládí enlivosti 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 v těsné blízkosti nerealizuje. Indikativně lze vycházet z kalkulace nákladů na kapacity vlastních zaměstnanců i zajištění ním vlastním personálem a z hodinových sazeb služeb

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

poradenských spole ností, protože nejobvyklejší bude z ejm zajišt ní kombinací jejich vstupu (p íprava smluv extern , dojednávání a organizace kontraktace intern ). Po ítat s vytížením nemalé ásti kapacit svých právník a obvykle i IT zam stnanc a podp rné administrativy je vhodné na dva až p t m síc .

Obce by m ly rovn ž v novat pozornost tomu, zda úpravu smluvní dokumentace, softwaru apod. nemají právo požadovat od svých dodavatel zdarma v rámci tzv. legislativního maintenance, které je astou sou ástí smluv.

## **IV. ORGANIZAČNÍ OPATŘENÍ**

### **1. ŠKOLENÍ**

Proškolení by se m lo týkat všech zam stnanc p icházejících do styku s osobními údaji, což je p evázná ást pracovník ú ad územních samospráv. Bylo zjišt no, že k lednu 2018 absolvovala n jaký typ školení ke GDPR v třína tajemník obecních ú ad .

V rámci posledního tvrtroku p íprav by se m li proškolit nejlépe na po átku datové analýzy vedoucí odbor , aby mohli ú inn spolupracovat p i mapování agend. V dalším pr b hu implementace je vhodné proškolit zam stnance IT odd lení, aby m li p edstavu o zásadách GDPR a pot eb ných opat eních. Sou ástí tohoto školení by už nicmén m ly být i konkrétní kroky, které bude nutné v IT oblasti provést. Na konci implementace GDPR, resp. p ed za átkem ú innosti GDPR, by m li absolvovat školení referenti a všichni, kdo zpracování osobních údaj vykonávají. Lze jim tak již p edat více návodné postupy ešení.

Školení by mlo být prováděno někdy nikoli zcela externím - ideální bylo již angažování pověřence, velmi vhodné je školení od sdružení samospráv, výborná je samozřejmě i forma workshop, kde se může vyměnit mnoho zkušeností s dobrou praxí tam, kde se provádí. Pokud je na implementaci GDPR najat externí dodavatel, může i školení provádět on a je vhodné smluvně zajistit, aby všestandardy školení vnoval odpovědný 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 příslušnosti implementace.

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

Vzhledem k výše uvedeném nejsou školící aktivity zvlášť alespoň náročné, ještěeba je však za lenit do poptávkovo-vého/smluvního balíku přizajistování pověřence/výběru externího implementátora/modelu spolupráce v rámci sdružení samospráv. Náklady se podle formy školení, lektor, počtu účastníků i dalších požadavků mohou pohybovat v rozmezí tisíc až sedmi tisíc Kč za hodinu. Nemusí jít o zcela jednorázový náklad, GDPR požaduje pravidelné ověřování opatření na zajištění bezpečnosti osobních údajů (§ 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 (příslušné formy) nové povinnosti lépe utkví v paměti.

## **2. IT OPATŘENÍ**

Opatření v oblasti IT lze považovat za nejnáročnější, jak aspektů, tak i finanční. Bude nutné posoudit, zda je níže uvedené IT opatření potřeba zavést v rámci stávajících produktů a systémů, které má úvod k dispozici, anebo je třeba pořízení zcela nového softwarového vybavení i rozšíření stávajících produktů o licence k dalším funkcionalitám i kombinacím 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 bez zbytku povinnostem z GDPR plynoucích.

Z právního 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 přencem varianty řešení, dostupné produkty a řešení v etapách různých možností zajistit. 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 úvodů zpracování

- minimalizace zpracovávaných osobních údaj
- omezení jejich uložení jen na nezbytnou nutnou dobu

Z uvedeného vyplývají hlavní obvyklé IT nástroje v následujícím výtu:

- Zmapování nestrukturovaných dat (zejména e-maily, souborové servery, soubory v cloudových ešeních jako SharePoint i interní komunikační kanály) není neobvyklé (v instituci to bývá více než 50% dat) a týká se alespoň jištění 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 výhledové, jsou dost nákladné), hlídá se indexování i korekce<sup>10</sup> anebo ešení interními jednoduchými opatřeními (viz dále ást pojednávající o možnostech u nej-ast jeho typu t. chto dat - e-mail),
- 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 údaji m – 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 (zjednodušené eno dat v databázích), který doporučuje i GDPR, je i pseudonymizace osobních údajů – obec by mohla posoudit, kde je třeba zavést. Mohlo by se brát v potaz, že dle GDPR je

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

pseudonymizace standardní nástroj, takže rozhodn není vyhrazena jen pro citlivá data apod. Vhodná je všude, kde k n kterým operacím nebo po ást doby zpracování není nutné jednozna né ur ení osoby,

- Posouzení vhodnosti šifrování osobních údaj by se m lo provést zejména u citlivých osobních údaj , údaj na p e-nosných za ízeních (zejména notebooky, tablety) a podobn ,
- Rychlost a uživatelský komfort nástroj pro ízení p ístup (p ístupová práva budou vyplývat z datové analýzy a interních sm rnic),
- Možnosti stávajících nástroj dob e rozpoznávat a zve ej ovat data ur ená ke zve ejn ní, a již v rámci ú edních desek nebo povinností v oblasti otev ených dat, a také je p evád t do strojov itelného formátu dle požadavk zákona i standard pro otev ená data,
- U p enosných za ízení posouzení nastavení z hlediska bezpe nosti (zejm. prevence a ešení ztráty dat nebo za ízení) a odd lení oblasti soukromých/služebních dat v souladu s doporu eními WP29, a již jde o možnosti užívání služebních mobil , notebook apod. k soukromým ú el m i koncept využívání vlastních za ízení zam stnanc pro služební ú ely (BYOD),
- Nezbytné je i zhodnotit stávající ešení zálohování, nebo právo být zapomenut (právo na výmaz osobních údaj ) se vztahuje i na osobní údaje v zálohách.

Je z ejmé, že opat ení v IT jsou náro ná jak na mapování možností pro nevhodn jším ešení, na samotné jejich zavedení v etn testování a nebude ojedin lá i nezbytnost

po ídit nový softwarový produkt nebo rozšíí it stávající. Náklady na licence k software mohou být až vyšší statisíce, i když obvykle spíše menší ástky. Odhad lov kohodin IT pracovník se pohybuje rozhodn také ve stovkách. V této oblasti je zejména z ejmé, že do ú innosti GDPR nebude vše stoprocentn zajišt no. Nutná bude asto prioritizace opat ení, základními opat eními bude ízení p ístupu a správa za ízení. Doporu it lze ur it též prov it pln ní povinnosti logování (i nahlížecích) p ístup k osobním údaj m – plyne už z dnešní legislativy, ale nebývá vždy pln na stoprocentn . ÚOOÚ s touto povinností pravideln pracuje. Ne bude neobvyklé, že navržené postupy v IT se budou realizovat postupn a až po ú innosti GDPR.

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

Stanovení odpov dností za zpracování osobních údaj je prvním krokem p ed tvorbou sm rnic. Vyplýne z mapování dat a stávajících p i azení odpov dností v rámci organiza ní struktury. V interních sm rnicích lze doporu it upravit

- procesy v p ípadech nových institut GDPR resp. i staronových, kde se právní úprava neplnila dokonale: co, kdo, kdy koná v p ípad realizace práv subjekt údaj na p ístup, výmaz, opravu<sup>11</sup>,
- proceduru pro situace tzv. incident , zejména pak za jist ní informování ÚOOÚ eventuáln i subjekt údaj ( ást odpov dnosti a role zpracovatel a pov ence by m la být vt lena ve smlouvách s nimi),

<sup>11</sup> I. 13 - 17 GDPR, p ípadn též práva na omezení zpracování dle I. 18 GDPR (práva na p enositelnost, námitka proti zpracování i proti automatizovanému zpracování nebudou u obci ve v tšin p ípad relevantní).

- modelový souhlas se zpracováním osobních údaj , je-li u obce relevantní,
- modelové pou ení subjekt údaj o zpracování dle l. 13 a 14 GDPR, pro relevantní situace (situace by m ly být za len ny do proces ),
- nutná jsou stanovení odpov dností konkrétních pozic a povinností zam stnanc obecn (zde pak musí následovat skute né, nejen formální seznámení, daných osob, a samo- z ejm prokazatelné),
- prakti nosti sm rnic pom že i odkaz na interní p edpisu související (spisový ád, bezpe nostní politika obecn , provozní ád IT), pom že tak i souladu p edpis a vnit ní logice systému (typicky u skartace).

Není vhodné opisovat do sm rnic text GDPR, zejména ne obecné zásady apod., m lo by jít o praktický dokument s konkrétními informacemi „kdo, kdy, jak“. Po ítat je t eba i s dalšími úpravami v souvisejících vnit ních dokumentech v etn organiza ního ádu.

Vzhledem k pom rn volným pravidl m pro vydávání a schvalování interních sm rnic lze p ípadn dopady na obce dávkovat a to p ijetím sm rnice upravující základní a nutné

záležitosti s tím, že její doplnní lze o ekávat na základě zkušeností s realizací nových institut a práv po úpravě GDPR. I dozorový úřad po úpravě s postupným náplňováním GDPR a náplň směrnice lze na základě zkušeností rozvíjet o větší detailech.

Náročnost na kapacity je nižší, je však třeba poúčitat se s průběžnou prací na směrnici, jak je popsáno výše, a obvykle i nutností provést ostatní stávající vnitřní přepravy na poli bezpečnosti, obsluhy informačních systémů, ale třeba i spisový úřad (zejména skartu náhrady), 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 (rozumí elektronické), na které již Ministerstvo vnitra vydalo metodiku, a zajistit náhradou, aby spisová služba fungovala v souladu s požadavky GDPR, se opírá o několik střejných doporučení:

- Provést revizi spisového a skartu náho plánu, zejména skartu náhrady, které by mohly být v souladu se zásadou minimalizace stanoveny jen po nezbytně dlouhou době 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 archiválí,

- 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 i úzení přístupu i v systému spisové služby pro naplnění požadavků GDPR,
- Využít práv osob na přístup k údajům do systému zaznamenávat, pamatovat na ochranu osobních údajů těchto osob (anonymizace) při poskytování,

Výslovné shrnutí právní situace: využití práva na výmaz osobních údajů nemáže obstát na neskartovaný dokument a na dokument po skartání lze 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 významné osobní údaje a je ve speciálním díle v rámci 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 v etně citlivých, zároveň splňují podmínu automatizovaného vedení a nejsou tedy z povinnosti GDPR výzvy (GDPR nedopadá pouze na neautomatizované evidence, kde nejsou osobní

údaje p ístupné podle zvláštních kritérií). Navíc samotné e-mailové adresy, zejména pokud jsou tvo eny jménem a p íjmením (a to i pracovní), bývají asto samy o sob osobním údajem.

Stanoví-li se ú el zpracování osobních údaj v e-mailech, je to vedení korespondence, které vyplývá z mnoha výslovných i implicitních povinností územních samospráv. Pro provedení zásady minimalizace osobních údaj ( l. 5 písm. c) pov enec GDPR) bude nevhodn jím postupem zam it se na p ílohy coby zdroj mnoha osobních údaj , asto i citlivých a komplexních (nap . CV).

Obec si m že interní procesy nastavit tak, že

- a) interním p edpisem uloží každou relevantní p ílohu „zpracovat“ tj. zejména uložit do p íslušné složky agendy,
- b) nastaví automatické odstran ní (nevratné smazání) p íloh po ur it dob , nap . 6 m sících,
- c) úpravu metodik u e-mail v ú ad lze využít i pro p e-nastavení politik, které d lají na poli ochrany osobních údaj také problém – a to e-mailové adresy zam stnanc . Pokud jsou tvo eny jménem a p íjmením, p jde o osobní údaj spadající pod pravidla GDPR. V p ípad adresy tvo ené nikoli jménem, ale nap . pozicí (poverenec@urad.cz) se vy eší jak problém se zbytnou kategorií osobních údaj tvo ících e-mailové adresy, tak se zastupitelností pracovník ,
- d) s tím souvisí doporu ení WP 29 týkající se zpracování osobních údaj v zam stnání<sup>12</sup>, kde se u r zných typ

<sup>12</sup> stanovisko WP 29 . 2/2017 ke zpracování osobních údaj 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 opakovan zd raz uje právo zam stnanc na zachování ochrany soukromého života i v zam stnání. Kontrola zam stnavatele, co do obsahu korespondence, aktivit online apod. je i na za ízeních zam stnavatele nutn omezená. Zájmy zam stnavatele doporu uje WP29 zohlednit ešením, které se jeví velmi praktické a lze doporu it zavést i u zam stnavateli - územních samospráv, a to vyhradit zam stnanc m ur itý prostor (na pevném disku, ve složce pošty apod.) pro soukromé aktivity, kam je p ístup zam stnavatele omezený, zatímco v ostatním bude právo zam stnavatele na kontrolu vyšší.

Uvedená doporu ení ohledn nastavení e-mailové politiky je teba realizovat nejen pomocí organiza ních opat ení (sm rnice), ale je nutné provést zm ny v informa ních systémech a zejména pak pr b žn kontrolovat a trvat na jejich zažití. Je možné se domnívat, že v dob ú innosti GDPR by již mohlo být reálné mít p ipravenou novou sm rnici a b žící nebo dokon ené úpravy v nastavení v IT systémech. Zásadní bude proškolení a pevné zavedení v rámci ú adu. Dá se p edpokládat, že ÚOOÚ nebude v první fázi kontrol požadovat stoprocentní zajistní souladu s GDPR i v nestrukturowaných datech typu e-mail , mj. i proto, že vodítka WP29 nebyla a nejsou k dispozici v dostate ném p edstihu p ed ú inností GDPR. Vyhledov do budoucna se však zm ny doporu ují.

### **3. NEAUTOMATIZOVANÉ ZPRACOVÁNÍ**

Celá analýza pojednává o automatizovaném zpracování osobních údaj , které je dnes p evažující realitou ve v tšin agend u v tšiny obcí. V plánování p íprav na GDPR je však teba myslet i na opat ení v oblasti zpracování tzv. pa-

pírového i obecn ji analogového (nap . osobní údaje na magnetických páskách).

Nejnáro n jší ástí bude z ejm zmapování t chto p e- trvávajících agend u v tších obcí, zavedení odpovídajících organiza ních opat ení (nap . ízení p ístupu, bezpe nost), která jsou oproti digitální podob osobních údaj v tšinou snazší.

Lze spíše o ekávat, že pravidla pro skartaci, umis ování analogových dokument jsou historicky vžitá a obvykle ne- bude t eba zásadních zm n.

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

Pot ebná je i rekapitulace nových povinností daných GDPR, která naopak pro naprostou v tšinu obcí relevantní nebude (nemusí to však platit o organizacích jimi z izovaných, viz informace níže v textu), a proto není pot eba je poptávat do školení, implementaci nebo je jinak významn ji zahrnovat do plán implementace.

### **1. PORTABILITA**

Dobrou zprávou pro územní samosprávu je, že nový institut

p enositelnosti osobních údaj ( l. 20 GDPR) se jich z 99 % nebude týkat. Samotné na ízení totiž vylu uje z této povinnosti ( l. 20 odst. 3) zpracování nezbytné pro spln úkolu provád ného ve ve ejném zájmu nebo p i výkonu vejné moci.

Zajišt ní povinnosti p enositelnosti osobních údaj se tak bude týkat bu atypických inností v rámci samostatné p sobnosti anebo v p ísp vkových organizacích. Musí jít o osobní údaje poskytnuté samotným subjektem údaj na základ souhlasu anebo pro pln ní smlouvy a jde-li zárove o automatizované zpracování. Portabilita tak tedy dopadne ur it na v tší knihovny.

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

Samotné obce nebudou muset ešit také speciální povinnost získat namísto dít te mladšího 13 let (jak ur uje v kovou hranici eský návrh doprovodného zákona) souhlas jejich zákonného zástupce. Týká se totiž jen nabídky služeb informa ní spole nosti (p enos dat, p ipojení, ale i r zné sociální sít , aplikace apod.), což je v kombinaci s cílením na d ti u obce i v samostatné p sobnosti nepravd podobné.

Je však t eba mít na pam ti, že pokud by v rámci podpory své innosti nabízeli r zné online aplikace p ísp vkové or-

ganizace jako je sportovní i kulturní zařízení obce, školy a podobn., je nezbytné si obstarat prokazatelný způsobem souhlas zákonného zástupce. Výjimkou jsou dle GDPR jen preventivní poradenské online služby pro dospělé, aby byl zachován jejich smysl.

Pro jakékoli jiné zpracování platí už dle těchto zásad, a to že právní titul zpracování zahrnuje vodu zájmu správce i třetí osoby, je už třetí posuzován ještě přísněji v takém zásluhu do jeho práv a že případné zpracování osobních údajů musí plnit adu informačních povinností dle čl. 13 a 14 GDPR formou dle této příslušné (i když je však všechno zpracování ze zákonného 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. Aby se doporučuje za lenit rizikovost zpracování, která vyplývá zejména z kategorie osobních údajů i závlah, kterých se zpracováním dosáhne, již do fáze datové analýzy a tvorby záznamů o zpracování, nemusí být povaha vysokého rizika vždy jasná. GDPR také svým užem národním zákonodárcem možnost prohlásit určité druhy zpracování za jednoznamenavými vysoce rizikové a tedy podléhající DPIA anebo naopak výjimky určitých druhů zpracování, které DPIA vyloučí. V aktuálně známé podobě návrhu doprovodného zákona se tyto výjimky neobjevují. Pro územní samosprávu už třetina 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 vodové zprávy dopad na ochranu soukromí). Pozornost je tedy u obce spíše zaměřena dovnitř – na systémy kontroly i automatizovaného hodnocení

zaměstnanc – kritéria lze celkem návodn najít v Pokynech WP29 pro DPIA.

V posuzování dopad je třeba vzít v potaz i doporu ení WP 29, aby byla DPIA i alespo její závry obsahující doporu ení zveřejnena (napl uje se tak princip transparentnosti daný I. 5 i dalšími částmi GDPR). Tuto povinnost by měla obec mít na paměti, nepředstavuje tém žádnou zátěž a-sovou ijinou.

Pokud se týká organizací spadajících pod obec, nejálost ji bude DPIA podléhat kamerový systém městské policie a jeho parametry. Spadá pod pojem systematického monitorování veřejných prostorů, a to již i s moduly pro automatizované rozpoznávání osob, nestandardního chování apod. Tyto inosti 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“ ešení návratu více policist nebo strážník 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).
- Všechny jsou dokumenty WP 29 dostupné zde:  
<https://www.uouu.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 český Posouzení vlivu na ochranu osobních údajů. Jde o nástroj, který napomáhá správci a zpracovatelem 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 mohly podklady pro sestavení poptávky, kontrolu a srovnání nabídek.

Manuál je pojat prakticky - poskytuje konkrétní vzory a shrnuje postupy ve kterých resp. ty nejdříve leží jich krokůch přípravy: tvorba záznamů o zpracování, resp. v případě „obohacených záznamů o zpracování“ provedení datové analýzy, úpravu smluv se zpracovatelem a nové instituty souhlasu.

# **VZOR OBOHACENÉHO ZÁZNAMU O ZPRACOVÁNÍ**

Proti povinnému záznamu o zpracování dle GDPR je po et informací zásadn rozší en, má to však smysl – p i jednom mapování dat se nashromáždí další údaje, které velmi pomohou p i pln ní dalších povinností. Záznamy o zpracování v této podob znamenají provedení velké ásti mapování dat. Hv zdi kou jsou ozna eny informace, které mají návaznost na n jakou z povinností dle GDPR, ve vedlejším sloupci je tato povinnost odkázána.

Základ – informaci o všech zpracováni (resp. zjedno- dušen agendách) obec m že získat ze stávajících p ehled , které má k dispozici: organiza ní ád, spisový a skarta ní ád, oznámení o vykonávání p sobnosti v agend 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?

Fyzické umístění osobních údajů  
Doba uchovávání a čím je daná

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

*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 OOJ 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) i jiné speciální předpisy eskomého právního ádu. Odkaz na konkrétní ustanovení GDPR v této smlouvě jen v případech, kdy je „didakticky“ vhodné nebo poprvé zmíněn určitý institut dle GDPR. Smluvní vzor pochází 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 nelze je použít (např. povinnost informovat subjekt údaje v případě incidentu, který nepředstavuje riziko pro práva a svobody subjektu údaje). V případě různých druhů zpracování resp. v různých kategoriích 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. nebo kurzívou v textu, kde jsou varianty odděleny lomítkem (eventuálně doprovázeny vysvětlujícím textem kurzívou v závorce).

Ze zde uvedených klauzulí lze zkonstruovat i zcela novou smlouvu, nahrazující předešlou. Výběr postupu závisí především na obsahu předložené smlouvy a náročnosti definování ustanovení, které se mají/nemají. Označení „subjekt“

údaj " lze nahradit ozna ením „klient“ apod. dle p vodní smlouvy, úzu vztah mezi správcem a zpracovatelem i jejich dalšími smluvními vztahy se subjekty údaj .

Zavedené zkratky:

- „správce“
- „zpracovatel“
- „osobní údaje“ (rozum j údaje upravené touto smlouvou definované v úvodních ustanoveních)
- „smlouva“ (p vodní smlouva)
- „dodatek“ (aktuální dodatek, kterým se p ípadn m ní p - vodní 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 úely této smlouvy,

b) zpracovávat osobní údaje v souladu se závazky v této smlouv 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 údaj ,

d) (VAR) pokud je zpracovatel povinen zasílat osobní údaje mimo EU nebo mezinárodní organizaci, musí zpracovatel informovat správce o právním základ této povinnosti před za-hájením zpracování osobních údaj ,

e) zajistit dle smyslu l. 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 mimořádnosti, nemají-li povinnost mimořádnosti ze zákona

b) byli odpovídajícím způsobem proškoleni

c) mimořádný 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 vy-máhat.

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 I. 15 GDPR,
- b) práva na opravu svých osobních údajů dle I. 16 GDPR,
- c) práva na výmaz osobních údajů dle I. 17 GDPR,
- d) práva na omezení zpracování dle I. 18 GDPR,
- e) práva namítat zpracování osobních údajů dle I. 21 GDPR,
- f) práva namítat zpracování dle I. 21 GDPR,
- g) práva na posouzenitelnost údajů dle I. 20 GDPR,
- h) práva namítat automatizované rozhodování v etnoprofilování dle I. 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 připojit veškerou dokumentaci ev. ji 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/ zpracovatele 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) p i zpracování DPIA,
- b) p i p edb žně konzultaci s Ú adem na ochranu osobních údaj dle l. 36 GDPR,
- c) (není povinné dle GDPR, m že být vhodné u b žících zpracování) p i p íprav i zm nách záznam o zpracování o-sobních údaj dle l. 30 GDPR, zejména je povinen
  - i) písemn vést jméno a kontaktní údaje správce, p ípadných dalších zpracovatel a p ípadného pov ence ochrany osobních údaj ,
  - ii) kategorie zpracování osobních údaj ,
  - iii) p ípadné poskytování osobních údaj do zemí mimo EU s dokumentací p íjetí odpovídajících záruk,
  - iv) je-li to možné, popis technických a organizačních bez pečnostních opatření.

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

- a) požadavku na zp ístupn í osobních údaj od orgán ve ejné moci v etn orgán inných v trestním ízení,
- b) dotazu i šet ení Ú adu na ochranu osobních údaj týkající se osobních údaj 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 údaj ,
- b) zajišt ní trvalé d v rnosti, integrity, dostupnosti a odol-nosti systém pro zpracování osobních údaj ,
- c) v p ípad technických i fyzických problém obnovit dos-tupnost osobních údaj ,
- d) zavést pravidelné testování a hodnocení ú innosti tech-nických a organiza ních bezpe nostních opat ení a prokázat je na vyžádání správci.

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

(1) Zpracovatel se zavazuje při ukončení zpracování z dů-vodu\_\_\_\_ 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 v etapě provádění auditu a kontroly 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 úrovne poskytovaných služeb, tj. SLA klauzule,

systém schvalování subdodavatelu služby cloud computingu obcí,

podmínky ukončení smluvního vztahu z pohledu bezpečnosti,

zízení kontinuity iností v souvislosti s poskytovanou službou cloud computingu,

urcení vlastníka uchovávaných dat,

dohoda o duvernosti smluvního vztahu (NDA klauzule, nebude tedy zveřejneno ani v registru smluv),

stanovení úrovne ochrany dat z pohledu duvernosti, 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 vůči 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 pau-

šalizování 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 podmínkou/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 přetrívání 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 dobře 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 (nap. pro poskytování této 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 automa-

tizovanému 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 následném odkliknutím volby Odvolávám souhlas s účastí v anketách

požadovat přístup ke svým osobním údajům a poskytnutí jejich kopie

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

vymazat svých osobních údajů, jsou-li zpracovávány bezplatného právního titulu

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

Jak dlouho 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 umí-

stění; *cloud*).

Správcem Vašich osobních údajů tedy bude:





iure  
...není nám to jedno



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/>