ZPRÁVA
O VÝSLEDKU VSTUPNÍHO AUDITU OSOBNÍCH ÚDAJŮ A STANOVENÍ ÚČELU ZPRACOVÁNÍ

ČÁST 2.: IMPLEMENTACE

Město Příbram 2018

Evropská unie
Evropský sociální fond
Operační program Zaměstnanost

OBECNÁ PRAVIDLA ANALÝZY RIZIK A DOPADŮ

1. OBECNÉ HODNOCENÍ HROZEB A RIZIK

1.1 Metody analýzy rizik v kontextu GDPR

Řízení rizik je vykonáváno podle článku 25 a článku 32 GDPR. Řízení rizik je prováděno s cílem určit vhodná technická a organizační opatření, která je nezbytné zavést pro zajištění bezpečnosti osobních údajů při jejich zpracování a pro zmírnění nebo eliminaci rizik pro práva subjektu údajů vztahujícím se k realizovanému zpracování.

Analýza rizik v kontextu GDPR je unikátní v porovnání s dosavadními postupy analýzy či jiného posuzování rizik[1], a to s ohledem na posuzování hodnoty aktiv, hrozeb a stanovení dalších parametrů analýzy rizik z pohledu dopadu na subjekt údajů nebo na informace, které obsahují osobní údaje subjektu údajů.

S ohledem na předpoklad Kolektivu, že v rámci Správce došlo či dochází k adaptaci principů a technik dle ZKB, zvolil Kolektiv metodu analýzy rizika, která ze ZKB vychází, a doplnil ji o části posuzující a vyhodnocující problematiku z pohledu subjektu údajů a jeho práv.

Na základě identifikace primárních aktiv z kapitoly Metodika vyplňování formulářů, Kolektiv provedl ohodnocení primárních aktiv dle jejich kritičnosti pro Správce. GDPR nepředepisuje povinný formát analýzy rizik a taktéž nikterak nezvažuje hodnotu aktiva. Hodnota aktiv je z pohledu GDPR stejná, GDPR předepisuje chránit osobní informace jako celek. V rámci ISO 27001 se tím způsobem řeší, zda aktivum vstoupí do analýzy rizik či nikoliv. Nicméně s ohledem na modelový charakter a prioritizaci opatření, kterou je vhodné zvolit s ohledem na implementační náklady s cílem harmonizace prostředí Správce s požadavky nařízení GDPR, zvolil Kolektiv následující kategorizaci aktiv, a to:

- Běžná hodnota aktiva – jedná se o osobni údaje zaměstnanců – bodová hodnota 1,
- Střední hodnota aktiva – obsahuje osobni údaje občanů – bodová hodnota 3,
- Vysoká hodnota aktiva - obsahuje citlivé osobni údaje – bodová hodnota 5.

Následně byla provedena definice hrozeb a identifikace pravděpodobnosti výskytu hrozeb u daného aktiva. V dalším kroku bylo provedeno expertní posouzení zranitelnosti jednotlivých aktiv vůči hrozbám. Na závěr bude proveden výpočet celkové míry rizika.

[1] Např. dle zákona o kybernetické bezpečnosti a jeho prováděcí vyhlášky č. 316/2014 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti (dále jen „vyhláška o kybernetické bezpečnosti“)

Proces analýzy rizik obsahuje následující kroky:

- Určení a ohodnocení primárních aktiv,
- Identifikace pravděpodobnosti hrozeb,
- Identifikace zranitelnosti (rizikovosti),
- Výpočet celkové míry rizika.

Celý proces analýzy rizik obsahuje následující základní pojmy:

- hrozba (*threat*) – jakákoliv událost, která může způsobit narušení důvěrnosti, integrity a dostupnosti aktiva,
- zranitelnost (*vulnerability*) – vlastnost aktiva nebo slabina na úrovni fyzické, logické nebo administrativní bezpečnosti, která může být zneužita hrozbou,
- celková míra rizika – pravděpodobnost, že hrozba zneužije zranitelnost a způsobí narušení důvěrnosti, integrity nebo dostupnosti,
- opatření (*countermeasure*) – technické nebo organizační opatření, které snižuje zranitelnost a chrání aktivum před danou hrozbou.

1.2 Metoda určení a ohodnocení aktiv

Kolektiv určil primární aktiva v kontextu problematiky GDPR na základě úvodního sběru informací a jejich vyhodnocení. Aktivum chápeme jako objekt (aplikace, informační systém, kartotéka, spisovna, portál, evidence či jiné listinné nebo elektronické úložiště), který obsahuje osobní údaje v souladu s čl. 4 GDPR.

Klíčovým krokem posouzení rizik, která primárním aktivům hrozí, je ohodnocení samotných primárních aktiv. To je provedeno posouzením požadavků na důvěrnost, integritu a dostupnost aktiv, případně dat v aktivech obsažených a služeb aktivy poskytovaných.

Jelikož Správce nemá zavedený registr aktiv, který by obsahoval skutečné hodnoty těchto aktiv, byla Kolektivum vytvořena následující stupnice hodnoty primárních aktiv, která vyjadřuje, nakolik jsou tato primární aktiva pro Správce kritická:

Stupeň	Hodnota	Kritérium
1	Velmi nízká	Ztráta, poškození, narušení bezpečnosti primárního aktiva má jen nepatrný nebo žádný vliv na ochranu osobních údajů v rámci organizace Správce. Z pohledu GDPR obsahuje aktivum osobní údaje zaměstnanců Správce.
2	Nízká	Ztráta, poškození, narušení bezpečnosti primárního aktiva má nízký dopad na zákonné povinnosti Správce v rámci ochrany osobních údajů. Narušením primárního aktiva nedojde k uplatnění sankcí v rámci GDPR.
3	Střední	Ztráta, poškození, narušení bezpečnosti primárního aktiva má střední dopad na zákonné povinnosti Správce v rámci ochrany osobních údajů. Narušením primárního aktiva nedojde k uplatnění sankcí v rámci GDPR. Porušení zákonných povinností nebude mít zásadní vliv na fungování organizace Správce jako celku. Z pohledu GDPR obsahuje aktivum osobní údaje občanů.
4	Vysoká	Ztráta, poškození, narušení bezpečnosti primárního aktiva je velmi významná, může vést k neakceptovatelnému porušení zákonných požadavků v rámci ochrany osobních údajů. Narušením primárního aktiva pravděpodobně dojde k uplatnění sankcí v rámci GDPR. Porušení zákonných povinností bude mít vliv na fungování organizace Správce jako celku.
5	Velmi vysoká	Ztráta, poškození, narušení bezpečnosti primárního aktiva je katastrofická, může vést neakceptovatelnému porušení zákonných povinností ohledně ochrany osobních údajů vyplývajících z GDPR. Narušením primárního aktiva dojde k uplatnění sankcí v rámci GDPR. Porušení zákonných povinností bude mít zásadní vliv na fungování organizace Správce jako celku. Z pohledu problematiky GDPR aktivum obsahuje citlivé osobni údaje.

Kvalifikace aktiv byla provedena na základě expertního posouzení Kolektivum, jelikož přesná hodnota aktiv pro organizaci nebyla stanovena. Tuto metriku je vhodné následně zavést a zařadit ji do pravidelného hodnocení v rámci organizace.

1.3 Hrozby a identifikace pravděpodobnosti hrozeb

Prvním krokem hodnocení rizik byla identifikace hrozeb a zranitelností. Východiskem tohoto hodnocení je seznam obvyklých hrozeb dle standardů a hrozeb týkající se ochrany osobních údajů vycházejících z GDPR či vycházející z dané problematiky.

Chtěli bychom zdůraznit, že v rámci použité metodiky jsou úmyslně hodnoceny všechny možné hrozby podle našeho interního seznamu obvyklých hrozeb, a to i v případě, že se na Správce nevztahují. Například, pokud Správce nepoužívá VPN, přesto je hrozba napadení VPN v seznamu ponechána, i když riziko jejího napadení je následně ohodnoceno jako nulové. Tento metodický postup má dvě výhody – jednak není možno na některé obvyklé riziko omylem zapomenout. Ale hlavně, pokud by se někdy v budoucnosti stalo, že by Správce zavedl používání VPN, velmi snadno dokáže vyhodnocení rizik aktualizovat na existující stav.

Hrozba představuje vliv, jehož následkem je poškození analyzovaného systému IT a jeho aktiv. Cílem je identifikovat hrozby, kterým mohou být vystavena primární aktiva Správce v jeho správě nebo využívaná v jeho činnosti a pravděpodobnosti výskytu této hrozby.

1.3.1 Osobnostní práva subjektu údajů

Dle čl. 10 Listiny základních práv a svobod každý má právo, aby byla zachována jeho lidská důstojnost, osobní čest, dobrá pověst a chráněno jeho jméno. Každý má právo na ochranu před neoprávněným zasahováním do soukromého a rodinného života. Každý má právo na ochranu před neoprávněným shromažďováním, zveřejňováním nebo jiným zneužíváním údajů o své osobě.

Právní stát je založen na představě o jednotlivci jako důstojné lidské bytosti, rovné v právech se všemi ostatními bytostmi. Lidská důstojnost je všem ostatním hodnotám nadřazena, a proto také musí být tyto hodnoty definovány a vykládány v hranicích vymezených lidskou důstojností. **Povinností veřejné moci je zajistit respekt a ochranu nedotknutelné důstojnosti člověka** (čl. 1 odst. 1 Listiny základních práv a svobod). Rovnost jednotlivce v důstojnosti a právech je základem uznání hodnoty každého člověka, a to bez ohledu na jeho další charakteristiky (jako např. schopnosti či znalosti) a užitečnost či prospěšnost pro celek (nález Pl. ÚS 83/0. V nálezu IV. ÚS 412/04 Ústavní soud zdůraznil, že těžištěm ústavního pořádku je jednotlivec a jeho práva garantovaná tímto pořádkem. **Proto je třeba vycházet z priority občana nad státem, a tím i z priority základních občanských a lidských práv a svobod** (nález Pl. ÚS 43/93). Stát má povinnost důstojnost každého respektovat, a je-li třeba, musí ji i chránit vůči třetím osobám, neboť každý člověk má nárok na respekt a uznání své osoby. Subjektivní právo na zachování důstojnosti je výslovně garantováno čl. 10 odst. 1 Listiny základních práv a svobod.

V nálezech IV. ÚS 412/04 a I. ÚS 557/09 propojil Ústavní soud důstojnost se základním právem na osobnost. Nedotknutelnost lidské důstojnosti umožňuje člověku plně užívat jeho osobnosti.

Z práva na důstojnost a čest se dovozuje respekt k vlastnímu životu, fyzické, psychické a duchovní integritě, soukromí, osobní svobodě a k vlastnictví.

Právo na život obsažené v čl. 6 Listiny základních práv a svobod v sobě v ústavněprávním kontextu zahrnuje základní východisko, že lidský život je hoden absolutní ochrany pro jeho hodnotu samotnou, a to bez ohledu na rasu, pohlaví, národnost, občanství jednotlivce.

Právo na psychickou a duchovní integritu vyjadřuje zásadní nepřípustnost jakýchkoli nedobrovolných zásahů do tělesné schránky člověka a jeho vědomí. Z nedotknutelnosti osoby plyne, že jakýkoliv zásah do tělesné a duševní integrity je nepřípustný, pokud se tak neděje v rámci zákona, na základě svobodného a informovaného souhlasu dané osoby (s výjimkami, kdy souhlas není třeba, při současném absolutním zákazu mučení a ponižujícího zacházení). Součástí tohoto práva je i právo rozhodovat o vlastní fyzické a psychické integritě, což se pojí s případy přerušení těhotenství[2], jakož i s právem na sexuální sebeurčení, včetně sexuální orientace[3].

Jednou z nejvýznamnějších složek osobnosti každé fyzické osoby od narození až do smrti je její identita morální i fyzická, která ji zcela nezaměnitelně odlišuje od ostatních fyzických osob. Vážným zásahem do práva na ochranu osobnosti tak může proto být přiřazení osobních údajů určité osoby někomu, komu tyto identifikační údaje nepatří, nebo dokonce úmyslné zcizení něčí identity.

Specifickým problémem dotýkajícím se práv dětí je oprávněný zájem na tom, aby dítě znalo svoji identitu, včetně svého původu, svých předků, o čemž má být citlivým způsobem ve vhodné době informováno.

Právo na soukromí obsahuje právo učinit neveřejným záležitosti svého rodinného a partnerského života a projevů osobní povahy, o kterých se člověk rozhodne, že je nechce učinit veřejnými. Toto právo platí i tehdy, kdy se soukromé jednání uskutečňuje ve veřejném prostoru. Součástí práva na soukromí je právo na respekt k soukromému a rodinnému životu, jakož i k obydlí a ke korespondenci. Právo na soukromý život se v této dimenzi projevuje především jako negativní právo – svoboda, tj. jako právo bránící v první řadě veřejné moci ve vměšování (v zásazích) do tzv. osobní soukromé sféry. Nicméně lze z těchto práv dovodit i pozitivní závazek státu spočívající v takové právní úpravě, která zabrání i třetím, soukromým osobám zasahovat do osobní soukromé sféry. Zásahem

[2] ESLP ve věci Vo proti Francii, body 79 a násl.
[3] ESLP ve věci Dudgeon proti Spojenému království nebo Schalk a Kopf proti Rakousku, kde se právo na sebeurčení prolíná s rodinným životem

do osobní soukromé sféry je i sběr a uchovávání údajů týkajících se soukromého života a také sledování, hlídání a pronásledování ze strany veřejné moci, a to i ve veřejném prostoru či na veřejně přístupných místech. Do soukromého života řadíme i aktivity profesní, obchodní či sociální[4]. ESLP ve své judikatuře k právu na respekt k soukromému životu dle čl. 8 Úmluvy o ochraně lidských práv a základních svobod označil za zásahy do soukromí jednotlivců mimo jiné i zásahy v podobě kontroly dat, obsahu pošty a odposlechu telefonních hovorů[5], zjišťování telefonních čísel telefonujících osob[6], zjišťování údajů o telefonním spojení[7].

Z toho pak také přímo pramení důraz na ochranu před jakýmkoli nakládáním s osobními údaji, které by bylo prosto respektu k lidské důstojnosti, ohrožovalo by život, fyzickou, psychickou a duchovní integritu včetně její identity a také soukromí a další ústřední hodnoty, jako například osobní svobodu, nebo vlastnictví.

Z principu rovnosti v důstojnosti vyplývá současně zákaz diskriminace.

Podle ustálené judikatury ESLP se diskriminací rozumí rozdílné zacházení s osobami nacházejícími se ve srovnatelné situaci, které nemá objektivní a rozumné odůvodnění.

Přítomnost diskriminace lze zjistit následujícím testem:

a) k vyčlenění srovnatelného jednotlivce nebo skupiny;
b) ze zakázaného ("podezřelého, neospravedlnitelného") důvodu;
c) které mu je k tíži (uložením břemene nebo odepřením dobra); a
d) vyčleňování není možné ospravedlnit, tedy:
e) nesleduje žádný legitimní či akceptovatelný důvod (veřejného, legitimního zájmu)
f) opatření je nepřiměřené (disproporční).

Základním imperativem při tvorbě jakéhokoli systému nakládání s osobními údaji proto je, že musí vždy vytvářet vysoký stupeň ochrany ústavních práv, tedy klást tomu odpovídajícím způsobem důraz na ochranu života, fyzické, psychické a duchovní integrity, soukromí, případně osobní svobody a vlastnictví osob.

Měřítkem dostatečnosti respektu systému nakládání s osobními údaji k základním ústavním hodnotám bude, že systém úspěšně projde výše popsaným testem diskriminace a testem proporcionality. Čím

[4] srov. Rozsudek ESLP - Niemietz proti Německu
[5] viz. rozsudek Klass a další proti Německu, rozsudek Leander proti Švédsku, rozsudek Kruslin proti Francii či rozsudek Kopp proti Švýcarsku
[6] viz. rozsudek P. G. a J. H. proti Spojenému království
[7] srov. výše citované rozhodnutí ve věci Amman proti Švýcarsku

více se má zásah do soukromí jednotlivce dotýkat dat z jeho intimní sféry, tím přísnější nároky jsou kladeny na proporcionalitu takového zásahu.

Dále bude třeba vždy garantovat právo na informační sebeurčení, což je právo rozhodnout dle vlastního uvážení, zda, v jakém rozsahu a jakým způsobem a za jakých okolností mají být skutečnosti ze soukromého života zpřístupněny jiným subjektům (čl. 10 odst. 3 Listiny základních práv a svobod).

Např. **kamerové sledování veřejného prostoru** nebo preventivní síťové či plošné sledování, musí být vždy testovány z hlediska proporcionality zásahu do práva na soukromí (jeho omezení), přičemž přísné nároky jsou kladeny již na hodnocení samotné nutnosti zásahu do práva na informační sebeurčení. ESLP dovodil z práva na soukromý život v podobě práva na informační sebeurčení i pozitivní povinnost státu, který má, ovšem jen za určitých okolností, povinnost umožnit jednotlivci získat data, která z jeho soukromé sféry stát shromáždil a zpracoval[8].

U práva na informační sebeurčení se současně uplatní určitá omezení u veřejně činných osob, které musí strpět větší míru invaze do soukromí v zájmu veřejné kontroly nad svým počínáním, která má souvislost s výkonem veřejné aktivity. Taktéž musí strpět veřejnou kritiku, nikoli však zveřejňování nepravdivých informací o sobě.

Informační sebeurčení dítěte je modifikováno vůlí nositelů rodičovské zodpovědnosti. Ti by měli dbát, aby se veřejnost nedozvídala informace ze soukromého života dítěte, které mohou být vnímány jako pro dítě ponižující, zesměšňující či jinak způsobilé narušit jeho řádný (rozuměno zejména psychický) vývoj. Rodiče vykonávají rodičovskou zodpovědnost s ohledem na zájem dítěte.

Rozhodování třetích osob o nejlepších zájmech dítěte vychází z uspokojení základních potřeb dítěte (výživa, bydlení, zdraví), jeho rozvoje, názorů a přání dítěte, totožnosti dítěte, citového spojení, jeho zdraví, bezpečí, ochrany, zaopatření, péče, soudržnosti rodiny, trvalosti domova, vazeb dítěte na kamarády, ze školních vztahů, rizik náhradní péče, kulturního pozadí či náboženské víry). Samotné rozhodnutí pak musí sledovat cíl stabilního, a nikoliv přechodného řešení, které sleduje skutečně dlouhodobé zájmy dítěte.

Vedle práva na zachování cti a důstojnosti osob a práva na informační sebeurčení působí samostatně právo na informace upravené v článku 17 Listiny základních práv a svobod, kde garantuje právo na vyjádření názoru, tedy i přesvědčení a idejí, a to jakoukoliv formou; dále garantuje svobodu vyhledávat, přijímat a rozšiřovat ideje a informace, a to bez ohledu na hranice státu.

Při střetu základního politického práva na informace a jejich šíření s právem na ochranu osobnosti a soukromého života, tedy základních práv, která stojí na stejné úrovni, bude vždy věcí nezávislých

[8] rozsudek Rotaru proti Rumunsku

soudů, aby s přihlédnutím k okolnostem každého jednotlivého případu pečlivě zvážily, zda jednomu právu nebyla nedůvodně dána přednost před právem druhým. Ústavní soud odepřel ochranu sdělování vědomě nepravdivých informací (nález I. ÚS 453/03). Přitom uvedl, že legitimitu zveřejnění informace nelze dovodit, pokud byla dominantně motivována touhou poškodit difamovanou osobu, pokud si šiřitel sám informaci neověřil, anebo pokud ji poskytl bezohledně, aniž by se řádně staral o to, zda je či není pravdivá.

Ústavní soud ve své judikatuře vychází z teze, podle níž jednotlivec musí mít k dispozici informace o fungování státní moci k utvoření si svobodného názoru za účelem toho, aby mohl případně iniciovat či participovat na veřejné diskusi, a tak státní moc kontrolovat (Pl. ÚS 2/10). V poslední době judikatura Ústavního soudu také brání zneužívání práva na informace a vyvažuje toto právo s oprávněnými zájmy subjektů dat (IV. US 1378/1.

Čl. 17 odst. 5 Listiny základních práv a svobod ukládá veřejné správě přiměřeným způsobem poskytovat informace o své činnosti, což se děje zejména v mezích správního řádu a zákona o svobodném přístupu k informacím.

1.3.2 Detailní popis relevantních hrozeb

V následující tabulce jsou uvedeny hrozby, která jsou relevantní k posuzovaným primárním aktivům. Vždy je uvedena kategorie hrozeb a vysvětlení, co se pod jejich jednotným označením skrývá.

Hrozby – kategorie	Popis
Vnější útoky	• Zneužití přístupu k PC s možností neautorizovaného přístupu k OÚ nebo diskreditace OÚ; • Zneužití přístupu k počítačové síti s možností neautorizovaného přístupu k OÚ nebo diskreditace OÚ; • Krádež nebo prolomení hesla do IS nebo aplikace s možností neautorizovaného přístupu k OÚ nebo diskreditace OÚ; • Útok na IS nebo aplikace s cílem diskreditace či zcizení OÚ nebo omezení funkčnosti; • Útok na web s možností zcizení nebo modifikace OÚ, která jsou na webové prezentaci uvedeny; • Cílený útok na OÚ s motivem jejich odcizení a neoprávněného užití s možností cílené diskreditace organizace; • Narušení referenčních OÚ v aplikacích nebo IS; • Fyzické zcizení nebo poškození primárního aktiva včetně listinných evidencí s osobními daty; • Průnik z vnější sítě do vnitřní sítě (prolomení perimetru) s cílem zcizení nebo kompromitace OÚ, uložených v IS nebo aplikacích;

Hrozby – kategorie	Popis
	• Kompromitace dohledových prostředků nebo prostředků ke sledování a monitorování přístupu k OÚ; • Kompromitace identity oprávněného uživatele Správce nebo Kolektivu.
Technické chyby	• Chyby zálohování; • Výpadek elektřiny; • Výpadek hardwaru koncové stanice; • Výpadek softwaru koncové stanice; • Poškození nebo ztráta dat; • Mechanické poškození listinné evidence osobních údajů; • Narušení řádné čitelnosti listinné evidence osobních údajů; • Poškození/selhání programového vybavení; • Nedostatečná ochrana vnějšího perimetru; • Nedostatečná údržba informačního systému nebo aplikace, kde jsou evidovány OÚ; • Nedostatečné postupy při identifikaci a odhalení incidentů; • Dlouhodobé přerušení podpory dodavatele SW; • Nedostatečná ochrana prostředků IS; • Technické chyby ochrany úložišť listin obsahující OÚ.
Lidský faktor	• Obecná chyba uživatele; • Opomenutí uživatele; • Nedostatečné školení nebo povědomí o nakládání s OÚ nebo jejich ochraně OÚ; • Zkoušení prolomení zabezpečení uživatelem; • Poškození fyzické vrstvy sítě; • Zavlečení škodlivého SW; • Porušení bezpečnostní politiky uživatelem; • Zneužití oprávnění ze strany uživatelů; • Zneužití oprávnění ze strany administrátorů; • Narušení fyzické bezpečnosti – kancelář, serverovna; • Nepřítomnost/zranění/smrt administrátora informačního systému; • Nedostatečné vymezení bezpečnostních pravidel; • Nedostatečná míra nezávislé kontroly; • Nedostatečná ochrana úložišť listin obsahující OÚ.
Narušení integrity OÚ	• Neoprávněné manipulování evidencemi OÚ na úrovni IS nebo aplikací pod správou Správce; • Neoprávněné manipulování s listinnými evidencemi obsahující OÚ; • Provedení neoprávněných činností; • Zneužití vedených osobních údajů; • Nevhodné či nesprávné nastavení přístupových oprávnění; • Fyzické narušení listiny obsahující OÚ.
Neoprávněný přístup	• K OÚ má přístup osoba, která k danému úkonu nemá oprávnění; • Modifikace vedených OÚ; • Nedostatečné monitorování činnosti uživatelů; • Nedostatečné monitorování činnosti administrátorů.
Narušení dostupnosti	• Nedostupnost osobních údajů z důvodu pochybení organizačního charakteru; • Nedostupnost osobních údajů z důvodu technického pochybení.

Hrozby – kategorie	Popis
Ztráta osobních údajů	• Nevhodná manipulace s listinnou evidencí obsahující OÚ; • Technické chyby v IS uchovávající osobní údaje; • Úmyslné zcizení OÚ v listinné podobě z listinné evidence; • Úmyslný export OÚ z IS nebo aplikací; • Výmaz OÚ z IS nebo aplikací; • Předání listinné evidence OÚ neautorizované osobě bez udání důvodu a bez dostatečné evidence a povinnosti navrátit předané OÚ.
Narušení práv a svobod subjektu údajů	• Narušení práva na soukromí; • Narušení práva na ochranu cti a důstojnosti; • Narušení práva na informační sebeurčení; • Narušení práva na život; • Narušení práva na duševní a tělesnou integritu; • Narušení práva subjektu údajů na informace a přístupu k osobním údajům; • Narušení práva subjektu údajů na výmaz (právo být zapomenut); • Narušení práva subjektu údajů na omezení zpracování OÚ; • Narušení práva subjektu údajů na přenositelnost OÚ; • Narušení práva na ochranu OÚ; • Úmyslná kompromitace osobních údajů třetím subjektem; • Narušení zákazu diskriminace; • Narušení ochrany identity; • Hmotné ztráty subjektu údajů; • Neoprávněné zrušení pseudonymizace.

Dále je pro každé aktivum posouzena pravděpodobnost výskytu hrozby. Pro vlastní analýzu byla použita následující kritéria pro hodnocení pravděpodobnosti hrozby:

Stupeň	Četnost výskytu, Pravděpodobnost	Kritérium
1	Velmi nízká	Uplatnění hrozby je vysoce nepravděpodobné nebo nulové.
2	Nízká	Hrozba se může uplatnit méně než 1 x za rok, resp. nebo kritické období.
3	Střední	Hrozba se může uplatnit zhruba 1x za rok, resp. hrozba se jednou uplatnila v průběhu kritického období.
4	Vysoká	Hrozba se může uplatnit zhruba 1x za měsíc, resp. hrozba se uplatnila jednou v průběhu více než 1x v kritickém období.
5	Velmi vysoká	Hrozba se může uplatnit zhruba 1x týdně, resp. hrozba se uplatnila denně v kritickém období.

1.3.3 Identifikace zranitelnosti (rizikovosti)

Odhad zranitelností zahrnuje slabá místa posuzovaných aktiv. Pro analýzu byla použita následující kritéria pro hodnocení zranitelností:

Stupeň	Zranitelnost aktiva	Kritérium
0	Žádná	Vyhrazeno pro případy, kdy aktivum u Správce neexistuje (blíže viz vysvětlení v kapitole Hodnocení pravděpodobnosti hrozeb k aktivům)
1	Velmi nízká	Hrozba se nemůže vůči aktivu uplatnit.
2	Nízká	Aktivum je chráněno, resp. je odolné velmi dobře proti uplatnění hrozby.
3	Střední	Aktivum je chráněno částečně resp. je mírně odolné proti uplatnění hrozby.
4	Vysoká	Aktivum je chráněno, resp. je odolné velmi nedostatečně proti uplatnění hrozby.
5	Velmi vysoká	Aktivum není chráněno vůbec.

Míra zranitelnosti a účinnost existujících ochranných opatření spolu úzce souvisí. Míra zranitelnosti určitou hrozbou je vlastností aktiva. Může být snížena jedině vhodným protiopatřením.

1.3.4 Celková míra rizika (riziková expozice)

Cílem identifikace míry rizika bylo zajištění optimálního výběru ochranných nebo nápravných opatření, která působí proti těmto rizikům.

Ohodnocení míry rizika se provádí jako kombinace (součin) tří hodnot:

- Hodnota aktiva na stupnici velmi nízká, nízká, střední, vysoká, velmi vysoká.
- Pravděpodobnost hrozby na stupnici velmi nízká, nízká, střední, vysoká, velmi vysoká.
- Zranitelnost na stupnici velmi nízká, nízká, střední, vysoká, velmi vysoká.

Celková míra rizika je tak určena bezrozměrným číslem – rizikovým skóre. Bezrozměrné číslo je zvoleno, protože hodnocení je kalkulováno z heterogenních hodnot, které nelze převést na stejnorodé jednotky.

Rizikové skóre se vypočítává podle níže uvedené rovnice:

Rizikové skóre = hodnota aktiva * pravděpodobnost * zranitelnost

Rizikové skóre se pohybuje v rozmezí 0–125 bodů. Hranice akceptovatelného rizika je předmětem manažerského rozhodnutí na straně Správce, u kterého byla analýza rizik prováděna. Celková míra expozice pak doporučuje pořadí priorit při řešení a implementaci organizačních a technických opatření.

1.4 Metoda vyhodnocení vstupní analýzy

Veškeré poznatky zjištěné v průběhu dílčích analýz popsaných v předchozích podkapitolách byly následně vyhodnoceny a jsou adresovány nejzávažnější problémy v právní, technické a organizační oblasti.

Jakmile byly tyto problémy identifikovány, provedl Kolektiv jejich detailní popis a navrhnul adekvátní opatření, která budou směřovat ke zlepšení současné situace.

Posledním navazujícím krokem byla příprava plánu implementace. Tento plán obsahuje doporučený postup Správce pro implementaci opatření v oblasti technické, organizační a právní.

Kolektiv pro potřeby této systémové analýzy sloučil rizika při jejich hodnocení do tří kategorií, a to nízká rizika, běžná a vysoká. Zbytkové riziko Kolektiv neuvažuje.

Vyhodnocená vstupní analýza (tedy tak zvaná rozdílová analýza, *Gap Analysis*) je předmětem studie v následujícím svazku.

2. ZHODNOCENÍ RIZIK (DPIA) U SPRÁVCE

2.1 Analýza a hodnocení rizik

Analýzou a hodnocením rizik je míněno posouzení vlivu na ochranu osobních údajů DPIA (Data Protection Impact Assessment) podle Nařízení GDPR. Cílem analýzy rizik je provést posouzení rizik vztahujících se k primárním a podpůrným aktivům při jejich zpracování v rámci správce osobních údajů. Analýza rizik je prováděna kvalitativně za účasti vedoucích pracovníků správce.

V rámci analýzy rizik jsou hodnoceny všechny hrozby a zranitelnosti definované v §4, odst. 4 až 7 vyhlášky č. 316/2014 Sb., přičemž uvedené hrozby a zranitelnosti jsou dále detailizovány či rozděleny podle potřeby.

Hodnocení hrozeb a zranitelností je prováděno ze dvou různých pohledů. Jedná se o:

a) Riziko zpracování pro práva subjektu údajů (Impact)

b) Riziko zpracování pro zajištění bezpečnosti, které má tři složky:

- Dopad do plnění úkolů nebo podnikání správce (Dopad, resp Hodnota)
- Četnost hrozby (Četnost, resp. Pravděpodobnost)
- Zranitelnost daného aktiva (Zranitelnost)

2.2 Rizika zpracování osobních údajů

Na základě definovaných primárních aktiv Kolektiv provedl jejich ohodnocení, a to dle stupnice, která je definována v kapitole Metoda určení a ohodnocení aktiv. Kolektiv podotýká, že tato analýza rizik je prováděna z pohledu subjektu údajů dle nařízení GDPR. Hodnota aktiv a další stanovení parametrů analýzy rizik jsou stanoveny z pohledu dopadu na subjekt údajů nebo na informace, které obsahují osobní údaje subjektu údajů.

Ohodnocení aktiv (Hodnota) pro účely analýzy rizik je uvedeno v tabulce:

Název Aktiva	Stupeň hodnocení	Popis hodnocení
Listinné úložiště v rámci výkonu agend Správce	**5**	Kolektiv obecně hodnotíohodnotil aktivum na nejvyšší stupeň hodnoty, jelikož v tomto aktivu je vysoká koncentrace osobních údajů a osobních údajů, které se dají označit jako citlivé včetně osobních údajů vztahujících se ke kategorii zvláště zranitelných subjektů údajů. Z pohledu dopadu na subjekty osobních údajů se jedná o vysoký stupeň dopadu na práva a dalších povinností vyplývající z nařízení GDPR ke vztahu subjektům osobních údajů. Dalším důvodem pro vysoký stupeň hodnocení aktiva je dopad realizace práv subjektů osobních údajů na toto aktivum. Ztráta, poškození, narušení bezpečnosti primárního aktiva je katastrofická, může vést neakceptovatelnému porušení zákonných povinností ohledně ochrany osobních údajů vyplývajících z GDPR. Narušením primárního aktiva dojde k uplatnění sankcí v rámci GDPR. Porušení zákonných povinností bude mít zásadní vliv na fungování organizace jako celku a mají zásadní dopad na subjekt údajů a realizaci práv subjektu údajů.
Listinné úložiště v rámci vnitřního chodu Správce	**3**	Kolektiv obecně hodnotíohodnotil aktivum na střední hodnotu, a to z důvodu, že obsah tohoto aktiva, a tedy i všechny osobní údaje vedené v tomto aktivu závisí na libovolném rozhodnutí Správce. Aktivum nedisponuje takovou širokou škálou osobních údajů jako v případě úložiště spojené s výkonem agend Správce vůči občanům. Kolektiv nepředpokládá, že v rámci ztráty, poškození a narušení bezpečnosti tohoto aktiva by došlo k uplatnění sankcí vyplývající z GDPR. Narušení aktiva nebude mít zásadní vliv na fungování Správce.

Název Aktiva	Stupeň hodnocení	Popis hodnocení
Informační systém spisové služby	**5**	Kolektiv obecně hodnotíohodnotil aktivum na nejvyšší stupeň hodnoty, jelikož v tomto aktivu je vysoká koncentrace osobních údajů a osobních údajů, které se dají označit jako citlivé včetně osobních údajů vztahujících se ke kategorii zvláště zranitelných subjektů údajů. Z pohledu dopadu na subjekty osobních údajů se jedná o vysoký stupeň dopadu na práva a dalších povinností vyplývající z nařízení GDPR ke vztahu subjektům osobních údajů. Dalším důvodem pro vysoký stupeň hodnocení aktiva je dopad realizace práv subjektů osobních údajů na toto aktivum. Ztráta, poškození, narušení bezpečnosti primárního aktiva je katastrofická, může vést neakceptovatelnému porušení zákonných povinností ohledně ochrany osobních údajů vyplývajících z GDPR. Narušením primárního aktiva dojde k uplatnění sankcí v rámci GDPR. Porušení zákonných povinností bude mít zásadní vliv na fungování organizace jako celku a mají zásadní dopad na subjekt údajů a realizaci práv subjektu údajů.
Agendové informační systémy	**5**	Kolektiv obecně hodnotíohodnotil aktivum na nejvyšší stupeň hodnoty, jelikož v tomto aktivu je vysoká koncentrace osobních údajů a osobních údajů, které se dají označit jako citlivé včetně osobních údajů vztahujících se ke kategorii zvláště zranitelných subjektů údajů. Z pohledu dopadu na subjekty osobních údajů se jedná o vysoký stupeň dopadu na práva a dalších povinností vyplývající z nařízení GDPR ke vztahu subjektům osobních údajů. Dalším důvodem pro vysoký stupeň hodnocení aktiva je dopad realizace práv subjektů osobních údajů na toto aktivum. Ztráta, poškození, narušení bezpečnosti primárního aktiva je katastrofická, může vést k neakceptovatelnému porušení zákonných povinností ohledně ochrany osobních údajů vyplývajících z GDPR. Narušením primárního aktiva dojde k uplatnění sankcí v rámci GDPR. Porušení zákonných povinností bude mít zásadní vliv na fungování organizace jako celku a mají zásadní dopad na subjekt údajů a realizaci práv subjektu údajů.
Ekonomický informační systém	**5**	Kolektiv obecně hodnotíohodnotil aktivum na nejvyšší stupeň hodnoty, jelikož v tomto aktivu je vysoká koncentrace osobních údajů a osobních údajů, které se dají označit jako citlivé včetně osobních údajů vztahujících se ke kategorii zvláště zranitelných subjektů údajů. Z pohledu dopadu na subjekty osobních údajů se jedná o vysoký stupeň dopadu na práva a dalších povinností vyplývající z nařízení GDPR ke vztahu subjektům osobních údajů. Dalším důvodem pro vysoký stupeň hodnocení aktiva je dopad realizace práv subjektů osobních údajů na toto aktivum. Ztráta, poškození, narušení bezpečnosti primárního aktiva je katastrofická, může vést neakceptovatelnému porušení zákonných povinností ohledně ochrany osobních údajů vyplývajících z GDPR. Narušením primárního aktiva dojde k uplatnění sankcí v rámci GDPR. Porušení zákonných povinností bude mít zásadní vliv na fungování organizace jako celku a mají zásadní dopad na subjekt údajů a realizaci práv subjektu údajů.

Název Aktiva	Stupeň hodnocení	Popis hodnocení
Portály	**3**	Kolektiv obecně hodnotíohodnotil aktivum na střední hodnotu, a to z důvodu, že obsah tohoto aktiva, a tedy i všechny osobní údaje vedené v tomto aktivu závisí na libovolném rozhodnutí Správce. Aktivum nedisponuje takovou širokou škálou osobních údajů jako v případě úložiště spojené s výkonem agend Správce vůči občanům. V rámci ztráty, poškození a narušení bezpečnosti tohoto aktiva nedojde k uplatnění sankcí vyplývající z GDPR. Narušení aktiva nebude mít vliv na fungování Správce.
Ostatní elektronická úložiště	**1**	Kolektiv obecně hodnotíohodnotil aktivum na běžnou hodnotu, a to z důvodu, že obsah tohoto aktiva, a tedy i všechny osobní údaje vedené v tomto aktivu závisí na libovolném rozhodnutí Správce. V rámci ztráty, poškození a narušení bezpečnosti tohoto aktiva nedojde k uplatnění sankcí vyplývající z GDPR. Narušení aktiva nebude mít vliv na fungování Správce.

Kolektiv v kapitole Hrozby a identifikace pravděpodobnosti hrozeb uvedl seznam obvyklých hrozeb dle standardů a hrozeb týkající se ochrany osobních údajů vycházejících z GDPR či z dané problematiky.

Kolektiv k jednotlivým hrozbám přiřadil pravděpodobnost uplatnění jednotlivých hrozeb, a to ke každému identifikovanému aktivu. Stupnice ohodnocení aktiv je uvedena v kapitole Hrozby a identifikace pravděpodobnosti hrozeb.

2.3 Hodnocení pravděpodobnosti hrozeb k aktivům

Kolektiv uvedl do hodnocení výši stupně pravděpodobnosti uplatnění hrozby včetně popisu zvolení dané výše pravděpodobnosti. Hodnocení pravděpodobnosti uplatnění hrozeb na jednotlivá aktiva je pro obecné případy organizací obdobných Správci uvedeno v tabulce.

	Listinné úložiště v rámci výkonu agend Správce	Listinné úložiště v rámci vnitřního chodu Správce	Informační systém spisové služby	Agendové informační systémy	Ekonomický informační systém	Portály	Ostatní elektronická úložiště
Vnější útoky	2	2	2	2	2	4	1
Technické chyby	2	1	3	2	3	3	2
Lidský faktor	3	3	2	3	3	3	3
Narušení integrity OÚ	3	2	2	2	2	2	2
Neoprávněný přístup	3	2	3	2	2	2	4
Narušení dostupnosti	2	2	3	3	3	3	2
Ztráta osobních údajů	2	2	2	2	2	2	3
Narušení práv a svobod subjektu údajů	3	2	2	2	2	2	3

2.4 Zranitelnosti aktiv vůči hrozbám

Kolektiv na základě zjištěných informací z mapování Správce přiřadil jednotlivým hrozbám zranitelnosti jednotlivých hrozeb, a to ke každému identifikovanému aktivu. Kolektiv uvedl do hodnocení výši stupně zranitelnosti aktiv vůči hrozbám včetně popisu zvoleného stupně zranitelnosti.

Hodnocení zranitelnosti aktiv vůči hrozbám je uvedeno v tabulce:

Název Aktiva	Hrozba	Zranitelnost	Hodnocení zranitelnosti
Listinné úložiště v rámci výkonu agend Správce	**Vnější útoky**	3	Na základě zjištěných informací Kolektiv přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na střední hodnotu. Zabezpečení listinných úložišť u oSprávce na nízké úrovni. Listiny nejsou většinou uloženy v uzamykatelných skříních a vstupy do místností, kde jsou listiny uloženy, nepředstavují zásadní překážku pro vnější útoky.
	Technické chyby	3	Na základě zjištěných informací Kolektiv přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na střední hodnotu. Ochrana před technickými chybami či vnějšími vlivy nedosahuje u Správce takové úrovně, aby byla zranitelnost ohodnocena na nízké úrovni. [redacted]
	Lidský faktor	4	Na základě zjištěných informací Kolektiv přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na vysokou hodnotu. Vysoká hodnota zranitelnosti tohoto aktiva byla Kolektivum stanovena z důvodu absence vnitřních předpisů zahrnující procesy nakládání s listinami a jejich úložišť, popřípadě absence školení v rámci ochrany osobních údajů.
	Narušení integrity OÚ	3	Na základě zjištěných informací Kolektiv přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na střední hodnotu. Střední hodnota zranitelnosti tohoto aktiva byla Kolektivum stanovena z důvodu absence vnitřních předpisů zahrnující procesy nakládání s listinami a jejich úložišť včetně procesů jejich zabezpečení.
	Neoprávněný přístup	3	Na základě zjištěných informací Kolektiv přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na střední hodnotu. [redacted]

Název Aktiva	Hrozba	Zranitelnost	Hodnocení zranitelnosti
	Narušení dostupnosti	2	Na základě zjištěných informací Kolektiv přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na nízkou hodnotu. Narušení dostupnosti osobních údajů u Správce je na nízké úrovni, a to i z důvodu menšího počtu agend.
	Ztráta osobních údajů	4	Na základě zjištěných informací Kolektiv přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na vysokou hodnotu. Vysoká hodnota zranitelnosti tohoto aktiva byla Kolektivum stanovena z důvodu absence vnitřních předpisů zahrnující procesy nakládání s listinami a jejich úložišť, [redacted]
	Narušení práv a svobod subjektu údajů	4	Na základě zjištěných informací Kolektiv přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na vysokou hodnotu. Vysoká hodnota zranitelnosti tohoto aktiva byla Kolektivum stanovena z důvodu zneužití osobních údajů v tomto aktivu, které by mělo za následek narušení práv a svobod subjektu údajů.
Listinné úložiště v rámci vnitřního chodu Správce	**Vnější útoky**	3	Na základě zjištěných informací Kolektiv přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na střední hodnotu. Zabezpečení listinných úložišť je u Správce na nízké úrovni. Listiny nejsou většinou uloženy v uzamykatelných skříních a vstupy do místností, kde jsou listiny uloženy, nepředstavují zásadní překážku pro vnější útoky.
	Technické chyby	3	Na základě zjištěných informací Kolektiv přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na střední hodnotu. Ochrana před technickými chybami či vnějšími vlivy nedosahuje u Správce takové úrovně, aby byla zranitelnost ohodnocena na nízké úrovni. [redacted]
	Lidský faktor	4	Na základě zjištěných informací Kolektiv přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na vysokou hodnotu. Vysoká hodnota zranitelnosti tohoto aktiva byla Kolektivum stanovena z důvodu absence vnitřních předpisů zahrnující procesy nakládání s listinami a jejich úložišť, popřípadě absence školení v rámci ochrany osobních údajů.
	Narušení integrity OÚ	3	Na základě zjištěných informací Kolektiv přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na střední hodnotu. Střední hodnota zranitelnosti tohoto aktiva byla Kolektivum stanovena z důvodu absence vnitřních předpisů zahrnující procesy nakládání s listinami a jejich úložišť včetně procesů jejich zabezpečení.

Název Aktiva	Hrozba	Zranitelnost	Hodnocení zranitelnosti
	Neoprávněný přístup	3	Na základě zjištěných informací Kolektiv přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na střední hodnotu. [redacted]
	Narušení dostupnosti	2	Na základě zjištěných informací Kolektiv přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na nízkou hodnotu. Narušení dostupnosti osobních údajů u Správce je na nízké úrovni, a to i z důvodu menšího počtu agend.
	Ztráta osobních údajů	4	Na základě zjištěných informací Kolektiv přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na vysokou hodnotu. Vysoká hodnota zranitelnosti tohoto aktiva byla Kolektivum stanovena z důvodu absence vnitřních předpisů zahrnující procesy nakládání s listinami a jejich úložišť, [redacted]
	Narušení práv a svobod subjektu údajů	4	Na základě zjištěných informací Kolektiv přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na vysokou hodnotu. Vysoká hodnota zranitelnosti tohoto aktiva byla Kolektivum stanovena z důvodu zneužití osobních údajů v tomto aktivu, které by mělo za následek narušení práv a svobod subjektu údajů.
Informační systém spisové služby	**Vnější útoky**	2	Na základě zjištěných informací Kolektiv přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na nízkou hodnotu. Ochrana informačního systému spisové služby je na vysoké úrovni a většinou jsou uložiště hostované u poskytovatele IS spisové služby, které je dostatečně zabezpečeno.
	Technické chyby	2	Na základě zjištěných informací Kolektiv přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na nízkou hodnotu. Ochrana informačního systému spisové služby je na vysoké úrovni a většinou jsou uložiště hostované u poskytovatele IS spisové služby, které je dostatečně zabezpečeno. IS spisové služby jsou ochráněny před technickými chybami, které by mohly nastat a nedochází ke ztrátě či zcizení dat.
	Lidský faktor	2	Na základě zjištěných informací Kolektiv přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na nízkou hodnotu. Nízká úroveň byla Kolektivum zvolena s ohledem na již dlouhou tradici IS spisových služeb u Správce, kde jsou zaběhlé procesy využívání daného IS a u Správce nedochází k časté fluktuaci zaměstnanců pracujících s daným IS.

Název Aktiva	Hrozba	Zranitelnost	Hodnocení zranitelnosti
	Narušení integrity OÚ	2	Na základě zjištěných informací Kolektiv přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na nízkou hodnotu. Nízká úroveň byla Kolektivum zvolena s ohledem na již dlouhou tradici IS spisových služeb u Správce, kde jsou zaběhlé procesy využívání daného IS a u Správce nedochází k časté fluktuaci zaměstnanců pracujících s daným IS.
	Neoprávněný přístup	2	Na základě zjištěných informací Kolektiv přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na nízkou hodnotu. Nízká úroveň byla Kolektivum zvolena s ohledem na omezený počet zaměstnanců Správce, kteří mají přístupy do IS spisové služby a nedochází k časté fluktuaci osob mající přístupy do IS spisové služby. Dané osoby mají již zavedené procesy užití IS spisové služby, takže by nemělo docházet k neoprávněným přístupům k IS spisové služby.
	Narušení dostupnosti	3	Na základě zjištěných informací Kolektiv přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na střední hodnotu.
	Ztráta osobních údajů	3	Na základě zjištěných informací Kolektiv přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na střední hodnotu. [redacted]
	Narušení práv a svobod subjektu údajů	3	Na základě zjištěných informací Kolektiv přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na střední hodnotu. Střední hodnota zranitelnosti tohoto aktiva byla Kolektivum stanovena z důvodu zneužití osobních údajů v tomto aktivu, které by mělo za následek narušení práv a svobod subjektu údajů, a to i s ohledem na zranitelnosti aktiva k ostatním hrozbám.
Agendové informační systémy	**Vnější útoky**	2	Na základě zjištěných informací Kolektiv přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na nízkou hodnotu. Ochrana Agendového informačního systému je na vysoké úrovni a většinou jsou uložiště hostované u poskytovatele AIS, které je dostatečně zabezpečeno.
	Technické chyby	2	Na základě zjištěných informací Kolektiv přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na nízkou hodnotu. Ochrana AIS je na vysoké úrovni a většinou jsou uložiště hostované u poskytovatele AIS, které je dostatečně zabezpečeno. AIS jsou ochráněny před technickými chybami, které by mohly nastat a nedochází ke ztrátě či zcizení dat.
	Lidský faktor	2	Na základě zjištěných informací Kolektiv přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na nízkou hodnotu. Nízká úroveň byla Kolektivum zvolena s ohledem na již dlouhou tradici AIS u Správce, kde jsou zaběhlé procesy využívání daného IS a u Správce nedochází k časté fluktuaci zaměstnanců pracujících s daným AIS.

Název Aktiva	Hrozba	Zranitelnost	Hodnocení zranitelnosti
	Narušení integrity OÚ	2	Na základě zjištěných informací Kolektiv přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na nízkou hodnotu. Nízká úroveň byla Kolektivum zvolena s ohledem na již dlouhou tradici AIS u Správce, kde jsou zaběhlé procesy využívání daného IS a u Správce nedochází k časté fluktuaci zaměstnanců pracujících s daným AIS.
	Neoprávněný přístup	3	Na základě zjištěných informací Kolektiv přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na střední hodnotu. Střední úroveň byla Kolektivum zvolena s ohledem na omezený počet zaměstnanců Správce, kteří mají přístupy do AIS a nedochází k časté fluktuaci osob mající přístupy do AIS. [redacted]
	Narušení dostupnosti	3	Na základě zjištěných informací Kolektiv přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na střední hodnotu.
	Ztráta osobních údajů	3	Na základě zjištěných informací Kolektiv přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na střední hodnotu. [redacted]
	Narušení práv a svobod subjektu údajů	3	Na základě zjištěných informací Kolektiv přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na střední hodnotu. Střední hodnota zranitelnosti tohoto aktiva byla Kolektivum stanovena z důvodu zneužití osobních údajů v tomto aktivu, které by mělo za následek narušení práv a svobod subjektu údajů, a to i s ohledem na zranitelnosti aktiva k ostatním hrozbám.
Agendové informační systémy	**Vnější útoky**	2	Na základě zjištěných informací Kolektiv přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na nízkou hodnotu. Ochrana Agendového informačního systému je na vysoké úrovni a většinou jsou uložiště hostované u poskytovatele AIS, které je dostatečně zabezpečeno.
	Technické chyby	2	Na základě zjištěných informací Kolektiv přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na nízkou hodnotu. Ochrana AIS je na vysoké úrovni a většinou jsou uložiště hostované u poskytovatele AIS, které je dostatečně zabezpečeno. AIS jsou ochráněny před technickými chybami, které by mohly nastat a nedochází ke ztrátě či zcizení dat.
	Lidský faktor	2	Na základě zjištěných informací Kolektiv přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na nízkou hodnotu. Nízká úroveň byla Kolektivum zvolena s ohledem na již dlouhou tradici AIS u Správce, kde jsou zaběhlé procesy využívání daného IS a u Správce nedochází k časté fluktuaci zaměstnanců pracujících s daným AIS.

Název Aktiva	Hrozba	Zranitelnost	Hodnocení zranitelnosti
	Narušení integrity OÚ	2	Na základě zjištěných informací Kolektiv přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na nízkou hodnotu. Nízká úroveň byla Kolektivum zvolena s ohledem na již dlouhou tradici AIS u Správce, kde jsou zaběhlé procesy využívání daného IS a u Správce nedochází k časté fluktuaci zaměstnanců pracujících s daným AIS.
	Neoprávněný přístup	3	Na základě zjištěných informací Kolektiv přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na střední hodnotu. Střední úroveň byla Kolektivum zvolena s ohledem na omezený počet zaměstnanců Správce, kteří mají přístupy do AIS a nedochází k časté fluktuaci osob mající přístupy do AIS. [redacted]
	Narušení dostupnosti	3	Na základě zjištěných informací Kolektiv přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na střední hodnotu.
	Ztráta osobních údajů	3	Na základě zjištěných informací Kolektiv přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na střední hodnotu. [redacted]
	Narušení práv a svobod subjektu údajů	3	Na základě zjištěných informací Kolektiv přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na střední hodnotu. Střední hodnota zranitelnosti tohoto aktiva byla Kolektivum stanovena z důvodu zneužití osobních údajů v tomto aktivu, které by mělo za následek narušení práv a svobod subjektu údajů, a to i s ohledem na zranitelnosti aktiva k ostatním hrozbám.
Ekonomický informační systém	**Vnější útoky**	2	Na základě zjištěných informací Kolektiv přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na nízkou hodnotu. Ochrana Ekonomického informačního systému je na vysoké úrovni a většinou jsou uložiště hostované u poskytovatele Ekonomického informačního systému, které je dostatečně zabezpečeno.
	Technické chyby	3	Na základě zjištěných informací Kolektiv přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na střední hodnotu. [redacted]
	Lidský faktor	3	Na základě zjištěných informací Kolektiv přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na střední hodnotu. Střední úroveň byla Kolektivum zvolena s ohledem na možnost způsobení chyb uživateli Ekonomického informačního systému, a to i z důvodu nezavedení interních aktů, které by řešili procesy užití Ekonomického IS.

Název Aktiva	Hrozba	Zranitelnost	Hodnocení zranitelnosti
	Narušení integrity OÚ	3	Na základě zjištěných informací Kolektiv přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na střední hodnotu. Střední úroveň byla Kolektivum zvolena s ohledem na možnost způsobení chyb uživateli Ekonomického informačního systému, a to i z důvodu nezavedení interních aktů, které by řešily procesy užití Ekonomického IS. [redacted]
	Neoprávněný přístup	3	Na základě zjištěných informací Kolektiv přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na střední hodnotu. Střední úroveň byla Kolektivum zvolena s ohledem na omezený počet zaměstnanců Správce, kteří mají přístupy do Ekonomického IS a nedochází k časté fluktuaci osob mající přístupy do Ekonomického IS.
	Narušení dostupnosti	3	Na základě zjištěných informací Kolektiv přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na střední hodnotu.
	Ztráta osobních údajů	3	Na základě zjištěných informací Kolektiv přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na střední hodnotu. [redacted]
	Narušení práv a svobod subjektu údajů	3	Na základě zjištěných informací Kolektiv přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na střední hodnotu. Střední hodnota zranitelnosti tohoto aktiva byla Kolektivum stanovena z důvodu zneužití osobních údajů v tomto aktivu, které by mělo za následek narušení práv a svobod subjektu údajů, a to i s ohledem na zranitelnosti aktiva k ostatním hrozbám.
Portály	**Vnější útoky**	3	Na základě zjištěných informací Kolektiv přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na střední hodnotu.
	Technické chyby	2	Na základě zjištěných informací Kolektiv přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na nízkou hodnotu. Portály jsou zpravidla poskytovány externími subjekty a uloženy v rámci cloudového řešení, takže zranitelnost je na nízké úrovni.
	Lidský faktor	3	Na základě zjištěných informací Kolektiv přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na střední hodnotu. Střední úroveň byla Kolektivum zvolena s ohledem na možnost způsobení chyb administrátory portálů Objenatele.
	Narušení integrity OÚ	3	Na základě zjištěných informací Kolektiv přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na střední hodnotu. Střední úroveň byla Kolektivum zvolena s ohledem na možnost způsobení chyb redaktory a administrátory portálů Správce.
	Neoprávněný přístup	2	Na základě zjištěných informací Kolektiv přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na nízkou hodnotu. Kolektiv nepředpokládá neoprávněných přístup na portály Správce.
	Narušení dostupnosti	3	Na základě zjištěných informací Kolektiv přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na střední hodnotu.

Název Aktiva	Hrozba	Zranitelnost	Hodnocení zranitelnosti
	Ztráta osobních údajů	3	Na základě zjištěných informací Kolektiv přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na střední hodnotu. [redacted]
	Narušení práv a svobod subjektu údajů	3	Na základě zjištěných informací Kolektiv přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na střední hodnotu. Střední hodnota zranitelnosti tohoto aktiva byla Kolektivum stanovena z důvodu zneužití osobních údajů v tomto aktivu, které by mělo za následek narušení práv a svobod subjektu údajů, a to i s ohledem na zranitelnosti aktiva k ostatním hrozbám.
Ostatní elektronická úložiště	**Vnější útoky**	2	Na základě zjištěných informací Kolektiv přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na střední hodnotu. Správce má ostatní elektronická úložiště odděleny od veřejně dostupné sítě.
	Technické chyby	2	Na základě zjištěných informací Kolektiv přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na střední hodnotu. Správce provádí zálohu dat.
	Lidský faktor	3	Na základě zjištěných informací Kolektiv přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na střední hodnotu. Střední úroveň byla Kolektivum zvolena s ohledem na možnost způsobení chyb uživatelů ostatních elektronických úložišť, kdy dochází ke ztrátě či jinému znehodnocení dat obsahující osobní údaje.
	Narušení integrity OÚ	3	Na základě zjištěných informací Kolektiv přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na střední hodnotu. Střední úroveň byla Kolektivum zvolena s ohledem na možnost způsobení chyb uživatelů ostatních elektronických úložišť, kdy dochází ke ztrátě či jinému znehodnocení dat obsahující osobní údaje.
	Neoprávněný přístup	3	Na základě zjištěných informací Kolektiv přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na střední hodnotu. [redacted]
	Narušení dostupnosti	2	Na základě zjištěných informací Kolektiv přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na střední hodnotu.
	Ztráta osobních údajů	4	Na základě zjištěných informací Kolektiv přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na vysokou hodnotu. [redacted]

Název Aktiva	Hrozba	Zranitelnost	Hodnocení zranitelnosti
	Narušení práv a svobod subjektu údajů	4	Na základě zjištěných informací Kolektiv přiřadil hodnocení zranitelnosti aktiva vůči této hrozbě na vysokou hodnotu. Vysoká hodnota zranitelnosti tohoto aktiva byla Kolektivum stanovena z důvodu zneužití osobních údajů v tomto aktivu, které by mělo za následek narušení práv a svobod subjektu údajů, a to i s ohledem na zranitelnosti aktiva k ostatním hrozbám.

RIZIKOVÉ SKÓRE VYHODNOCENÝCH AGEND

3. RIZIKOVÉ SKÓRE VYHODNOCENÝCH AGEND

3.1 Hodnoty zranitelnosti

Dále byly Zhotovitelem podle předcházející kapitoly stanoveny hodnoty zranitelnosti jednotlivých aktiv vůči stanoveným hrozbám, které jsou uvedeny v tabulce:

	Listinné úložiště v rámci výkonu agend Objednatele	Listinné úložiště v rámci vnitřního chodu Objednatele	Informační systém spisové služby	Agendové informační systémy	Ekonomický informační systém	Portály	Ostatní elektronická úložiště
Vnější útoky	3	3	2	2	2	3	2
Technické chyby	3	3	2	2	3	2	2
Lidský faktor	4	4	2	2	3	3	3
Narušení integrity OÚ	3	3	2	2	3	3	3
Neoprávněný přístup	3	3	2	3	3	2	3
Narušení dostupnosti	2	2	3	3	3	3	2
Ztráta osobních údajů	4	4	3	3	3	3	4
Narušení práv a svobod subjektu údajů	4	4	3	3	3	3	4

4. ZÁVĚREČNÉ RIZIKOVÉ SKÓRE

4.1 Závěrečné rizikové skóre

V následující tabulce je uvedeno závěrečné rizikové skóre k jednotlivým aktivům včetně indikátorů:

- celková míra rizika hrozby – indikátor ukazuje celkové míry rizika hrozeb dle jejich výše. Dle výše indikátoru je tedy patrné, které hrozby jsou pro Správce nejzávažnější a mohou zde směřovat technická a organizační opatření;
- celkové míra rizika aktiva – indikátor ukazuje celkové míry rizika aktiv dle jejich výše. Dle výše indikátoru je tedy patrné, která aktiva jsou nejnáchylnější a potřebují zvýšenou pozornost či ochranu ze strany Správce.

	Listinné úložiště v rámci výkonu agend Objednatele	Listinné úložiště v rámci vnitřního chodu Objednatele	Informační systém spisové služby	Agendové informační systémy	Ekonomický informační systém	Portály	Ostatní elektronická úložiště	**Indikátor celkové míry rizika**
Vnější útoky	30	30	20	20	20	60	10	**190**
Technické chyby	30	15	30	20	45	30	20	**190**
Lidský faktor	60	60	20	30	45	45	45	**305**
Narušení integrity OÚ	45	30	20	20	30	30	30	**205**
Neoprávněný přístup	45	30	30	30	30	20	60	**245**
Narušení dostupnosti	20	20	45	45	45	45	20	**240**
Ztráta osobních údajů	40	40	30	30	30	30	60	**260**
Narušení práv a svobod subjektu údajů	60	40	30	30	30	30	60	**280**
Indikátor celkové míry hrozby	**330**	**265**	**225**	**225**	**275**	**290**	**305**	

4.2 Vyhodnocení

Z výsledků kapitoly Závěrečné rizikové skóre jasně vyplývá, na které problémy se Správce musí do budoucna soustředit:

Jednoznačně nejvyšší riziko zneužití osobních údajů zanáší lidský faktor (indikátor celkové míry rizika je až 305).

Menší, avšak významná jsou též rizika spojená s narušením dostupnosti (tzn. dočasný nebo dlouhodobý výpadek provozu výpočetní techniky. Rizika spojená s neoprávněným přístupem jsou menší, avšak také znatelná.

Z hlediska zpracovávaných agend jsou v největším riziku listinná úložiště, kde je indikátor celkové míry hrozby až 330. To je vcelku srozumitelné, protože většina agend má základ v listinných dokumentech. Dále jsou v ohrožení nestrukturovaná úložiště (to znamená PC, na kterých zaměstnanci pracují – souvisí s lidským faktorem), zde je míra hrozby až 305. S malým odstupem (míra hrozby 290) následují portály, protože jsou exponované a přístupné komukoliv. A konečně také ekonomický software (s mírou hrozby 275), protože jeho napadení by mělo veliké ekonomické důsledky.

ROZDÍLOVÁ ANALÝZA

5. ZHODNOCENÍ SOUČASNÉHO STAVU

5.1 Informační systém

Činnosti Správce a jejich rozsah jsou definovány příslušnými zákony a vyhláškami ČR.

Správce spravuje své záležitosti samostatně - samostatná působnost. Státní správu, jejíž výkon byl zákonem svěřen orgánu Správce, vykonává tento orgán jakou svou přenesenou působnost. V rámci přenesené působnosti je Správce na základě zákona č. 314/2002 Sb. obcí s pověřeným obecním úřadem a obcí s rozšířenou působností.

V této pozici je pro Správce základním manažerským prostředkem informační systém, jehož robustnost určuje míru kybernetické bezpečnosti a zprostředkovaně i míru ochrany osobních údajů.

Informační systém jako takový je realizován z velkého množství systémů a aplikací, které podporují realizaci jednotlivých agend Správce. Část aplikací je provozována lokálně (aplikace podporující výkon samosprávy), část aplikací je provozována centrálně nadřízenými orgány (např. ministerstva).

Informační systém Správce je centralizován v jeho sídle. Zde jsou v uzavřené serverovně umístěny servery a základní infrastruktura. Serverová část je tvořena fyzickými stroji, které hostují virtuální stroje vytvářené pomocí MS terminál. [redacted]

[redacted]

[redacted]

Připojení do Internetu je realizováno prostřednictvím firewallu, firewall vytváří DMZ, ve které jsou provozovány webové servery.

Pracovní stanice jsou zařazeny do domény [redacted]. Uživatelé se hlásí pomocí svých jmenných účtů a autentizují se heslem, na které je uplatňována doménová politika.

Většina provozovaných aplikací je provozována v architektuře klient-server, tj. na stanici je spouštěn klient aplikace, který komunikuje se serverovou částí. Data jsou ukládána do úložiště serverové aplikační části, což je databáze na serveru. Některé aplikace se spouštějí lokálně pomocí zástupce na ploše, který otevírá webový prohlížeč, ve kterém je spouštěna aplikace. Aplikace spravované IT neukládají data na lokální disky PC (až na výjimky) Dokumenty uložené uživatelem na lokální disk ale politika IT nezakazuje (např. ukládání na Plochu).

Uživatelé mají k dispozici úložiště v souborovém systému, a to jednak na své pracovní stanici a jednak prostřednictvím sdílených adresářů. Sdílené adresáře jsou mapovány a připojovány jako sdílený disk.

[redacted]

Vzdálené aplikace jsou provozovány nadřízenými organizacemi - zde je kontrola Správce pouze nad klienty na pracovních stanicích.

[redacted]

Nejsou evidovány žádné nezabezpečené bezdrátové sítě.

5.1.1 Klíčový uživatel

V IT systému je nastavena hierarchie rolí a tomu odpovídající hierarchie přístupových oprávnění.

Klíčový uživatel - představitel uživatelů informačního systému, zpravidla vedoucí organizační jednotky (odbor, oddělení, atd.), která informační systém používá pro podporu výkonu své agendy. Vedoucí IT dokáže takového zaměstnance určit, ale nikde takové věci neeviduje.

Role systémového a bezpečnostního správce mohou být kumulovány do jedné osoby. Aktuálně je IT oddělení obsazeno 3 specialisty, kteří zajišťují chod infrastruktury a aplikací.

5.2 Hlavní služby realizované IS

Jaké jsou hlavní služby, které realizuje IS, shrnuje následující tabulka:

Název služby	Účel
Strategie a rozvoj	Rozpracované jsou, ale nejsou oficiální.
Služby infrastrukturní	Externě zajišťuje [redacted]
Služby aplikační	Správa a aktualizace aplikací, konfigurace, správa číselníků, typů dokumentů, šablon, přístupová oprávnění, nastavování tisku (pro informační systémy uvedené v portfoliu informačních systémů).
Služby datové	Příprava dat pro import, vytváření exportních dávek, převody dat, vytváření specifických reportů, sestav, statistik.
Služby GIS	Správa GIS aplikací, tvorba digitální účelových map, mapových vrstev (pasporty komunikací, veřejného osvětlení, dopravního značení, zimní údržby, městské zeleně), správa podkladových katastrálních map, územního plánu, územně analytických podkladů. Skrze GePro.
Bezpečnost	Zajištění technické bezpečnosti (firewall, antivirus, autentizace uživatelů), organizační bezpečností (systém řízení bezpečnosti, odpovědnosti, bezpečnostní politika, smluvní vztahy), objektové bezpečnosti (zabezpečení fyzického přístupu, fyzická ochrana ICT) a personální bezpečnosti (smluvní podmínky, bezpečnostní pravidla). To vše je zajištěno v menší míře a pouze na IT. Kromě základní technické bezpečnosti se jí více na jednotlivých odborech nevěnují.
Vzdělávání/ školení	Aktivně žádné vzdělávání zaměstnanců ze strany IT neprobíhá.
Zajištění podpory uživatelům	Podpora uživatelů je prováděna.
Projektové řízení	Účast při řízení projektů, zastoupení v realizačních týmech projektů v oblasti zajištění ICT, konzultace, specifikace technických parametrů. Týká se vedoucího pracovníka IT.

5.3 Některé zvláštní případy

Kolektiv řešil některá nejasná, nestandardní nebo neobvyklá zjištění a zaujal k nim následující doporučující stanoviska.

5.3.1 Záznamová kamera v IT u kopírky

Eventuální instalace kamery se záznamovou 24 hodinovou smyčkou je podle názoru Kolektivu legální a je v souladu s GDPR. Jedná se o ochranu oprávněného zájmu Správce, směřujícího k ochraně majetku, ochraně pořádku a bezpečnosti na pracovišti.

Proti tomuto názoru se mohou zaměstnanci odvolat. Případné odvolání je třeba vyřešit ve lhůtě pro odvolání.

5.3.2 Nezáznamová kamera před dveřmi Odboru práva a VZ

Kamera, umístěná před dveřmi odboru práva a VZ, pokud je v on-line režimu, tedy bez záznamu, je plně v souladu s GDPR.

5.4 Hlavní informační systémy a prostředky

Hlavní informační systémy a prostředky, pomocí kterých se uvedené služby realizují:

Název	Účel	Výrobce/dodavatel
E-spis	Komplexní vedení spisové služby, automatizovaná evidence a oběh písemností v celém jejich životním cyklu, včetně ePodatelny a komunikace s ISDS.	ICZ a.s.
Intranet - úkolovník, školský úkolovník	Různé webové aplikace na intranetu obce. Jedná se o primárně podpůrné programy pro usnadnění práce a komunikace.	Internet PB, KAO.cz
PROXIO	Agendový informační systém PROXIO. Jeho součástí je např. ekonomika (MS Dynamics NAV) a AGENDIO. S jeho pomocí probíhají správní řízení v několika odborech.	Marbes
AGENDIO	Systém na zpracování agend, např. popelnice, místní daně a poplatky,… pro různé odbory.	Marbes
VITA	Agendový program, s jehož pomocí probíhají v několika odborech správní řízení, viz např. níže uvedená.	VITA software s.r.o.
VITA Památky	Agenda státní památkové péče.	VITA software s.r.o.
VITA Přestupky	Agenda přestupků a jiných správních deliktů.	VITA software s.r.o.
VITA Silniční úřad	Agenda speciálního stavebního úřadu - silniční, zvláštní užívání komunikací.	VITA software s.r.o.
VITA Stavební úřad	Agenda územního a stavebního řízení.	VITA software s.r.o.
VITA Úřad územního plánování	Agenda územního plánování.	VITA software s.r.o.
VITA Vodoprávní úřad	Agenda speciálního stavebního úřadu - vodoprávní.	VITA software s.r.o.
YAMACO	Agenda pro myslivecké plánování a statistiky, protokoly honiteb, evidence honebních společenství, psů, ulovené zvěře, tvorba statistik pro Ministerstvo životního prostředí apod.	Janeček Karel Ing. YAMACO Software
EVI - evidence odpadů, přepravy a zařízení od původců a oprávněných osob	Vedení průběžné evidence odpadů při každém vzniku, zneškodnění nebo předání odpadu.	INISOFT s.r.o.
ESPI - vedení správních řízení v oblasti ekologie a odpadů	IS zpracovává data o správních řízeních v oblasti odpadového hospodářství pro potřeby MŽP. IS zajišťuje služby evidence rozhodnutí ve správních činnostech.	INISOFT s.r.o.
MP Manager	Událostní informační systém pro řízení procesu městské policie. Správa událostí a přestupků, Statistika MV, Informace o RZ, Pokutové bloky, Personalistika, Úkoly, Mobilní	FT Technologies a.s.

Název	Účel	Výrobce/dodavatel
	aplikace, Mapový monitoring, Evidence techniky.	
Matrika	Aplikace je určena pro práci matričních úřadů.	GSoft Society s.r.o.
Proxio	Řešení pro oblast účetnictví, banky, pokladny, knihy přijatých a odeslaných faktur, majetku a skladové evidence.	Marbes
OKnouze	OKnouze je klient aplikace MPSV CZ. [redacted]	MPSV CZ
Codexis, Beck, Aspi	Právní informační systém	Atlas Consulting spol. s r.o.
Exchange	Poštovní server	Microsoft
MISYS/MISYS WEB	Geografický informační systém	GEPRO spol. s.r.o.
Fingera	Docházkový systém	Fingera s.r.o.
VEMA	Mzdy, personalistika	Vema, a. s.
Veřejný web	Webové stránky města	Internet PB

Dále systém obsahuje:

- Kancelářský software
- Lokální úložiště
- Tiskárny a multifunkční zařízení
- PC a notebook
- Mobilní zařízení [redacted]
- HelpDesk (Skrze „Úkolovník“ od PB internet)

Lokální informační systémy jsou plně pod správou IT Správce.

Jako klíčový uživatel je nastaven představitel uživatelů informačního systému. Je to zpravidla vedoucí organizační jednotky (odbor, oddělení, ...), která informační systém používá pro podporu výkonu své agendy. Vedoucí IT dokáže takového zaměstnance určit, ale nikde takové věci neeviduje.

Role systémového a bezpečnostního správce mohou být kumulovány do jedné osoby. Aktuálně je IT oddělení obsazeno 3 specialisty, kteří zajišťují chod infrastruktury a aplikací.

5.5 Ochrana dat a informačního systému

IT oddělení je tvořeno obsazeno 3 pracovníky, žádný z nich není dedikován pro ochranu dat a informačního systému. Vlastní role bezpečnostního manažera ať už pro fyzickou nebo informační bezpečnost není vytvořena a obsazena.

IT oddělení provozuje informační systémy a ve smyslu GDPR není ani správcem, ani Kolektivum OÚ. S OÚ je na oddělení IT pracováno na systémové úrovni, IT oddělení realizuje požadavky na bezpečnost stanovené jednotlivými odbory na základě platných zákonných norem a předpisů.

Otázka	Odpověď
Máte implementovánu nějakou bezpečnostní normu nebo standard? Jakou?	Ne nebylo implementováno, není požadováno. Neexistuje na oficiální úrovni.
Jaká je hierarchie řízení bezpečností? Hierarchie řízení bezpečností IT/IS?	Není vytvořena hierarchie řízení bezpečnosti IS. Role jsou v rámci oddělení sloučeny - bezpečnost a provoz dohromady.
Kdo je zodpovědný za řízení bezpečností? Kdo je zodpovědný za řízení bezpečnosti IT/IS?	Vedoucí IT [redacted]
Jsou výše uvedené role definovány včetně pravomocí a zodpovědností?	Není definováno. Existuje zmínka v Koncepci ISVS
Jakou bezpečnostní dokumentací máte zavedenu? Bezpečnostní politika, bezpečnostní politika IT/IS, bezpečnostní směrnice, plány obnovy atd. Je možné získat nebo je k nahlédnutí?	Existuje neaktualizovaný dokument pro řízení IS jako takového. Bezpečnostní politika není jako taková vytvořena. Opět neoficiální, kusé nebo neaktuální. Situace by měla být vyřešena na základě výzvy 33.
Máte zavedenu bezpečnostní dokumentaci řídící bezpečnost informací v listinné podobě - spisový řád, archivační řád nebo jejích ekvivalenty? Je možné získat nebo je k nahlédnutí?	Je zavedena dokumentace pro řízení úřadu.
Personální obsazení oddělení bezpečnosti IT/IS? Kolik osob? Kolik uživatelů/PC/serverů/aplikací na starosti?	Oddělení bezpečnosti neexistuje. IT má 3 pracovníky, kteří zajišťují chod [redacted] pevných PC, [redacted] notebooků [redacted] serverů
Jsou uživatelé a zaměstnanci pravidelně školení ohledně bezpečností IT/IS, objektové bezpečnosti atd.?	Není zaveden systém pravidelného školení uživatelů a správců/administrátorů v oblasti bezpečnosti IS, aktuálních IS hrozeb atd. Vzdělávání probíhá jen z vlastní vůle zaměstnanců IT se dlouhodobě vzdělávat.

5.6 Bezpečnostní opatření IS

V níže uvedené tabulce jsou zaznamenána jednotlivá opatření. Sloupec Jak je opatření prováděno popisuje implementaci v základní podobě, sloupec Zodpovědnost uvádí, kdo je zodpovědný za provoz opatření a sloupec Politika uvádí, kdo definuje politiku (pravidla) pro dané opatření.

[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	
[redacted]	[redacted]			
[redacted]	[redacted]			
[redacted]	[redacted]			
[redacted]	[redacted]	[redacted]		[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]			
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]		[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]		
[redacted]	[redacted]			[redacted]
[redacted]	[redacted]			
[redacted]	[redacted]			[redacted]
[redacted]	[redacted]			[redacted]
[redacted]	[redacted]			
[redacted]	[redacted]			
[redacted]	[redacted]			[redacted]
[redacted]	[redacted]			[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]			
[redacted]	[redacted]			
[redacted]	[redacted]			

[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]		
[redacted]	[redacted]	[redacted]	[redacted]	
[redacted]	[redacted]			[redacted]
[redacted]	[redacted]			[redacted]
[redacted]	[redacted]			
[redacted]	[redacted]			
[redacted]	[redacted]			
[redacted]	[redacted]			

5.7 Další nálezy

V souvislosti s GDPR nelze kvantifikovat dostatečnost bezpečnostních opatření, protože Správce nemá zpracovánu analýzu rizik IT. Explicitně je potřebné uvážit požadavek na:

- Šifrování OÚ
- Anonymizaci/pseudonymizaci OÚ
- Zajištění dostupnosti a obnovy OÚ

Cekovou úroveň zabezpečení, s ohledem na dříve získané rizikové skóre, hodnotíme jako vyhovující.

Již teď je však možné upozornit na níže uvedené oblasti, které bude vhodné řešit v budoucnosti:

- Záznamy činnosti/Logování - v daném okamžiku jsou události vyhodnocovány manuálně a *ad hoc*. **Rozšířenému logování a tudíž šanci identifikovat potenciální problém nebo zpětně odhalit příčiny incidentu, brání technická omezení práce s logy.** Je možné zapnout rozšířené logování, nicméně pokud není nasazen prostředek, který by logy jako takové spravoval a analyzoval, nemá takové opatření smysluplný efekt ba právě naopak (zaplnění disků, nemožnost analýzy logů). Proto doporučujeme implementovat:

  zajištění Log management nástroje (správa a uchovávání logů a analýza logů). Dle informací by tyto nástroje mohly být dodány v již řešení výzvě 28.

  SIEM - nástroj umožňující analyzovat bezpečnostní události na jednotlivých prostředcích

- Autentizace uživatelů - v současné době se uživatelé autentizují kombinací jména a hesla. Tento systém je zranitelný neboť je závislý na práci jednotlivých uživatelů s hesly (paradox bezpečného hesla) a tuto zranitelnost nelze eliminovat jakýmkoliv organizačním opatřením. Největší hrozbou je obecně uživatel a je tudíž potřebné zajistit, aby se k OÚ dostal jen a pouze oprávněný uživatel a o tomto byl proveden nezpochybnitelný záznam. Proto doporučujeme implementovat:

  Dvoufaktorovou autentizaci u přístupů do emailu přes webové rozhraní či jiné webové aplikace umožňující připojení mimo vnitřní síť

- Ochrana před malware - posuzovaný subjekt má implementovány anti X systémy. Tyto operační systémy nemají již výrobcem odstraňovány chyby a představují tak pro malware potenciální cíl. Je potřebné si uvědomit, že stávající technologie anti-X řešení je založena na znalosti malware, a proto nelze chránit systémy, data a OÚ před kódy, které jsou zcela nové a ještě výrobci anti-X

neanalyzované. Malware jako takový může jednak zničit OÚ, ale může také poskytnout útočníkovi vzdálený přístup k OÚ. Proto doporučujeme implementovat:

Výměna operačních systémů nebo nasazení tenkých klientů/VDI

- Zajištění dostupnosti OU - přestože jsou nasazeny prostředky pro zajištění dostupnosti a obnovy systémů po havárii, je vhodné tuto oblast posílit a to nejenom na aplikační úrovni. Proto doporučujeme:

  Posílení redundance a vysoké dostupnosti infrastruktury

  Zpracování havarijních plánů a postupů

- Incident management - v daném okamžiku není po procesní stránce dle mého názoru dostatečně řešen (stanovení zodpovědností, klasifikace incidentů, postupy pro řešení incidentů, postupy pro analýzu incident atd.). Proto doporučujeme:

  Zpracovat směrnici/pracovní postup pro incident management

  Zrychlit modernizaci síťových prvků, stejně tak zajistit modernizaci firewallů

- DLP systém – ochrana před ztrátou dat je nezbytnou součástí IT oddělení, ve spojitosti s GDPR je ještě daleko důležitější.
- Zajištění školení zaměstnanců ze strany IT. Případná tvorba informačních dokumentů v případě zvýšeného nebezpečí spojeného s IT. Proto doporučujeme:

  Pravidelné školení zaměstnanců IT, případné zavedení vzdělávacího plánu s důrazem na bezpečnost

  Systém předávání vědomostí a školení dalších zaměstnanců mimo IT

- Zajistit správu a omezení přenosných zařízení – přenosná zařízení mohou být zdrojem ohrožení systému a uložených dat. Zároveň mohou obsahovat osobní údaje a jsou vystaveny ztrátě i krádeži. Proto doporučujeme implementovat:

  Inventarizaci přenosných zařízení

  Zabezpečení přenosných zařízení (použitím hesla a šifrováním)

  Omezení používání přenosných zařízení, která nespadají pod organizaci

- Zajistit správu chytrých mobilních telefonů – zejména z důvodů připojení pracovních emailových schránek a možné ztrátě takto vybaveného zařízení. Proto doporučujeme implementovat:

  Invetarizovat tato zařízení

  Zapojení systému pro správu chytrých mobilních telefonů

  Nastavení jednotného bezpečnostního standardu pro tyto zařízení

  Zabezpečení proti odcizení nebo napadení škodlivým softwarem (antivirová aplikace)

- Sjednocení podmínek pro technickou podporu. Vzdálené připojení i v rámci technické podpory může být potencionálním místem pro uník osobních údajů. Proto doporučejeme implementovat:

  Jednotný řád pro vzdálené připojení technické podpory s důrazem na dohled a bezpečnost připojení

  Omezení odesílání záloh systémů pro potřeby řešení technických problémů, případně anonymyzování záloh před odesláním

IMPLEMENTACE

6. IMPLEMENTAČNÍ PLÁN

Legenda:

- provede a zodpovídá **Správce**
- provede a zodpovídá **Kolektiv**
- konzultuje, provede a zodpovídá **DPO**

6.1 Dokumentová základna

Týká se všech součástí, odborů i oddělení.

Pro účinné a spolehlivé zabezpečení ochrany osobních údajů, základní nezbytností je nastartování a implementace procesů, kterými se ustanovuje a udržuje dokumentová základna Správce. Postup, jak se toho dosáhne, navrhujeme Správci v kapitole Detailní popis realizace procesů bezpečnosti OÚ. Jedná se zejména o tyto dokumenty:

1. **Směrnice k ochraně osobních údajů,**
2. **Spisový a skartační řád, resp. Skartační plán.**
3. **Směrnice pro nakládání s klíči (pro každé pracoviště individuálně podle místních možností a potřeb).**
4. **Informační memorandum.**
5. **Směrnice pro postup při uplatnění práv subjektů.**

6.2 Fyzická bezpečnost a ochrana perimetru

Týká se všech součástí, odborů i oddělení.

Otázky fyzické bezpečnosti a kybernetické bezpečnosti jsou primárně řešeny jinými předpisy[9], než je GDPR. Nicméně, bez zajištění fyzické bezpečnosti jak listinných, tak i elektronických dokumentů, byla by jakákoliv ochrana OÚ čistě iluzorní. Proto je potřeba, posílit na všech pracovištích fyzickou ochranu, a to zejména:

1. **Zajistit uzamykatelné a odolné skříně (pro každé pracoviště individuálně podle místních možností a potřeb) a také zajistit, aby se do nich dokumenty opravdu ukládaly.**
2. **Kde je to možné, opatřit kanceláře odolnějšími dveřmi, na vnější straně namontovat dveřní kování s koulí (pro každé pracoviště individuálně podle místních možností a potřeb).**

[9] Zákon č. 181/2014 Sb., Zákon o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti)

6.3 Elektronická bezpečnost a prevence

Realizace se týká zejména IT odboru.

Protože velká část zpracování IT je řešena pomocí IT technologií, je na místě soustředit se na kybernetickou bezpečnost a na naplnění požadavků příslušného zákona. č. 181/2014 Sb. Nicméně, jedním ze základních principů GDPR je **předcházení bezpečnostním incidentům** a důraz na prevenci.

Menší, avšak významná jsou též rizika spojená s narušením dostupnosti. Může se jednat o dočasný nebo dlouhodobý výpadek provozu výpočetní techniky, ale velkým rizikem je především narušení dostupnosti IT v důsledku onemocnění nebo absence správce IT. Je nejisté, jestli aktuální stav je dostatečně bezpečným řešením.

Plán bezpečnosti informací definuje základní strategii a zásady týkající se managementu zabezpečení informací (ISMS), určuje základní bezpečnostní pravidla pro provoz, používání a údržbu informačních a komunikačních technologií s cílem zajistit požadovanou dostupnost a ochranu informací a minimalizaci škod vzniklých v důsledku možných bezpečnostních incidentů. Lze jedině doporučit, aby IT oddělení Správce v dohledné době takový plán sestavilo a schválilo.

Na základě provedených auditů doporučujeme, aby byla u Správce jako celku provedena následující bezpečnostní a preventivní opatření, přičemž časový harmonogram a stanovení priorit záleží na možnostech a uvážení Správce:

1. **Zpracovat a schválit obecný Plán bezpečnosti informací ve smyslu zák. č. 181/2014 Sb., Zákon o kybernetické bezpečnosti.**
2. **Pořídit analytický nástroj SIEM - nástroj umožňující analyzovat bezpečnostní události na jednotlivých prostředcích.**
3. **Implementovat dvoufaktorovou autentizaci u přístupů do emailu přes webové rozhraní či do jiné webové aplikace umožňující připojení mimo vnitřní síť.**
4. **Ve vzdálenější perspektivě doporučujeme nasazení tenkých klientů/VDI, které se nám (ve spojení s dobře chráněnými servery) jeví jako bezpečnější.**
5. **Posílení dostupnosti: zvýšení redundance a vysoké dostupnosti infrastruktury, zpracování havarijních plánů a postupů, řešení zvýšené zastupitelnosti správců.**
6. **Zpracovat směrnici/pracovní postup pro incident management.**
7. **Zrychlit modernizaci síťových prvků, stejně tak zajistit průběžnou modernizaci firewallů.**

8. **Zintenzívnit správu a omezení přenosných zařízení, jakož i chytrých mobilů. Tento požadavek je kodifikován Směrnicí pro ochranu OÚ, ale odbor IT jej musí realizovat. Konkrétně to znamená následující: inventarizovat tato zařízení, zapojit systém pro jejich správu a nastavení jednotného bezpečnostního standardu pro tato zařízení, zabezpečení proti odcizení nebo napadení škodlivým softwarem.**
9. **Sjednotit podmínky pro technickou podporu, zejména pomocí vzdáleného připojení. Proto doporučujeme implementovat (a) jednotný řád pro vzdálené připojení technické podpory, s důrazem na dohled a bezpečnost připojení, (b) omezení odesílání záloh systémů pro potřeby řešení technických problémů, případně anonymizování záloh před odesláním.**

6.4 Zpracovatelé

Týká se všech součástí, odborů i oddělení.

Důležitým principem GDPR je, že Správce OÚ odpovídá za veškeré bezpečnostní incidenty, neboť má povinnost jim předcházet. V jeho nejvlastnějším zájmu proto je, zavázat **veškeré spolupracující zpracovatele** (zejména právnické, ale i fyzické podnikající osoby), kteří se setkávají nebo potenciálně mohou setkávat s OÚ subjektů, k zachovávání GDPR.

Vhodnou formou může být uzavření zpracovatelské smlouvy:

1. **Uzavřít zpracovatelské smlouvy se všemi existujícími zpracovateli.**
2. **Vytvořit interní předpis, kterým se zajistí, že se odpovídající zpracovatelská smlouva uzavře s jakýmkoliv novým zpracovatelem.**

Postup, jak se zpracovatelská smlouva uzavře, navrhujeme Správci v kapitole Detailní popis realizace procesů bezpečnosti OÚ.

Seznam zpracovatelů, jak vyplynul z provedeného auditu, shrnuje následující tabulka:

Název	Účel	Výrobce/ Dodavatel
E-spis	Komplexní vedení spisové služby, automatizovaná evidence a oběh písemností v celém jejich životním cyklu, včetně ePodatelny a komunikace s ISDS.	ICZ a.s.
Intranet	Různé webové aplikace na intranetu obce. Jedná se o primárně podpůrné programy pro usnadnění práce a komunikace.	Internet PB, KAO.cz
PROXIO	Integrovaný systém programů pro státní správu, jehož součástí je řada specializovaných programů.	Marbes
VITA	Integrovaný systém programů pro státní správu, jehož součástí je řada specializovaných programů.	VITA software s.r.o.
YAMACO	Agenda pro myslivecké plánování a statistiky, protokoly honiteb, evidence honebních společenství, psů, ulovené zvěře, tvorba statistik pro Ministerstvo životního prostředí apod.	Janeček Karel Ing. YAMACO Software
EVI	Vedení průběžné evidence odpadů při každém vzniku, zneškodnění nebo předání odpadu.	INISOFT s.r.o.
ESPI	IS zpracovává data o správních řízeních v oblasti odpadového hospodářství pro potřeby MŽP. IS zajišťuje služby evidence rozhodnutí ve správních činnostech.	INISOFT s.r.o.
MP Manager	Událostní informační systém pro řízení procesu městské policie. Správa událostí a přestupků, Statistika MV, Informace o RZ, Pokutové bloky, Personalistika, Úkoly, Mobilní aplikace, Mapový monitoring, Evidence techniky.	FT Technologies a.s.
Matrika	Aplikace je určena pro práci matričních úřadů.	GSoft Society s. r. o.

Název	Účel	Výrobce/ Dodavatel
OKnouze	OKnouze je klient aplikace MPSV CZ. _ [redacted]	MPSV CZ
Codexis, Beck, Aspi	Právní informační systém	Atlas Consulting spol. s r.o.
Exchange	Poštovní server	Microsoft
MISYS/MISYS WEB	Geografický informační systém	GEPRO spol. s.r.o.
Fingera	Docházkový systém	Fingera s.r.o.
VEMA	Mzdy, personalistika	Vema, a. s.
Veřejný web	Webové stránky města	Internet PB

6.5 Lidský faktor

Týká se všech součástí, odborů i oddělení.

Jednoznačně nejvyšší riziko zneužití osobních údajů zanáší lidský faktor (indikátor celkové míry rizika dosahuje hodnoty až 305). Proto je vliv lidského faktoru podchycen závazným předpisem, jako je Směrnice pro ochranu osobních údajů. Dále je včleněn buď do pracovních smluv, nebo do závazku fyzických osob k mlčenlivosti. Případně též je řešen dalšími interními směrnicemi Správce.

Současně platí, že plnění všech předpisů a závazků osobami je vlivem různých faktorů (neznalost, stres, úmysl a další) velmi nespolehlivé. Částečně to je řešeno seznámením a kontrolou zaměstnanců ve věci Směrnice. Pro zvýšenou bezpečnost doporučujeme navíc:

1. **Provést kontrolu, že všechny osoby, které přicházejí do styku s osobnímu údaji subjektů (např. zaměstnanci, DPP, DPČ, Zastupitelé, RM a další), jsou nějakou formou zavázány k mlčenlivosti.**
2. **Doporučujeme zavedení e-learningu a testování zaměstnanců z hlediska ochrany osobních údajů minimálně v míře platné Směrnice na ochranu osobních údajů a vytvoření k tomu nutných vzdělávacích materiálů.**

6.6 Souhlasy subjektů se zpracováním OÚ

Týká se vybraných součástí, odborů i oddělení.

V praxi může nastat situace, že Správce potřebuje zpracovávat osobní údaje subjektu, přičemž právní titul pro zpracování těchto údajů chybí. V takovém případě je možné situaci vyřešit souhlasem dotčených subjektů OÚ. Je třeba mít na mysli, že udělit souhlas se zpracováním osobních údajů je možnost, nikoli povinnost.

Z pohledu obecného nařízení bude platný jen takový souhlas, který byl shromážděn transparentním způsobem, a dotčená osoba jej udělila svobodně. Musí být udělen pro jeden či více konkrétních účelů (pro každý zvlášť), musí být udělen svobodně (není svobodný, je-li plnění smlouvy učiněno závislým na souhlasu, který jinak není pro toto plnění nezbytný). Mlčení neznamená souhlas a souhlas lze kdykoli odvolat.

Povinností správce je doložit, že subjekt údajů souhlas se zpracováním svých osobních údajů udělil, a proto je potřeba jej vyžadovat písemně.

Postup uzavření zpracovatelské smlouvy

(vytvoření obecné šablony pro souhlasy)

a. Kolektiv navrhl a Správci předal vzor souhlasu.
b. Správce vzor uváží a vytvoří závaznou šablonu souhlasu.
c. Kolektiv se k šabloně odborně vyjádří z hlediska GDPR (aniž by poskytoval právní poradenství).

(jednotlivé odbory: uzavírání konkrétních souhlasů podle šablony)

d. Správce zajistí, že subjekty podepíší souhlas pro konkrétní případy.
e. Kdyby se stalo, že některý subjekt odmítne podepsat souhlas, bude se situace řešit s pomocí DPO.

6.7 Detailní popis realizace procesů bezpečnosti OÚ

Týká se všech součástí, odborů i oddělení.

Týká se všech procesů bezpečnosti OÚ.

Postup realizace procesů vedoucích k ochraně osobních údajů

(příprava a nastartování procesu, zajišťovaného dokumentem)

a. Kolektiv navrhl a Správci předal vzor dokumentu, aktuální ke dni předání Implementace.
b. Správce vzor uváží a vytvoří závaznou šablonu dokumentu.
c. Kolektiv se k šabloně odborně vyjádří z hlediska GDPR (aniž by poskytoval právní poradenství).
d. Správce ve svém pracovním pořádku zajistí uvedení dokumentu do praxe.
e. Kolektiv po konzultaci se Správcem navrhne:
    i. plán školení k dokumentu,
    ii. plán kontrol dodržování dokumentu
    iii. Správce o návrzích obou plánů rozhodne.
f. Správce vytvoří plán aktualizací dokumentu.

(proces průběžné realizace, kontroly, změn a školení k dokumentu)

g. Cyklicky, v termínech stanovených plánem kontrol dodržování dokumentu, Správce provede kontrolu[10] dodržování dokumentu:
    i. pokud shledá závady v dodržování, v pracovním pořádku rozhodne o nápravě.
    ii. pokud shledá, že je potřeba dokument změnit (upravit, doplnit) na aktuální situaci, vytvoří a předá DPO seznam požadavků.
    iii. DPO požadavky na změny posoudí a vyřídí, tzn. buď je zapracuje, nebo zamítne.
h. Cyklicky, v termínech stanovených plánem aktualizací dokumentu, proběhne aktualizace dokumentu:
    i. DPO připraví a Správci ke chválení předloží novou verzi dokumentu, ve které jsou zapracovány všechny předcházející akceptované změny.
    ii. Správce v pracovním pořádku rozhodne o návrhu změny dokumentu.
i. Cyklicky, zpravidla v termínech stanovených plánem školení, nebo po závažných změnách dokumentu, Správce rozhodne o provedení školení zaměstnanců.
j. Odbornou náplň školení, včetně přednášek a případných studijních materiálů, zajišťuje DPO.

[10] Po dohodě může DPO upozorňovat Správce na blížící se termíny.

6.8 Detailní popis postupu uzavření zpracovatelské smlouvy

Týká se všech součástí, odborů i oddělení.

Týká se všech procesů bezpečnosti OÚ.

Postup uzavření zpracovatelské smlouvy

(vytvoření šablony pro zpracovatelskou smlouvu)

a. Kolektiv navrhl a Správci předal vzor zpracovatelské smlouvy.

b. Správce vzor uváží a vytvoří závaznou šablonu Smlouvy.

c. Kolektiv se k šabloně odborně vyjádří z hlediska GDPR (aniž by poskytoval právní poradenství).

(jednotlivé odbory: uzavírání konkrétních smluv podle šablony)

d. **pokud je Smlouva podle šablony pro zpracovatele akceptovatelná**:

   i. Správce se zpracovatelem dohodne znění konkrétní smlouvy.

e. **pokud zpracovatel už má svůj návrh smlouvy (tzn. nechce Smlouvy podle vzoru):**

   i. Podle dohody, Kolektiv může zprostředkovat zpracování posudku/verze smlouvy odbornou advokátní kanceláří.

   ii. Správce uváží vyjádření Kolektivu a bude postupovat podle svého rozhodnutí.

7. VZOR SMĚRNICE PRO UPLATNĚNÍ PRÁV SUBJEKTŮ OÚ V SOUVISLOSTI S GDPR

7.1. Právní rámec pro uplatnění práv subjektů OÚ

Nařízení Evropského parlamentu a Rady (EU) 2016/679, ze dne 27. dubna 2016, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů), označované jako "GDPR", zavedlo pro fyzické osoby – subjekty osobních údajů – několik významných nových práv:

1. Právo na informace a přístup k osobním údajům
2. Právo na opravu
3. Právo na výmaz („právo být zapomenut")
4. Právo na omezení zpracování
5. Právo vznést námitku
6. Právo na přenositelnost
7. Právo na stížnost dozorovému úřadu
8. Žaloba (vůči dozorovému úřadu / správci nebo zpracovateli)

Tomu **odpovídají nové povinnosti na straně Správce OÚ**, protože Správce musí mít připraveny postupy a procesy, kterými dokáže práva subjektů naplnit. Lhůta pro Správce je vesměs 30 dní (s možnými výjimkami v přesně specifikovaných případech). Nastavení příslušných postupů a procesů je předmětem této směrnice.

7.2. Obecně: způsob komunikace s klientem

Je na klientovi, jakou formu uplatnění svých práv zvolí, přičemž Správce musí akceptovat jakoukoliv formu.

Nicméně, Správce má povinnost prokazovat, že s podáním subjektu naložil podle práva, zejména že podání vyřídil správně a včas. Proto je třeba upřednostňovat takové formy podání, které subjekt provede písemnou formou (dopis, datové schránky, dokument předaný na podatelně, e-mail). V případě, že podání není učiněno písemně (rozhovor, telefonát), je potřeba o podání alespoň učinit záznam, ve kterém se uvede:

- identifikace toho, kdo právo uplatňuje,
- podstata toho, co uplatňuje,
- datum,
- identifikace toho, kdo záznam učinil.

Všechna podání se vyřizují v pracovním pořádku.

Veškerou korespondenci se subjektem je třeba provádět tak, aby ji bylo možno později doložit. Tedy přednostně písemnou formou (dopis, datové schránky, dokument předaný osobně proti podpisu, v krajním případě e-mail). Pokud korespondenci nelze vést písemně, je potřeba o každém kroku alespoň učinit záznam, ve kterém se uvedou nejméně údaje tyto údaje:

- kterého subjektu se záznam týká
- podstata věci, která je řešena,
- datum,
- identifikace toho, kdo záznam učinil.

Se všemi dokumenty, včetně veškerých záznamů, se zachází podle Spisového a skartačního řádu.

7.3. Právo na informace a přístup k osobním údajům

7.3.1. Všeobecně

Právo na informace a přístup k osobním údajům představuje oprávnění subjektu údajů na **základě jeho aktivní žádosti** získat od správce informaci (potvrzení), zda jsou či nejsou jeho osobní údaje zpracovávány a pokud jsou zpracovávány, má subjekt údajů právo tyto osobní údaje získat a zároveň má právo získat následující informace:

- účely zpracování
- kategorie dotčených osobních údajů
- příjemci nebo kategorie příjemců, kterým osobní údaje byly nebo budou zpřístupněny
- plánovaná doba, po kterou budou osobní údaje uloženy
- veškeré dostupné informace o zdroji osobních údajů
- pokud nejsou získány od subjektu údajů, tak skutečnost, že dochází k automatizovanému rozhodování, včetně způsobu profilování
- existence práva požadovat od správce opravu nebo výmaz osobních údajů
- existence práva vznést námitku
- existence práva podat stížnost u dozorového úřadu.

7.3.2. Pracovní postup

Lze očekávat, že odpovědi na většinu dotazů již jsou obsaženy v Informačním memorandu. Proto se v prvním kroku zašle subjektu informace o tom, kde může odpovědi na své otázky najít. Vhodný vzor odpovědi je například zde:

(oslovení, úvod)

Správce OÚ zpracovává osobní údaje a další informace týkající se občanů v rámci samostatné a přenesené působnosti. Většina osobních údajů subjektů je tedy zpracovávána na základě povinností, uložených Správci OÚ zvláštními zákony, případně též smlouvami. Na taková zpracování osobních údajů o subjektech údajů se nevztahuje povinnost získat souhlas těchto osob. Pokud jsou některé osobní údaje zpracovávány mimo zákonnou povinnost, pak taková zpracování podléhají souhlasu občanů. Tato zpracování však Správce OÚ provádí jen výjimečně.

Zpracování osobních údajů Správcem OÚ je prováděno zákonným a spravedlivým způsobem, je pro občany transparentní a informace a všechna sdělení, týkající se zpracování těchto osobních údajů, jsou snadno přístupné. Účely, pro které jsou osobní údaje zpracovávány, jsou jednoznačné a legitimní a jsou stanoveny v okamžiku shromažďování osobních údajů. Rozsah shromažďovaných osobních údajů je vždy přiměřený, relevantní a omezený pouze na údaje nezbytné pro naplnění stanoveného účelu. Rovněž doba, po kterou jsou osobní údaje uchovávány, je omezena na nezbytné minimum. Při veškerém zpracování osobních údajů jsou aplikována opatření, která zaručují náležitou bezpečnost a důvěrnost těchto údajů, (např. zaručující zabránění neoprávněného přístupu k osobním údajům a k zařízení používanému k jejich zpracování).

Podrobné vymezení toho, jaké informace Správce zpracovává, za jakým účelem a z jakého důvodu, jak dlouho je uchovává a případně další důležité údaje, jsou zveřejněny na webových stránkách [doplnit odkaz].

Pokud tyto informace nepokládáte za dostačující, rádi Vám je upřesníme. Současně bychom Vás rádi informovali, že pokud by některé údaje, které o Vás zpracováváme, byly nepřesné nebo chybné, máte právo požádat o jejich opravu či vymazání, a to [upřesnit, kde]. U informací, které zpracováváme z důvodu oprávněného zájmu, máte navíc možnost vznést námitku proti jejich zpracování. Námitka se uplatňuje tamtéž a v případě, že by jí nebylo vyhověno, máte právo podat stížnost u dozorového úřadu.

(zakončení, závěr)

Pokud odpověď podle předcházejícího kroku subjekt neuspokojí, je třeba v první řadě ověřit, že se jedná o osobu oprávněnou informace požadovat, tzn. je potřeba ji identifikovat. Subjekt má právo na informace, týkající se výlučně sebe samého; na informace o jiných subjektech právo nemá.

Pokud je identifikace a právo subjektu potvrzeno, je třeba mu vyhovět postupem v pracovním pořádku.

7.4. Právo na opravu

V první řadě je potřeba ověřit, že se jedná o osobu oprávněnou informace opravovat, tzn. je potřeba ji identifikovat. Subjekt má právo opravovat informace, týkající se výlučně sebe samého; na opravu informace o jiných subjektech právo nemá.

Pokud je identifikace a právo subjektu potvrzeno, je třeba mu vyhovět postupem v pracovním pořádku. Oprava se musí provést postupem podle Spisového řádu, a to na všech místech, kde se nesprávná informace vyskytovala. Upozorňujeme zejména na to, že se musí zachovat soulad mezi listinnou a elektronickou formou.

Součástí vyřízení musí být též upozornění na možnost, podat stížnost dozorovému úřadu.

7.5. Právo na výmaz („právo být zapomenut“)

V první řadě je potřeba ověřit, že se jedná o osobu oprávněnou výmaz požadovat, tzn. je potřeba ji identifikovat. Subjekt má právo vymazat informace, týkající se výlučně sebe samého; na výmaz informace o jiných subjektech právo nemá.

Dále je potřeba ověřit, že se jedná o případ, kdy subjekt má nárok na výmaz informace. K výmazu může dojít výlučně v následujících případech:

- osobní údaje již nejsou potřebné pro účely, pro které byly shromážděny nebo jinak zpracovány,
- subjekt údajů odvolá souhlas a neexistuje žádný další právní důvod pro zpracování,
- subjekt údajů vznese námitky proti zpracování a neexistují žádné převažující oprávněné důvody pro zpracování,
- osobní údaje byly zpracovány protiprávně,
- osobní údaje musí být vymazány ke splnění právní povinnosti,
- osobní údaje byly shromážděny v souvislosti s nabídkou služeb informační společnosti podle článku 8 odst. 1 GDPR.

Naopak, osobní údaje nelze vymazat, jestliže:

- jde údaje nezbytné ke splnění zákonné povinnosti,
- jde výkon práva na svobodu projevu a informace,
- jsou zpracovány z důvodu veřejného zájmu na ochranu zdraví, archivace,
- jsou zpracovány pro určení, výkon nebo obhajobu právních nároků,
- se zpracovávají z důvodu ochrany životně důležitých zájmů subjektu,
- rovněž nelze vymazat osobní údaje, u kterých Správce je pouhým zpracovatelem (typickým příkladem jsou veřejné rejstříky).

Pokud je identifikace a právo subjektu potvrzeno, je třeba mu vyhovět postupem v pracovním pořádku. Výmaz se musí provést postupem podle Spisového řádu, a to na všech místech, kde se původní informace vyskytovala. Upozorňujeme zejména na to, že se musí zachovat soulad mezi listinnou a elektronickou formou.

V případě elektronických informací uložených v bezpečnostních zálohách, není provedení výmazu ze záloh technicky možné. Proto se postupuje náhradním způsobem – omezením přístupu k informacím. Provede se tak, že veškeré elektronické zálohy jsou bezprostředně po vzniku zašifrovány a heslo k nim je uloženo v zapečetěné obálce u vedoucího odboru IT. V případě, že by došlo k obnovení dat ze zálohy, veškeré výmazy provedené od poslední zálohy se zopakují ručně.

Součástí vyřízení musí být též upozornění na možnost, podat stížnost dozorovému úřadu.

7.6. Právo na omezení zpracování

Omezení zpracování osobních údajů musí nastat buď z podnětu subjektu OÚ, nebo automaticky. K omezení přístupu je nutno přistoupit v následujících případech:

- subjekt údajů popírá přesnost osobních údajů nebo
- zpracování je protiprávní a subjekt údajů odmítá výmaz osobních údajů a žádá místo toho o omezení jejich použití nebo
- správce již osobní údaje nepotřebuje pro účely zpracování, ale subjekt údajů je požaduje pro určení, výkon nebo obhajobu právních nároků nebo
- subjekt údajů vznesl námitku proti zpracování

Pokud k omezení má dojít z podnětu subjektu, v první řadě je potřeba ověřit, že se jedná o osobu oprávněnou omezení požadovat, tzn. je potřeba ji identifikovat. Subjekt má právo omezit zpracování informace, týkající se výlučně sebe samého; na omezení zpracování informace o jiných subjektech právo nemá.

Zejména upozorňujeme na skutečnost, že nelze omezit zpracování informace o subjektu, pokud se zpracovávají z důvodu plnění právní povinnosti, která se na Správce vztahuje, dále z důvodu veřejného zájmu a z důvodu ochrany životně důležitých zájmů subjektu. Rovněž nelze omezit zpracování osobních údajů, u kterých Správce je pouhým zpracovatelem (typickým příkladem jsou veřejné rejstříky).

Omezení zpracování musí nastat souběžně v listinné i v elektronické podobě dokumentu.

- U listinné podoby dokumentu se omezení provede tak, že se příslušné části dokumentu, případně celá složka, vyjmou a uloží se v příruční spisovně, na k tomu určené zabezpečené místo.
- U elektronické podoby se omezení provede tak, že se příslušná složka nebo její části zašifrují a heslo se v zalepené obálce uloží v příruční spisovně, na k tomu určené zabezpečené místo.

Součástí vyřízení musí být též upozornění na možnost, podat stížnost dozorovému úřadu.

7.7. Právo vznést námitku

Subjekt má právo vznést námitku proti zpracování osobních údajů, které se jej týkají, pokud jsou OÚ zpracovávány na základě:

- Plnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci
- Oprávněný zájem
- Přímý marketing

V případě, že subjekt OÚ vznese námitku proti zpracování, v první řadě je potřeba ověřit, že se jedná o osobu oprávněnou námitku podat, tzn. je potřeba ji identifikovat. Poté je potřeba ověřit, že ke zpracování OÚ dochází z některého výše uvedeného důvodu.

V tomto bodě má pracovník možnost volby. Podle instrukcí svého nadřízeného:

- buď může námitku akceptovat,
- nebo ji může zamítnout.

Pokud se pracovník rozhodl námitku akceptovat, buď musí příslušné osobní údaje vymazat (postupem analogickým ke kapitole 1. 4 Právo na výmaz), nebo musí omezit zpracování příslušných osobních údajů (postupem obdobným ke kapitole 1. 5 Právo na omezení zpracování). V tomto druhém případě lze doporučit, aby se na omezení zpracování dohodl se subjektem OÚ, nejlépe písemnou formou.

Pokud se pracovník rozhodl námitku zamítnout, musí prokázat, že zájem Správce převyšuje nad zájmem subjektu údajů. K tomu účelu shromáždí potřebné doklady a založí je do spisu.

7.8. Právo na přenositelnost

Subjekt má právo získat osobní údaje, které se ho týkají a které poskytl[11] správci, a to ve **strukturovaném, běžně používaném a strojově čitelném formátu**, a právo předat tyto údaje jinému správci. Přitom výkonem práva na přenositelnost nesmí být nepříznivě dotčena práva a svobody jiných osob. Toto právo lze uplatnit, pokud je **současně** splněno, že:

- zpracování je založené na právním důvodu (a) souhlasu nebo (b) smlouvy,
- zpracování se provádí automatizovaně.

V případě, že subjekt OÚ uplatní právo na přenositelnost, v první řadě je potřeba ověřit, že se jedná o osobu oprávněnou právo uplatnit, tzn. je potřeba ji identifikovat. Poté je potřeba ověřit, že jsou současně splněny obě výše uvedené podmínky a že výkonem práva na přenositelnost nebudou nepříznivě dotčena práva a svobody jiných osob.

Pokud nejsou splněny požadavky dané zákonem, požadavek se zamítne. V takovém případě je nutno uvést konkrétní důvod zamítnutí a subjekt OÚ poučit o jeho právu, podat proti rozhodnutí stížnost. Veškerá korespondence se založí do spisu, se kterým bude nakládáno podle Spisového řádu.

V případě, že jsou splněny všechny zákonné požadavky, data se subjektu vydají. [doplnit postup, jak se data pro subjekt nakopírují, na co a jak se zaúčtují případné náklady].

7.9. Právo na stížnost

Každý subjekt údajů má právo podat stížnost u některého dozorového úřadu, zejména v členském státě svého obvyklého bydliště, místa výkonu zaměstnání nebo místa, kde došlo k údajnému porušení, pokud se subjekt údajů domnívá, že zpracováním jeho osobních údajů je porušeno toto nařízení.

Pracovníci správce mají povinnost, na toto právo subjekt údajů výslovně upozornit, a to zřetelně a odděleně od jakýchkoli jiných informací, nejpozději v okamžiku první komunikace.

[11] podle platného výkladu (WP 29) jsou „údaje, jež správci poskytl“ data aktivně a vědomě poskytnutá subjektem údajů (např. emailová adresa, uživatelské jméno, věk atd.), nebo vysledovaná data poskytnutá subjektem na základě využívání služby nebo zařízení (vyhledávací historie, provozní a lokační údaje, atd.)

8. VZOR SMĚRNICE PRO OCHRANU OSOBNÍCH

Směrnice č. .... /2018/MěÚ

SMĚRNICE O OCHRANĚ OSOBNÍCH ÚDAJŮ

Čl. 1
Úvodní ustanovení

1. Tato Směrnice o ochraně osobních údajů (dále jen tato směrnice a/nebo směrnice) se jako interní akt řízení vydává na základě ust. § 13 zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, v platném znění a současně na základě Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů).

Čl. 2
Předmět, účel a působnost

1. Směrnice stanovuje opatření a pravidla, která zabraňují neoprávněnému nebo nahodilému přístupu k osobním údajům, a dále jejich změně, zničení či ztrátě, neoprávněným přenosům, jejich neoprávněnému zpracování, jakož i k jinému zneužití osobních údajů spravovaných a zpracovávaných Správcem OÚ. Ochranou osobních údajů dle směrnice se rozumí zajištění důvěrnosti spravovaných a zpracovávaných osobních údajů, jejich správnosti, integrity, dostupnosti a splnění dalších bezpečnostních a jiných požadavků v případě všech osobních údajů v míře potřebné pro činnost Správce OÚ, a to v souladu s Nařízením GDPR, se zákonem č. 101/2000 Sb. o ochraně osobních údajů v platném znění a s jinými právními předpisy.
2. Tato směrnice upravuje ochranu všech osobních údajů ve vlastnictví, ve správě Správce OÚ nebo Správcem OÚ zpracovávaných, bez ohledu na jejich podobu (tištěnou, psanou, uloženou elektronicky, odesílanou poštou, předávanou elektronicky, ústním podáním, telefonem, faxem apod.).
3. Za účelem ochrany osobních údajů je v rámci Správce OÚ ustanoven systém řízení ochrany osobních údajů, který je založen na těchto dokumentech, resp. vnitřních předpisech Správce OÚ:
   a) Organizační řád Městského úřadu Příbram,
   b) Spisový a skartační řád včetně Spisového a skartačního plánu,
   c) tato směrnice.
4. Systém ochrany osobních údajů definovaný touto směrnicí je navržen a zpracován v souladu s Nařízením Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů, dále jen „Nařízení GDPR“).
5. Přehled spravovaných agend osobních údajů formou Záznamů o činnostech zpracování je zaměstnancům Správce OÚ k dispozici u jeho Pověřence pro ochranu osobních údajů (DPO). Záznamy o činnostech zpracování jsou pravidelně aktualizovány.
6. Směrnice je závazná pro všechny osoby organizačně zařazené do struktury Správce OÚ, pro zaměstnance Správce OÚ, dále pro všechny další osoby, které nakládají s osobními údaji, které jsou ve správě Správce OÚ a zároveň vystupují v roli uživatelů v rámci Správce OÚ (např. zastupitelé) a povinnostmi v této směrnici stanovenými budou v přiměřeném rozsahu zavázány též osoby, které

osobní údaje zpracovávají na základě smlouvy uzavřené se Správcem OÚ jakožto správcem osobních údajů; toto ustanovení musí být v přiměřeném rozsahu součástí obsahu uzavřené smlouvy se zpracovatelem osobních údajů.

Čl. 3
Pojmy a definice

1. Pro účely této směrnice a ochrany osobních údajů v rámci Správce OÚ se rozumí:
   a) „osobními údaji" veškeré informace o identifikované nebo identifikovatelné fyzické osobě (dále jen „subjekt údajů"); identifikovatelnou fyzickou osobou je fyzická osoba, kterou lze přímo či nepřímo identifikovat, zejména odkazem na určitý identifikátor, například jméno, identifikační číslo, lokační údaje, síťový identifikátor nebo na jeden či více zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity této fyzické osoby; „zvláštními kategoriemi osobních údajů" osobní údaje, které vypovídají o rasovém či etnickém původu, politických názorech, náboženském vyznání či filozofickém přesvědčení nebo členství v odborech, a zpracování genetických údajů, biometrických údajů za účelem jedinečné identifikace fyzické osoby a údajů o zdravotním stavu či o sexuálním životě nebo sexuální orientaci fyzické osoby;
   b) „biometrickými údaji" osobní údaje vyplývající z konkrétního technického zpracování týkající se fyzických či fyziologických znaků nebo znaků chování fyzické osoby, které umožňuje nebo potvrzuje jedinečnou identifikaci, například zobrazení obličeje nebo daktyloskopické údaje;
   c) „zpracováním" jakákoliv operace nebo soubor operací s osobními údaji nebo soubory osobních údajů, které jsou prováděny pomocí či bez pomoci automatizovaných postupů, jako je shromáždění, zaznamenání, uspořádání, strukturování, uložení, přizpůsobení nebo pozměnění, vyhledání, nahlédnutí, použití, zpřístupnění přenosem, šíření nebo jakékoliv jiné zpřístupnění, seřazení či zkombinování, omezení, výmaz nebo zničení;
   d) „omezením zpracování" označení uložených osobních údajů za účelem omezení jejich zpracování v budoucnu;
   e) „pseudonymizací" zpracování osobních údajů tak, že již nemohou být přiřazeny konkrétnímu subjektu údajů bez použití dodatečných informací, pokud jsou tyto dodatečné informace uchovávány odděleně a vztahují se na ně technická a organizační opatření, aby bylo zajištěno, že nebudou přiřazeny identifikované či identifikovatelné fyzické osobě;
   f) „anonymizací" zpracování osobních údajů tak, že již nemohou být přiřazeny konkrétnímu subjektu údajů a subjekt údajů není nebo již přestal být identifikovatelným;
   g) „evidencí" jakýkoliv strukturovaný soubor osobních údajů přístupných podle zvláštních kritérií, ať již je centralizovaný, decentralizovaný, nebo rozdělený podle funkčního či zeměpisného hlediska;
   h) „Správcem OÚ" Město Příbram Sídlo úřadu: Tyršova 108 261 01 Příbram I. IČO: 00243132, jakožto právnická osoba, a orgán veřejné moci, který sám nebo společně s jinými určuje účely a prostředky zpracování osobních údajů;
   i) „zpracovatelem" fyzická nebo právnická osoba, orgán veřejné moci nebo agentura, která zpracovává osobní údaje pro správce;
   j) „příjemcem" fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, kterým jsou osobní údaje poskytnuty;

k) „souhlasem“ subjektu údajů jakýkoli svobodný, konkrétní, informovaný a jednoznačný projev vůle, kterým subjekt údajů dává prohlášením či jiným zjevným potvrzením své svolení ke zpracování svých osobních údajů;
l) „porušením zabezpečení osobních údajů“ porušení zabezpečení, které vede k náhodnému nebo protiprávnímu zničení, ztrátě, změně nebo neoprávněnému poskytnutí nebo zpřístupnění přenášených, uložených nebo jinak zpracovávaných osobních údajů;
m) „údaji o zdravotním stavu“ osobní údaje týkající se tělesného nebo duševního zdraví fyzické osoby, včetně údajů o poskytnutí zdravotních služeb, které vypovídají o jejím zdravotním stavu;
n) „záznamem o činnostech zpracování“ záznamy vedené Správcem OÚ o zpracování osobních údajů. Záznamy obsahují jméno a kontaktní údaje správce, účely zpracování, rozsah zpracovávaných osobních údajů, informace o příjemcích daných osobních údajů, o předávání údajů do třetích zemí, lhůtách pro výmaz jednotlivých kategorií údajů a popis přijatých technických a organizačních opatření k zajištění bezpečnosti údajů;
o) „dozorovým úřadem“ Úřad pro ochranu osobních údajů;
p) „Unií“ Evropská unie;
q) „Členské státy“ členské státy Evropské unie;
r) „pověřencem pro ochranu osobních údajů“/„pověřencem“/„DPO“ pověřenec pro ochranu osobních údajů podle oddílu 4 čl. 37 až 39 Nařízení GDPR;
s) „Vedením Správce OÚ“ starosta a tajemník městského úřadu;

2. V případě pochybností se pojmy uvedené v tomto článku vykládají dle Nařízení GDPR za zachování smyslu těchto pojmů v Nařízení GDPR uvedeném.

Čl. 4
Rozsah působnosti

1. Vedení Správce OÚ je odpovědné za to, že pravidla ochrany osobních údajů budou zachovávat zaměstnanci, a všechny další osoby, které nakládají s osobními údaji, které jsou ve správě Správce OÚ a zároveň vystupují v roli uživatelů nebo správců osobních údajů v rámci Správce OÚ.
2. Pravidla ochrany osobních údajů se vztahují rovněž na všechny další subjekty, které zpracovávají osobní údaje, jichž je Správce OÚ správcem. Tyto subjekty musí být k dodržování zásad ochrany osobních údajů zavázány postupem dle článku 23 této směrnice.

Čl. 5
Stanovení rolí v systému ochrany osobních údajů

1. Vedení Správce OÚ
   a) Odpovědnost za zajištění ochrany osobních údajů v souladu s Nařízením GDPR nese Vedení Správce OÚ a to zejména, tím, že:
      i. schvaluje Směrnici o nakládání a zpracování s osobními údaji Správce OÚ a její změny a aktualizace,
      ii. vyjadřuje se k osobě, která má vykonávat funkci Pověřence pro ochranu osobních údajů (dále také „Pověřenec“ a „DPO“),
      iii. jmenuje Pověřence pro ochranu osobních údajů,

iv. projednává pravidelnou zprávu o stavu ochrany osobních údajů Správce OÚ,pokud bude u Správce OÚ realizována.
v. rozhoduje o přijetí technických, fyzických a organizačních opatření pro zajištění souladu ochrany osobních údajů s Nařízením GDPR.

2. Pověřenec pro ochranu osobních údajů
   a) Pověřenec je jmenován Vedením Správce OÚ a je konkrétní osobou, která plní tyto úkoly při ochraně osobních údajů, za něž zároveň odpovídá:
      i. poskytování informací a poradenství vedoucím pracovníkům a zaměstnancům, kteří provádějí zpracování, o jejich povinnostech podle této směrnice, Nařízení GDPR a dalších předpisů Unie nebo členských států v oblasti ochrany údajů;
      ii. monitorování souladu této směrnice, Nařízení GDPR a dalších předpisů Unie nebo členských států v oblasti ochrany údajů a s vnitřními předpisy Správce OÚ v oblasti ochrany osobních údajů, včetně rozdělení odpovědnosti osob, zvyšování povědomí a odborné přípravy zaměstnanců či dalších osob a pracovníků zapojených do operací zpracování a souvisejících auditů;
      iii. vedení centrální evidence zpracování osobních údajů organizačními jednotkami Správce OÚ a její pravidelnou aktualizaci ve spolupráci s organizačními jednotkami;
      iv. vedení centrální evidence udělovaných souhlasů se zpracováním osobních údajů;
      v. zajištění pravidelného testování, posuzování a hodnocení účinnosti zavedených organizačních, technických a fyzických opatření pro zajištění bezpečnosti zpracování dle této směrnice;
      vi. zajištění monitoringu legislativních změn v oblasti ochrany osobních údajů a návrh na jejich implementaci v rámci Správce OÚ;
      vii. poskytování poradenství na požádání, pokud jde o posouzení vlivu na ochranu osobních údajů, a monitorování jeho uplatňování podle článku 35 Nařízení GDPR v rámci Správce OÚ;
      viii. spolupráce s dozorovým úřadem dle Nařízení GDPR;
      ix. působení jako kontaktní místo pro dozorový úřad v záležitostech týkajících se zpracování, včetně předchozí konzultace podle článku 36 Nařízení GDPR, a případně vedení konzultací v jakékoli jiné věci;
      x. působení jako kontaktní místo pro subjekty údajů. Subjekty údajů se mohou obracet přímo na Pověřence ve všech záležitostech souvisejících se zpracováním jejich osobních údajů a výkonem jejich práv podle Nařízení.
   b) Pověřenec pro ochranu osobních údajů bere při plnění svých úkolů patřičný ohled na riziko spojené s operacemi zpracování a současně přihlíží k povaze, rozsahu, kontextu a účelům zpracování.
   c) Pověřenec pro ochranu osobních údajů je přímo podřízen Vedení Správce OÚ.
   d) V souvislosti s plněním svých úkolů nebude Pověřenec propuštěn ani jinak sankcionován. Pověřence nelze nijak postihovat za nezávislý způsob výkonu povinností (tzn. za to, že zastává jiný názor než Správce OÚ, nebo že kontaktoval dozorový úřad, atp.), např. ukončením smlouvy o spolupráci, snížením odměny za výkon funkce pověřence nebo jakýmkoli jiným způsobem.
   e) Pověřenec je v souvislosti s výkonem svých úkolů vázán mlčenlivostí, a to v souladu s právem Unie nebo zákony a právními předpisy České republiky. Pověřenec může plnit i jiné úkoly a povinnosti, které však nesmějí vést ke střetu zájmů jeho činností.

3. Zodpovědné osoby
   a) Ke každé agendě osobních údajů je v rámci Správce OÚ určena zodpovědná osoba, za řádné a včasné určení zodpovědných osob odpovídá Vedení Správce OÚ. Všechny

zodpovědné osoby v rámci Správce OÚ jsou uvedeny v Záznamech o činnosti zpracování osobních údajů, které jsou zaměstnancům Správce OÚ k dispozici u DPO, nebov sekretariátech Vedení Správce OÚ. Každá Zodpovědná osoba má právo podat Pověřenci návrh na změnu této směrnice, Záznamu o činnostech zpracování, Posouzení vlivu nebo zavedených organizačních, technických a fyzických opatření pro zajištění bezpečnosti zpracování dle této směrnice.

b) Zodpovědné osoby mají právo a zároveň povinnost:
   i. pro případy vzniku nových druhů osobních údajů tuto skutečnost co nejdříve nahlásit Pověřenci, který provede aktualizaci Záznamů o činnostech zpracování a souvisejících opatření na ochranu osobních údajů;
   ii. informovat bezodkladně Pověřence o všech skutečnostech, které mají vliv na aktuálnost Záznamů o činnostech zpracování a souvisejících opatření na ochranu osobních údajů;
   iii. zabezpečit získání souhlasu subjektu údajů, a to v souladu se zákonem, není-li zpracování možné bez tohoto souhlasu;
   iv. zajistit, aby každý zaměstnanec Správce OÚ před prvním přístupem ke spravovaným osobním údajům byl prokazatelně seznámen a proškolen se zásadami ochrany osobních údajů, a s touto směrnicí včetně provedení ověření znalostí a zajistit v roční frekvenci prokazatelné opakování tohoto proškolení;
   v. zajistit, aby každý zaměstnanec Správce OÚ před prvním přístupem ke spravovaným osobním údajům písemně potvrdil, že byl seznámen a proškolen se zásadami ochrany osobních údajů, a s touto směrnicí včetně provedení ověření znalostí;
   vi. při uzavírání smluv s třetími stranami dbát na to, aby obsahovaly zásady zajištění ochrany osobních údajů, pokud je to vzhledem k povaze obsahu smlouvy relevantní a v odůvodněných případech zajistit uzavření smlouvy o zpracování osobních údajů s třetí osobou

4. Uživatelé osobních údajů
   a) Uživatelem osobních údajů, se rozumí zaměstnanec Správce OÚ používající spravované osobní údaje k plnění svých pracovních povinností. Za zaměstnance se považuje též osoba vykonávající činnost dle dohody o pracích konaných mimo pracovní poměr, či v jiném obdobném právním vztahu vůči Správci OÚ.
   b) Všichni Uživatelé osobních údajů mají za povinnost:
      i. dodržovat zásady vyplývající z této směrnice;
      ii. hlásit veškeré bezpečnostní incidenty svému nadřízenému, nebo přímo Pověřenci;
      iii. informovat Pověřence o zjištěných bezpečnostních nedostatcích při ochraně osobních údajů;
      iv. informovat Pověřence o změnách ve způsobu zpracování a nakládání s osobními údaji;
      v. vykonávat další činnosti vyplývající z platných vnitřních předpisů Správce OÚ, především zajistit řádný průběh skartačního řízení v souladu se Spisovým a skartačním řádem včetně Spisového a skartačního plánu Správce OÚ v součinnosti se zaměstnanci Centrální spisovny Správce OÚ.
5. Správce (Administrátor) dále jen „Správce“
   a) Správce je zaměstnanec Správce OÚ, který má na starost provoz a údržbu systémů a aplikací, archivaci a zabezpečení (elektronických) dat uživatelů, a je odpovědný za řízení a implementaci bezpečnosti systémů. Správce (Administrátor) má zpravidla přístup ke všem datům uloženým v informačních systémech Správce OÚ nebo fyzický přístup k zařízením, pomocí nichž jsou tato data zpracovávána.

b) Správce zabezpečuje spolupráci s jednotlivými uživateli osobních údajů při ochraně osobních údajů uložených ve výpočetní technice, včetně osobních stanic přidělených uživatelům osobních údajů, přenosných počítačů, notebooků, tabletů, mobilních telefonů, smartphonů a jiných obdobných přístrojů.

Čl. 6
Přístup k osobním údajům

1. K osobním údajům mají přístup pouze Zodpovědné osoby, Uživatelé osobních údajů, zpracovatelé a Správce, jiným osobám se přístup k osobním údajům zapovídá.

Čl. 7
Zásady zpracování osobních údajů

1. Osobní údaje musí být:
   a) ve vztahu k subjektu údajů zpracovávány korektně a zákonným a transparentním způsobem („zákonnost, korektnost a transparentnost");
   b) shromažďovány pro určité, výslovně vyjádřené a legitimní účely a nesmějí být dále zpracovávány způsobem, který je s těmito účely neslučitelný, přičemž další zpracování pro účely archivace ve veřejném zájmu, pro účely vědeckého či historického výzkumu nebo pro statistické účely se ve smyslu čl. 89 odst. 1 Nařízení GDPR a dle této směrnice nepovažuje za neslučitelné s původními účely („účelové omezení");
   c) přiměřené, relevantní a omezené na nezbytný rozsah ve vztahu k účelu, pro který jsou zpracovávány („minimalizace údajů");
   d) přesné a v případě potřeby aktualizované; musí být přijata veškerá rozumná opatření, aby osobní údaje, které jsou nepřesné s přihlédnutím k účelům, pro které se zpracovávají, byly bezodkladně vymazány nebo opraveny („přesnost");
   e) uloženy ve formě umožňující identifikaci subjektů údajů po dobu ne delší, než je nezbytné pro účely, pro které jsou zpracovávány; osobní údaje lze uložit po delší dobu, pokud se zpracovávají výhradně pro účely archivace ve veřejném zájmu, pro účely vědeckého či historického výzkumu nebo pro statistické účely podle čl. 89 odst. 1 Nařízení GDPR, a to za předpokladu provedení příslušných technických a organizačních opatření požadovaných Nařízením s cílem zaručit práva a svobody subjektu údajů („omezení uložení");
   f) zpracovávány způsobem, který zajistí náležité zabezpečení osobních údajů, včetně jejich ochrany pomocí vhodných technických nebo organizačních opatření před neoprávněným či protiprávním zpracováním a před náhodnou ztrátou, zničením nebo poškozením („integrita a důvěrnost").
2. Zpracovávány mohou být pouze osobní údaje, jež jsou pro každý konkrétní účel daného zpracování nezbytné. Povinnost zpracovávat pouze nezbytné osobní údaje se vztahuje k množství shromážděných osobních údajů, rozsahu jejich zpracování, doby jejich uložení a jejich dostupnosti. Správní, či jiný spis vedený Uživatelem osobních údajů může obsahovat pouze informace relevantní pro průběh řízení či jinou agendu Uživatele osobních údajů, pro niž je veden. Uživatel osobních údajů odpovídá za minimalizaci údajů, jež jsou zpracovávány dosažení účelu zpracování.
3. Písemnosti obsahující osobní údaje podléhají procesu fyzické a elektronické skartace v souladu se Spisovým a skartačním řádem včetně Spisového a skartačního plánu Správce OÚ, a to včetně

písemností a dalších dokumentů „na vědomí“, kopií písemností a dalších dokumentů bez čísla jednacího.

4. Pro statistické účely se stanoví povinnost osobní údaje anonymizovat.
5. Tato směrnice stanovuje povinnost všem uživatelům osobních údajů, zodpovědným osobám a správcům zamezit neoprávněnému přístupu ke shromážděným údajům.

Čl. 8
Zákonnost zpracování osobních údajů

1. Správce OÚ zpracovává pouze takové osobní údaje, jejichž zpracování je zákonné. Zpracování osobních údajů v odpovídajícím rozsahu je zákonné, pouze pokud je splněna nejméně jedna z těchto podmínek:
   a) subjekt údajů udělil souhlas se zpracováním svých osobních údajů pro jeden či více konkrétních účelů (dále jen „souhlas“/ „souhlas se zpracováním“);
   b) zpracování je nezbytné pro splnění smlouvy, jejíž smluvní stranou je subjekt údajů, nebo pro provedení opatření přijatých před uzavřením smlouvy na žádost tohoto subjektu údajů;
   c) zpracování je nezbytné pro splnění právní povinnosti, která se vztahuje na Správce OÚ jako správce osobních údajů;
   d) zpracování je nezbytné pro ochranu životně důležitých zájmů subjektu údajů nebo jiné fyzické osoby;
   e) zpracování je nezbytné pro splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci, kterým je pověřeno Správce OÚ jako správce osobních údajů;
   f) zpracování je nezbytné pro účely oprávněných zájmů Správce OÚ jako správce osobních údajů či třetí strany, kromě případů, kdy před těmito zájmy mají přednost zájmy nebo základní práva a svobody subjektu údajů vyžadující ochranu osobních údajů, zejména pokud je subjektem údajů dítě. Toto se netýká zpracování, prováděného Správcem OÚ jako správcem osobních údajů při plnění jeho úkolů jako orgánu veřejné moci.
2. Účel zpracování osobních údajů musí vycházet z právních základů uvedených v předcházejícím odstavci. Osobní údaje nesmějí být použity k jinému účelu, než ke kterému byly pořízeny nebo musí být takové zpracování nutné pro splnění úkolu prováděného ve veřejném zájmu či při výkonu veřejné moci, kterým je pověřen Správce OÚ jako správce osobních údajů.
3. Pokud je zpracování založeno na souhlasu subjektu údajů, je Uživatel osobních údajů povinen doložit, že subjekt údajů udělil souhlas se zpracováním svých osobních údajů. Uživatel osobních údajů je dále povinen zajistit a doložit splnění těchto požadavků na souhlas subjektu údajů a na jeho udělení kladených:
   a) Souhlas musí být udělen samostatně a musí být jasně odlišitelný od ostatních sdělení (jako samostatný dokument). Vzor souhlasu se zpracováním osobních údajů je zaměstnancům Správce OÚ k dispozici u Pověřence.
   b) Subjekt údajů vždy musí obdržet jednu kopii uděleného souhlasu, včetně informace o způsobu odvolání uděleného souhlasu. Originál souhlasu uloží Uživatele osobních údajů do správního spisu či do dokumentace.
   c) Pro zpracování zvláštních kategorií osobních údajů (biometrické údaje, fotografie, audio, video, zdravotní stav, sociální postavení a další) se uděluje vždy samostatný souhlas, oddělený od ostatních souhlasů, sdělení a informací (platí v případě, že není jiné oprávnění pro nakládání s osobními údaji).

d) Pro zpracování souhlasů s vytvořením kopie občanského průkazu (souhlas podle ustanovení § 15a zákona č. 328/1999 Sb., o občanských průkazech, v platném znění) se uděluje vždy samostatný souhlas, oddělený od ostatních souhlasů, sdělení a informací (platí v případě, že není jiné oprávnění pro nakládání s osobními údaji).
e) Subjekt údajů má právo svůj souhlas kdykoli odvolat. Odvoláním souhlasu není dotčena zákonnost zpracování vycházejícího ze souhlasu, který byl dán před jeho odvoláním. Před udělením souhlasu bude subjekt údajů o právu souhlas odvolat prokazatelně poučen. Uživatel osobních údajů zajistí, aby byl splněn právní požadavek spočívající v tom, že odvolání souhlasu se zpracováním osobních údajů bude subjektu údajů stejně dostupné jako poskytnutí souhlasu.
f) Uživatel osobních údajů je povinen ve spolupráci se Správcem (Administrátorem) zajistit výmaz osobních údajů v případě odvolání souhlasu se zpracováním osobních údajů, včetně výmazu v zálohách a kopiích dat.
g) Uživatel osobních údajů je povinen vést evidenci datových sad, jejichž zpracování je podloženo uděleným souhlasem subjektu údajů.

4. Zpracování údajů na základě uděleného souhlasu subjektu údajů je využíváno pouze v krajních případech, kdy je zpracování nezbytné a neexistuje jiné oprávnění pro zpracování osobních údajů.

Čl. 9
Opatření pro ochranu osobních údajů

1. Uživatel osobních údajů je povinen dodržovat pravidlo čistého stolu, tzn. neponechávat volně položené písemnosti obsahující osobní údaje bez dozoru na svém pracovním stole či jinde v kanceláři či na pracovišti, po ukončení pracovní doby je každý zaměstnanec povinen takové písemnosti obsahující osobní údaje uložit do uzamykatelných úložných prostor, tyto prostory uzamknout a klíče zajistit tak, aby k nim neměly přístup osoby bez oprávnění přístupu k uloženým osobním údajům. Výjimkou z tohoto pravidla je případ, kdy má zaměstnanec k dispozici samostatnou kancelář, v této kanceláři probíhá úklid výhradně za jeho přítomnosti a klíče od této kanceláře má k dispozici pouze daný zaměstnanec a dále jsou uloženy v prostoru s řízeným přístupem.
2. Uživatel osobních údajů je povinen v případě odchodu z kanceláře, pracovny či jiného pracoviště, kde jsou uloženy osobní údaje, nebo prostředky umožňující přístup k osobním údajům, a kde se již nenachází žádný další zaměstnanec Správce OÚ, zavřít okna a tuto místnost zamknout.
3. Uživatelům osobních údajů se zapovídá ponechat cizí osobu bez dozoru v kanceláři. Uživatel osobních údajů je povinen v případě přítomnosti cizí osoby v kanceláři, v pracovně či na jiném pracovišti, kde jsou uloženy osobní údaje, nebo prostředky umožňující přístup k osobním údajům, a kde se již nenachází žádný další zaměstnanec Správce OÚ, pokud Uživatel osobních údajů hodlá tuto místnost opustit, a v této místnosti se již nenachází žádný další Uživatel osobních údajů či zaměstnanec Správce OÚ, vyprovodit cizí osobu z místnosti, tuto místnost uzamknout a opětovný vstup cizí osoby do kanceláře umožnit až při vlastním návratu Uživatele osobních údajů do místnosti.
4. Uživatel osobních údajů je povinen uzamknout pracovní stanici výpočetní techniky s použitím hesla, kdykoli se vzdálí od pracovní stanice výpočetní techniky.
5. Uživatel osobních údajů je povinen využívat pro elektronické zpracování osobních údajů výhradně k tomu určené informační systémy Správce OÚ. Užívání jakýchkoli jiných medií, tj. pevných disků, CD disků, DVD disků, Blu-ray disků, FLASH disků, mikrofilmů a mikrofiší pro ukládání dokumentů

obsahujících osobní údaje je povoleno pouze se souhlasem Správce OÚ v případě, že není možné tuto dokumentaci ukládat do informačních systémů Správce OÚ.

6. Uživatel osobních údajů je povinen udržovat dokumenty obsahující osobní údaje a obsah svých emailových schránek v souladu s lhůtami stanovenými pro zpracování dle Spisového a skartačního řádu včetně Spisového a skartačního plánu Správce OÚ a v minimálním rozsahu umožňujícím dosažení účelu zpracování.
7. Uživatel osobních údajů je povinen využívat pro ukládání listinných dokumentů obsahujících osobní údaje a k ukládání fyzických nosičů, obsahujících osobní údaje v elektronické podobě k tomu určené zabezpečené úložné prostory a tyto úložné prostory při opuštění místnosti uzamknout. Uživatel osobních údajů je povinen k písemnostem obsahujícím osobní údaje přiřazovat řádně a včas skartační znaky dle platného dle Spisového a skartačního řádu včetně Spisového a skartačního plánu Správce OÚ. To platí i pro písemnosti, obsahující osobní údaje „na vědomí", kopie písemností a další dokumenty bez čísla jednacího či spisové značky.
8. Uživatel osobních údajů je povinen udržovat v tajnosti, tzn. nikomu nesdělovat přístupová oprávnění (přihlašovací jméno a heslo) k informačním systémům Správce OÚ, která mu byla přidělena, tato přístupová oprávnění je zakázáno si zapisovat či jinak poznamenávat (na papír, do souboru, apod.).
9. Uživatel osobních údajů je povinen při tisku písemností obsahujících osobní údaje tyto nikdy neponechávat bez dozoru na tiskárně, a to i tehdy, pokud se tiskárna nachází ve stejné místnosti. Toto pravidlo obdobně platí též pro použití jiných reprografických či jiných obdobných zařízení.
10. Uživateli osobních údajů se zakazuje přeposílat písemnosti obsahující osobní údaje na své nebo cizí soukromé emailové schránky (např. www.seznam.cz, www.gmail.com apod.).
11. Uživateli osobních údajů se zakazuje zasílat písemnosti obsahující osobní údaje emailem bez jejich dodatečného zabezpečení za pomoci šifrování (.ZIP nebo .PDF s heslem). V případě použití šifrování (.ZIP nebo .PDF s heslem) musí být heslo k souboru předáno jiným kanálem (SMS nebo telefonicky).
12. Uživatel osobních údajů je povinen pro předání osobních údajů použít výhradně spisovou službu Správce OÚ.
13. Uživateli osobních údajů se zakazuje ukládat na veřejné servery sítě Internet (např. www.uloz.to, www.uschovna.cz apod.) na sociální sítě Facebook, Twitter a další jakékoli písemnosti obsahující osobní údaje bez jejich zabezpečení šifrováním (.ZIP s heslem, .PDF s heslem). Technický přístup na úložiště Internetu, sociální sítě Facebook, Twitter a další je vyhrazen pouze těm předem určeným zaměstnancům, u nichž je takové sdílení dat odůvodněno charakterem jejich pracovní činnosti.
14. Uživateli osobních údajů se zapovídá provádět na svěřené výpočetní technice jakékoliv hardwarové zásahy (např. měnit komponenty počítače, připojovat vlastní externí zařízení apod.) a spouštět či instalovat jakýkoliv nepovolený software či připojovat jakákoli Správcem OÚ neschválená technická zařízení, paměťová media, výpočetní techniku, notebooky, mobilní telefony či smartphony nebo tablety.
15. Uživatel osobních údajů je povinen využívat mobilní zařízení Správce OÚ (technická zařízení, paměťová media, výpočetní techniku, notebooky, mobilní telefony či smartphony nebo tablety.) pouze při dodržení pravidel pro jejich zabezpečení definovaných Správcem, zejména je povinen použít Správcem nařízené šifrování v případě notebooku a hesla na mobilním telefonu či tabletu.
16. Uživateli osobních údajů se zakazuje využívat k přístupu k informačním systémům a datům Správce OÚ soukromá mobilní zařízení (paměťová media, výpočetní techniku, notebooky, mobilní telefony či smartphony nebo tablety apod.).
17. Uživateli osobních údajů se zakazuje jakkoliv měnit nastavení, případně vypínat ochranu proti škodlivému kódu (antivirový program, antispyware apod.) na svěřených prostředcích (paměťová media, výpočetní technika, notebooky, mobilní telefony či smartphony nebo tablety).

18. Uživatel osobních údajů je povinen v případě tisku na sdílené tiskárně či v případě použití jiného sdíleného obdobného reprografického zařízení tisky obsahující osobní údaje vždy zabezpečit PINem, a to tak, aby byly vytištěny až po zadání PINU na sdílené tiskárně či na jiném sdíleném obdobném reprografickém zařízení uživatelem osobních údajů.
19. Uživateli osobních údajů se zakazuje ukládat na vyměnitelná paměťová média jakékoliv písemnosti obsahující osobní údaje bez jejich zabezpečení pro předávání dat šifrováním (*.ZIP, *.PDF), a stejně tak se mu zakazuje vynášet tato paměťová media mimo prostory Správce OÚ. K ukládání písemností obsahujících osobní údaje jsou uživatelům osobních údajů k dispozici (u Správce IT) HW šifrované flash disky, jež jsou povinni použít. Vyměnitelnými médii se rozumí CD/DVD disky, přepisovatelné CD/DVD, pevné počítačové disky externí, flash disky apod.
20. Každý uživatel osobních údajů či jiný zaměstnanec Správce OÚ, který přichází do styku s písemnostmi obsahujícími osobní údaje uloženými na médiích (CD, DVD, papírové dokumenty, flash paměťové moduly) je povinen zajistit jejich bezpečnou likvidaci (skartování, vymazání, fyzické zničení) v souladu se dle Spisovým a skartační řádem včetně Spisového a skartačního plánu Správce OÚ.
21. Klíče od kanceláří, pracoven či jiných pracovišť, kde jsou uloženy či zpracovávány osobní údaje, nebo prostředky umožňující přístup k osobním údajům Správce OÚ vydává uživateli osobních údajů pouze prokazatelným způsobem, když o jejich vydání a vrácení bude vedena příslušná evidence. Správce OÚ podrobí evidenci a kontrole ukládání a zabezpečení náhradních klíčů od kanceláří, pracoven či jiných pracovišť, kde jsou uloženy či zpracovávány osobní údaje, nebo prostředky umožňující přístup k osobním údajům.
22. Uživatelé osobních údajů nejsou oprávněni hovořit (osobně ani telefonicky) o osobních údajích v přítomnosti třetích osob. Tato povinnost se vztahuje též na předávání informací zaměstnancům Správce OÚ, kteří nemají k těmto osobním údajům přístup.

Čl. 10
Předávání osobních údajů

1. Dokumenty obsahující osobní údaje, jakožto i osobní údaje samotné je v elektronické podobě povoleno předávat příjemcům mimo Správce OÚ pouze prostřednictvím systému datových schránek. V případech, kdy není možné dokumenty obsahující osobní údaje, jakožto i osobní údaje samotné předat prostřednictvím systému datových schránek nebo ve fyzické podobě, bude předání realizováno za využití šifrování (například .PDF nebo .ZIP), když heslo k souboru bude předáno jiným kanálem (SMS nebo telefonicky).

Čl. 11
Zveřejňování osobních údajů

1. Při zveřejňování osobních údajů budou provedena opatření, která zajistí, že veškeré zveřejňované osobní údaje (text, audio, video) budou anonymizovány v rozsahu zajišťujícím minimalizaci rozsahu zveřejňovaných osobních údajů při dosažení účelu zveřejnění uloženého legislativou. To znamená, že zveřejněné osobní údaje budou anonymizovány ve všech případech, kdy zákon nestanoví jinak. Výjimkou z tohoto pravidla jsou pouze ty případy zveřejnění osobních údajů, kdy ke zveřejnění byl subjektem údajů udělen souhlas dle Čl. 7. odst. 1 této směrnice.

2. Opatření zajišťující anonymizaci osobních údajů budou provedena u osobních údajů třetích osob ve smlouvách, které jsou zveřejněny v Registru smluv.
3. Při pořizování jakýchkoliv záznamů z akcí pořádaných Správcem OÚ budou účastníci akce informováni o pořizování audio/video dokumentace a o účelu o účelu pořizování audio/video dokumentace. Bude-li pořízení audio/video dokumentace zpracováním osobních údajů, je Uživatel osobních údajů povinen zajistit řádné a včasné udělení souhlasu subjektu údajů se zpracováním jeho osobních údajů.
4. V případě pořizování fotografické nebo video dokumentace z veřejných akcí Správce OÚ, bude zajištěno informování účastníků o pořizování této dokumentace za účelem zveřejnění na webových stránkách Správce OÚ apod. Ustanovení předcházejícího odstavce této směrnice tu platí obdobně.
5. Fotografie zaměstnanců Správce OÚ budou pořizovány a zveřejňovány na webových stránkách Správce OÚ anebo jinými způsoby, pouze tehdy, pokud k jejich pořízení a zveřejnění byl zaměstnancem jakožto subjektem údajů udělen souhlas dle Čl. VII. Odst. 1 této směrnice. Zveřejnění fotografií zaměstnanců Správce OÚ bez takového souhlasu je možné pouze u osob, u kterých je to odůvodnitelné s ohledem na výkon jejich činnosti či postavení v řídící struktuře Správce OÚ (starosta, zastupitel, tiskový mluvčí, pracovník pověřený marketingem apod.).

Čl. 12
Získávání informací od subjektu údajů

1. Příslušný zaměstnanec Správce OÚ či Uživatel osobních údajů v případě získání osobních údajů poskytne subjektu údajů předem tyto informace:
   a) totožnost a kontaktní údaje Správce OÚ a jeho příslušného zaměstnance (Uživatele osobních údajů);
   b) kontaktní údaje Pověřence;
   c) účely zpracování, pro které jsou získávané osobní údaje určeny, a právní základ pro jejich zpracování;
   d) oprávněné zájmy Správce OÚ nebo třetí strany v případě, že je zpracování založeno na opodstatněném zájmu Správce OÚ jako správce osobních údajů;
   e) případné příjemce nebo kategorie příjemců osobních údajů;
   f) doba, po kterou budou osobní údaje uloženy, nebo není-li ji možné určit, kritéria použitá pro stanovení této doby;
   g) existence práva požadovat od Správce OÚ jako od správce osobních údajů přístup k osobním údajům týkajících se subjektu údajů, jejich opravu nebo výmaz, popřípadě omezení zpracování, a vznést námitku proti zpracování, jakož i práva na přenositelnost údajů;
   h) existence práva odvolat kdykoli souhlas, aniž je tím dotčena zákonnost zpracování založená na souhlasu uděleném před jeho odvoláním (pokud je zpracování založeno na uděleném souhlasu se zpracováním osobních údajů);
   i) o právu podat stížnost u dozorového úřadu;
   j) o skutečnosti, zda poskytování osobních údajů je zákonným či smluvním požadavkem, nebo požadavkem, který je nutné uvést do smlouvy, a zda má subjekt údajů povinnost osobní údaje poskytnout, a poučení ohledně možných důsledků neposkytnutí těchto údajů.
2. Splnění informační povinnosti podle předcházejícího odstavce může být zajištěno zveřejněním Informačního memoranda na webových stránkách Správce OÚ.

3. Pokud Správce OÚ jako správce osobních údajů hodlá osobní údaje dále zpracovávat pro jiný účel, než je účel, pro který byly shromážděny, poskytne subjektu údajů ještě před uvedeným dalším zpracováním informace o tomto jiném účelu a příslušné další informace v rozsahu dle tohoto článku.

Čl. 13
Práva subjektu údajů

1. Subjekt údajů je oprávněn a může uplatnit u Správce OÚ právo na:
   a) přístup k osobním údajům
   b) opravu a výmaz osobních údajů
   c) omezení zpracování osobních údajů
   d) přenositelnost osobních údajů
   e) vznesení námitky
2. Naplnění práv subjektů údajů, jež byla u Správce OÚ uplatněna v souladu s Nařízením GDPR, je povinen zajistit Pověřenec.
3. Pokud je pro zajištění práv subjektů údajů nutné zapojení více organizačních jednotek Správce OÚ, zajišťuje jejich koordinaci a shromáždění potřebných informací Pověřenec.
4. Způsob podání žádosti o naplnění práv subjektů údajů je zveřejněn na webových stránkách Správce OÚ, případně dalšími vhodnými způsoby.
5. Subjektu údajů budou poskytovány informace v souladu se zásadami zpracování osobních údajů dle čl. 7 této směrnice a to stručným, transparentním, srozumitelným a snadno přístupným způsobem za použití jasných a jednoduchých jazykových prostředků, zejména pokud se jedná o informace určené dítěti, či osobě, u níž byla svéprávnost omezena, či u níž tento přístup odůvodňuje zvláštní důvody.
6. Informace jsou subjektu údajů poskytovány výhradně na základě prokazatelného jednoznačného ověření totožnosti subjektu údajů (předložení dokladu totožnosti, či použití datové schránky).
7. Informace jsou subjektu údajů poskytovány písemně nebo jinou formou, připuštěna je ve vhodných případech i elektronická forma. Pokud si to subjekt údajů vyžádá, budou informace poskytnuty pouze ústně.
8. Informace budou subjektu údajů poskytnuty bez zbytečného odkladu a nejpozději ve lhůtě do jednoho kalendářního měsíce od doručení žádosti. Tuto lhůtu je možné v případě potřeby a s ohledem na složitost a počet žádostí prodloužit o další maximálně dva kalendářní měsíce, kdy subjekt údajů musí být o takovém odůvodněném prodloužení lhůty k poskytnutí údajů vyrozuměn nejpozději ve lhůtě do jednoho kalendářního měsíce od doručení žádosti.
9. Pokud opatření, o něž subjekt údajů požádal, nejsou provedena, bude subjekt údajů bezodkladně a nejpozději ve lhůtě do jednoho kalendářního měsíce od doručení žádosti informován Správcem OÚ o důvodech nerealizování opatření a o jeho možnosti podat stížnost u dozorového úřadu a o možnosti žádat o soudní ochranu dle Nařízení GDPR.
10. Veškeré poskytované informace, sdělení a úkony budou Správcem OÚ poskytnuty a provedeny bezplatně. Jsou-li žádosti podané subjektem údajů zjevně (dle současné legislativy lze jako orientační měřítko vzít četnost 1 žádosti za 30 dní) nedůvodné nebo nepřiměřené, zejména protože jsou opakovány, lze přistoupit k:
    a) uložení přiměřeného poplatku zohledňujícího administrativní náklady spojené s poskytnutím požadovaných informací, sdělení nebo s učiněním požadovaných úkonů;
    b) odmítnutí žádosti vyhovět.

11. Zjevnou nedůvodnost nebo nepřiměřenost žádosti je zaměstnanec správce OÚ, či uživatel osobních údajů, který žádost subjektu údajů v rámci své činnosti u Správce OÚ vyřizuje, povinen odůvodnit a zdokumentovat.

Čl. 14
Právo subjektu údajů na přístup k osobním údajům

1. Subjekt údajů má právo získat od Správce OÚ jako správce osobních údajů potvrzení, zda osobní údaje, které se ho týkají, jsou či nejsou zpracovávány, a pokud jsou zpracovávány, má právo získat přístup k těmto osobním údajům a k následujícím informacím:
   a) účely zpracování;
   b) kategorie dotčených osobních údajů;
   c) příjemci nebo kategorie příjemců, kterým osobní údaje byly nebo budou zpřístupněny;
   d) plánovaná doba, po kterou budou osobní údaje uloženy, nebo není-li ji možné určit, kritéria použitá ke stanovení této doby;
   e) existence práva požadovat od Správce OÚ jako od správce osobních údajů opravu nebo výmaz osobních údajů týkajících se subjektu údajů nebo omezení jejich zpracování, anebo vznést námitku proti tomuto zpracování;
   f) právo podat stížnost u dozorového úřadu;
   g) veškeré dostupné informace o zdroji osobních údajů, pokud nejsou získány od subjektu údajů.
2. Správce OÚ jako správce osobních údajů poskytne subjektu údajů kopii zpracovávaných osobních údajů. Za další kopie na žádost subjektu údajů může Správce OÚ jako správce osobních údajů účtovat přiměřený poplatek na základě administrativních nákladů. Při stanovení výše administrativních nákladů Správce postupuje analogicky podle předpisů o svobodném přístupu k informacím. Jestliže subjekt údajů podává žádost v elektronické formě, poskytnou se informace v elektronické formě, která se běžně používá, pokud subjekt údajů nepožádá o jiný způsob.
3. Právem získat kopii uvedenou v předchozím odstavci nesmějí být nepříznivě dotčena práva a svobody jiných osob (údaje jiných osob musejí být anonymizovány).

Čl. 15
Oprava a výmaz osobních údajů

1. Subjekt údajů má právo na to, aby Správce OÚ jako správce osobních údajů bez zbytečného odkladu opravil nepřesné osobní údaje, které se ho týkají. S přihlédnutím k účelům zpracování má subjekt údajů právo na doplnění neúplných osobních údajů, a to i poskytnutím dodatečného prohlášení.
2. Subjekt údajů má právo na to, aby Správce OÚ jako správce osobních údajů bez zbytečného odkladu vymazal osobní údaje, které se daného subjektu údajů týkají, a Správce OÚ má povinnost osobní údaje bez zbytečného odkladu vymazat (tzv. „právo být zapomenut“), pokud je dán jeden z těchto důvodů:
   a) osobní údaje již nejsou potřebné pro účely, pro které byly shromážděny nebo jinak zpracovány;
   b) subjekt údajů odvolá souhlas, na jehož základě byly údaje zpracovány, a neexistuje žádný další právní důvod pro zpracování a jejich uchovávání;

c) subjekt údajů vznese námitky proti zpracování s ohledem na uplynutí lhůty pro zpracování nebo s ohledem na prokazatelnou nedostatečnost zabezpečení osobních údajů;
d) osobní údaje byly zpracovány protiprávně;
e) osobní údaje musí být skartovány ke splnění právní povinnosti stanovené právem Unie nebo zákony a platnými právními předpisy České republiky, které se na Správce OÚ jako správce osobních údajů vztahují.

3. Jestliže Správce OÚ jako správce osobních údajů osobní údaje zveřejnil a je povinen je podle odstavce 2 této směrnice vymazat, přijme s ohledem na dostupnou technologii a náklady na provedení přiměřené kroky, včetně všech technických opatření k tomu, aby informoval zpracovatele, kteří tyto osobní údaje zpracovávají, že je subjekt údajů žádá, aby též provedli výmaz veškerých odkazů na tyto osobní údaje, jejich kopie či replikace.
4. Odstavce 2 a 3 se neuplatní, pokud je zpracování nezbytné:
   a) pro výkon práva na svobodu projevu a informace;
   b) pro splnění právní povinnosti, jež vyžaduje zpracování podle práva Unie nebo ČR, které se na Správce OÚ jako na správce osobních údajů vztahuje, nebo pro splnění úkolu provedeného ve veřejném zájmu nebo při výkonu veřejné moci, kterým je Správce OÚ pověřeno;
   c) z důvodů veřejného zájmu v oblasti veřejného zdraví v souladu s čl. 9 odst. 2 písm. h) a i) a čl. 9 odst. 3 Nařízení GDPR;
   d) pro účely archivace ve veřejném zájmu, pro účely vědeckého či historického výzkumu či pro statistické účely podle zvláštních právních předpisů;
   e) pro určení, výkon nebo obhajobu právních nároků.
5. Požadavek subjektu údajů na výmaz nelze splnit, pokud je zpracování nezbytné pro splnění právní povinnosti.

Čl. 16

Právo na omezení zpracování

1. Subjekt údajů má právo na to, aby Správce OÚ jako správce osobních údajů omezil zpracování v kterémkoli z těchto případů:
   a) subjekt údajů popírá přesnost osobních údajů, a to na dobu potřebnou k tomu, aby Správce OÚ jako správce osobních údajů mohl přesnost osobních údajů ověřit;
   b) zpracování je protiprávní a subjekt údajů odmítá výmaz osobních údajů a žádá místo toho o omezení jejich použití;
   c) Správce OÚ jako správce osobních údajů již osobní údaje nepotřebuje pro účely zpracování, ale subjekt údajů je požaduje pro určení, výkon nebo obhajobu právních nároků; subjekt údajů vznesl námitku proti zpracování, dokud nebude ověřeno, zda oprávněné důvody Správce OÚ jako správce osobních údajů převažují nad oprávněnými důvody subjektu údajů.
2. Pokud bylo zpracování omezeno, mohou být tyto osobní údaje, s výjimkou jejich uložení, zpracovány pouze se souhlasem subjektu údajů, nebo z důvodu určení, výkonu nebo obhajoby právních nároků, z důvodu ochrany práv jiné fyzické nebo právnické osoby nebo z důvodů důležitého veřejného zájmu Unie nebo některého členského státu.
3. Subjekt údajů, který dosáhl omezení zpracování, musí být předem upozorněn na to, že bude omezení zpracování zrušeno.

Čl. 17
Oznamovací povinnost ohledně opravy nebo výmazu osobních údajů nebo omezení zpracování

1. Správce OÚ jako správce osobních údajů je povinen oznámit jednotlivým příjemcům, jimž byly osobní údaje zpřístupněny, veškeré provedené opravy nebo výmazy osobních údajů nebo omezení zpracování, s výjimkou případů, kdy se to ukáže jako nemožné nebo to vyžaduje nepřiměřené úsilí. Správce OÚ jako správce osobních údajů informuje subjekt údajů o těchto příjemcích, pokud tuto informaci subjekt údajů požaduje.
2. Splnění informační povinnosti podle předchozího odstavce může být zajištěno zveřejněním Informačního memoranda na webových stránkách Správce OÚ.

Čl. 18
Právo na přenositelnost údajů

1. Subjekt údajů má právo získat osobní údaje, které se ho týkají, jež poskytl Správci OÚ jako správci osobních údajů, ve strukturovaném, běžně používaném a strojově čitelném formátu, a má právo předat tyto údaje jinému správci, a to v případě, že:
   a) zpracování je založeno na uděleném souhlasu se zpracováním osobních údajů nebo na uzavřené smlouvě, a současně
   b) zpracování se provádí v elektronické podobě.
2. Subjekt údajů má právo na to, aby Správce OÚ jako správce osobních údajů osobní údaje předal přímo druhému správci, je-li to technicky proveditelné.
3. Toto právo se neuplatní na zpracování nezbytné pro splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci, kterým je Správce OÚ jako správce osobních údajů pověřeno.
4. Uplatněním práva na přenositelnost nesmí být nepříznivě dotčena práva a svobody jiných osob (údaje jiných osob musejí být anonymizovány).

Čl. 19
Právo vznést námitku

1. Subjekt údajů má z důvodů týkajících se jeho konkrétní situace právo kdykoli vznést námitku proti zpracování osobních údajů, které se jej týkají. Správce OÚ jako správce osobních údajů osobní údaje v takovém případě dále nezpracovává, pokud neprokáže závažné oprávněné důvody pro zpracování, které převažují nad zájmy nebo právy a svobodami subjektu údajů, nebo je zpracování nezbytné pro určení, výkon nebo obhajobu právních nároků.
2. Správce OÚ subjekt údajů o právu vznést námitku výslovně zřetelně a odděleně od jakýchkoli jiných informací poučí, a to nejpozději v okamžiku první komunikace se subjektem údajů.

Čl. 20
Řešení případů porušení zabezpečení osobních údajů

1. Zjištění případu porušení zabezpečení osobních údajů ohlásí zaměstnanec Správce OÚ neprodleně svému přímému nadřízenému (vedoucímu zaměstnanci) a Pověřenci pro ochranu osobních údajů.

2. Hlášení bude obsahovat alespoň tyto informace:
   a) popis povahy daného případu porušení zabezpečení osobních údajů, pokud je to možné, s uvedením kategorií a přibližného počtu dotčených subjektů údajů a kategorií a přibližného množství dotčených osobních údajů;
   b) popis pravděpodobných důsledků porušení zabezpečení osobních údajů pro Správce OÚ jako správce osobních údajů a pro subjekty údajů a jich práva;
   c) návrh okamžitých opatření k zamezení dalšímu porušení zabezpečení osobních údajů a návrh bezprostředních nápravných opatření.
3. Pověřenec pro ochranu osobních údajů ve spolupráci se Zodpovědnou osobou, Uživateli osobních údajů, Správcem, relevantními zpracovateli osobních údajů, případně dalšími relevantními zaměstnanci Správce OÚ, neprodleně rozhodne o dalším postupu.
4. Pověřenec pro ochranu osobních údajů neprodleně informuje starostu či statutárního zástupce Správce OÚ a předloží mu ke schválení návrh na řešení případu porušení zabezpečení osobních údajů a případně doporučení ohlášení porušení zabezpečení osobních údajů dozorovému úřadu.
5. Pověřenec pro ochranu osobních údajů neprodleně předloží vedoucímu pracovníku (starostovi či statutárnímu zástupci) Správce OÚ ke schválení návrh nápravných opatření pro zamezení opakování obdobného porušení zabezpečení osobních údajů. Nápravné opatření bude obsahovat kroky obnovy a postup k zamezení porušení zabezpečení a jeho opakování, termíny realizace opatření, jména zaměstnanců odpovědných za jejich splnění. Návrh nápravných opatření musí být konzultován s relevantními Zodpovědnými osobami, které ho svým podpisem potvrdí. Realizace nápravných opatření podléhá schválení vedení Správce OÚ.
6. Pověřenec pro ochranu osobních údajů provádí kontrolu plnění nápravných opatření a výsledky předkládá starostovi či statutárnímu zástupci Správce OÚ v termínech k tomu určených nápravným opatřením.

Čl. 21
Činnost při zjištění porušení zabezpečení osobních údajů

1. Jakékoli porušení zabezpečení osobních údajů nebo ztrátu dostupnosti osobních údajů (dále jen „incident"), nebo podezření takového porušení, je zaměstnanec Správce OÚ povinen hlásit Pověřenci pro ochranu osobních údajů a svému nadřízenému.
2. Podezření na incident se posuzuje pro potřeby postupu podle této směrnice stejně jako incident, dokud není zjištěno, že incident nevznikl.
3. V případě incidentu, spočívajícího ve ztrátě dostupnosti osobních údajů se ustanovení článku 19 použijí přiměřeně.
4. Pověřenec pro ochranu osobních údajů je odpovědný za řízení reakce na incident.
5. Pověřenec pro ochranu osobních údajů spolupracuje při řízení reakce na incident s vedoucími zaměstnanci Správce OÚ a pokud je to potřebné nebo nutné, se smluvními partnery Správce OÚ a s dalšími orgány veřejné správy. Spolupráce Pověřence s třetími osobami je podmíněna schválením Vedením Správce OÚ Správce OÚ.
6. Pověřenec pro ochranu osobních údajů vede dokumentaci činností a komunikace při reakci na incident tak, aby byla úplná a průkazná.
7. Úkony v reakci na incident se provádějí bez zbytečného odkladu, a pokud je to možné, okamžitě. Pokud některý z potřebných úkonů vyžaduje omezení dostupnosti informací nebo služby, informuje o tom Pověřence, a Vedení Správce OÚ.
8. Hlavními cíli reakce na incident jsou:

a) Ověřit, zda skutečně došlo k porušení zabezpečení osobních údajů.
b) Zjistit, zda došlo k neoprávněnému přístupu, zpřístupňování, přenosu nebo předávání osobních údajů, případně jinému nežádoucímu stavu nebo dopadu.
c) Zamezit možnosti neoprávněnému přístupu, zpřístupňování, přenosu nebo předávání osobních údajů.
d) Zjistit rozsah incidentu.
e) Zjistit, které osoby se mohly neoprávněně s osobními údaji seznámit.
f) Zjistit, kde se osobní údaje a informační systémy nacházejí v rozporu s obecně závaznými právními normami.
g) Opatřit důkazy pro řízení, vyšetřování nebo dokazování. Pokud je to třeba, použijí se forenzní metody a standardy.
h) Zjistit, zda je potřebné oznamovat incident třetím stranám.
i) Navrhnout a přijmout taková opatření, aby incident pominul.
j) Navrhnout a přijmout taková opatření, aby se incident neopakoval.
k) Sdílet nebo předat varování třetím osobám, zejména Úřadu, tak, aby se předešlo incidentům u dalších správců.

9. Činnost podle tohoto článku bude ukončena, jestliže o tom rozhodne Pověřenec na základě předložené zprávy a zabezpečených podkladů a informací, nebo pokud se prokáže, že k incidentu nedošlo.

Čl. 22
Ohlašování případů porušení zabezpečení osobních údajů dozorovému úřadu

1. Jakékoli porušení zabezpečení osobních údajů Správce OÚ jako správce osobních údajů prostřednictvím Pověřence bez zbytečného odkladu nejpozději do 72 hodin od okamžiku, kdy se o něm dozvěděl, ohlásí dozorovému úřadu, ledaže je nepravděpodobné, že by toto porušení mělo za následek riziko pro práva a svobody fyzických osob. Pokud není ohlášení dozorovému úřadu učiněno do 72 hodin, musí být současně s ním uvedeny důvody tohoto zpoždění.
2. Jakmile zpracovatel zjistí porušení zabezpečení osobních údajů, ohlásí je bez zbytečného odkladu Správci OÚ jako správci osobních údajů.
3. Ohlášení případů porušení zabezpečení osobních údajů musí přinejmenším obsahovat:
   a) popis povahy daného případu porušení zabezpečení osobních údajů včetně, pokud je to možné, kategorií a přibližného počtu dotčených subjektů údajů a kategorií a přibližného množství dotčených záznamů osobních údajů;
   b) jméno a kontaktní údaje Pověřence nebo jiného kontaktního místa, které může poskytnout bližší informace;
   c) popis pravděpodobných důsledků porušení zabezpečení osobních údajů;
   d) popis opatření, která Správce OÚ přijal nebo navrhl k přijetí s cílem vyřešit dané porušení zabezpečení osobních údajů, včetně případných opatření ke zmírnění možných nepříznivých dopadů.
4. Není-li možné poskytnout informace současně, mohou být poskytnuty postupně bez dalšího zbytečného odkladu. Pověřenec dokumentuje veškeré případy porušení zabezpečení osobních údajů, přičemž uvede skutečnosti, které se týkají daného porušení, jeho účinky a přijatá nápravná opatření. Tato dokumentace musí dozorovému úřadu umožnit ověření souladu s tímto ustanovením směrnice.

Čl. 23
Oznamování případů porušení zabezpečení osobních údajů subjektu údajů

1. Pokud je pravděpodobné, že případ porušení zabezpečení osobních údajů bude mít za následek vysoké riziko pro práva a svobody fyzických osob, oznámí Správce OÚ jako správce osobních údajů prostřednictvím Pověřence toto porušení bez zbytečného odkladu subjektu údajů.
2. V oznámení subjektu údajů se za použití jasných a jednoduchých jazykových prostředků popíše povaha porušení zabezpečení osobních údajů a uvedou se v něm přinejmenším informace a opatření uvedené v čl. 19 této směrnice.
3. Oznámení subjektu údajů se nevyžaduje, je-li splněna kterákoli z těchto podmínek:
   a) Správce OÚ jako správce osobních údajů zavedl náležitá technická a organizační ochranná opatření a tato opatření byla použita u osobních údajů dotčených porušením zabezpečení osobních údajů, a to zejména taková opatření, která činí tyto údaje nesrozumitelnými pro kohokoli, kdo není oprávněn k nim mít přístup (kupř. šifrování);
   b) Správce OÚ jako správce osobních údajů přijal následná opatření, která zajistí, že vysoké riziko pro práva a svobody subjektů údajů se již s vysokou pravděpodobností neprojeví;
   c) Oznámení by vyžadovalo nepřiměřené úsilí. V takovém případě musí být subjekty údajů informovány stejně účinným způsobem pomocí veřejného oznámení nebo jiného podobného opatření.
4. Jestliže Správce OÚ jako správce osobních údajů dotčenému subjektu údajů porušení zabezpečení osobních údajů ještě neoznámilo, je dozorový úřad oprávněn, požadovat, aby oznámení bylo provedeno.

Čl. 24
Zpracovatel

1. Pokud má být zpracování provedeno pro Správce OÚ jako pro správce osobních údajů, využije Správce OÚ pouze ty zpracovatele, kteří poskytují dostatečné záruky, že zavedou dostatečná technická a organizační opatření, jež zajistí, že zpracování bude splňovat požadavky Nařízení GDPR a této směrnice a že byla zajištěna ochrana práv subjektu údajů.
2. Zpracovatel není oprávněn zapojit do zpracování žádného dalšího zpracovatele bez předchozího písemného povolení Správce OÚ jako správce osobních údajů, k čemuž bude Správcem OÚ zavázán. Zpracovatel informuje předem Správce OÚ jako správce osobních údajů o zapojení dalších zpracovatelů nebo o nahrazení a změnách zpracovatelů, a poskytne tak Správci OÚ jako správci osobních údajů příležitost vyslovit vůči těmto změnám námitky a souhlas se zapojením dalšího zpracovatele neudělit.
3. Správce OÚ uzavře se zpracovatelem písemnou smlouvu, která stanoví práva a povinnosti zpracovatele při zpracování. Zodpovědná osoba je povinna zajistit, aby s každým zpracovatelem byla před zahájením zpracování uzavřena Smlouva o zpracování osobních údajů, která zavazuje zpracovatele vůči Správci OÚ jako správci osobních údajů a v níž je stanoven předmět a doba trvání zpracování, povaha a účel zpracování, typ osobních údajů a kategorie subjektů údajů, povinnosti a práva správce. Vzor Smlouvy o zpracování osobních údajů je umístěn u DPO.

Čl. 25
Kontrola dodržování ustanovení směrnice

1. Vedení Správce OÚ společně s vedoucími organizačních jednotek Správce OÚ a se zodpovědnými osobami zajistí kontrolu plnění povinností vyplývajících z ustanovení této směrnice pro nakládání s osobními údaji v mezích své působnosti.
2. Vedoucí pracovníci Správce OÚ zajistí, aby byli s dokumentem směrnice pro nakládání s osobními údaji seznámeni všichni zaměstnanci Správce OÚ včetně proškolení a ověření znalostí směrnice a povinností na úseku ochrany osobních údajů.
3. Pověřenec odpovídá za pravidelné testování, posuzování a hodnocení účinnosti zavedených organizačních, fyzických a technických opatření pro zajištění bezpečnosti zpracování dle směrnice o nakládání s osobními údaji Správce OÚ. Při provádění kontrolních činností jsou všichni zaměstnanci Správce OÚ povinni poskytovat Pověřenci součinnost. O provedených zjištěních vede Pověřenec pro ochranu osobních údajů prokazatelnou dokumentaci, kterou předkládá na vědomí starostovi či statutárnímu zástupci Správce OÚ.
4. Pověřenec předkládá doporučení ke změnám organizačních, fyzických a technických opatření pro zajištění bezpečnosti zpracování osobních údajů starostovi či statutárnímu zástupci Správce OÚ ke schválení vždy, když je takových změn zapotřebí.

Čl. 26
Revize směrnice

1. Správce OÚ provede revizi této směrnice pro nakládání s osobními údaji v případě potřeby, nejméně však jednou za dva roky a vždy, když revizi této směrnice navrhne Pověřenec.
2. Za zpracování, prosazení, údržbu a revize směrnice pro nakládání s osobními údaji odpovídá vedoucí Odboru vnitřních věcí Správce OÚ.

Čl. 27
Závěrečná ustanovení

1. Touto směrnicí jsou povinni řídit se všichni zaměstnanci Správce OÚ a všechny další osoby, které nakládají s osobními údaji, které jsou ve správě Správce OÚ, či je jinak zpracovávají.
2. Tato směrnice nabývá platnosti a účinnosti dnem 01. 07. 2018.

V Příbrami dne .....

.....	.....
Ing. Jindřich Vařeka	Ing. Jaroslava Poláková
starosta	tajemnice

Vydáno dne .....
[datum distribuce předpisu OVV]

Schvalovací doložka

k vnitřnímu předpisu města Příbram č. .... /2018/MěÚ, ...

Zpracoval:

Mgr. Jan Šmejkal,
doc. Ing. Josef Kokeš, CSc.

Schválil:

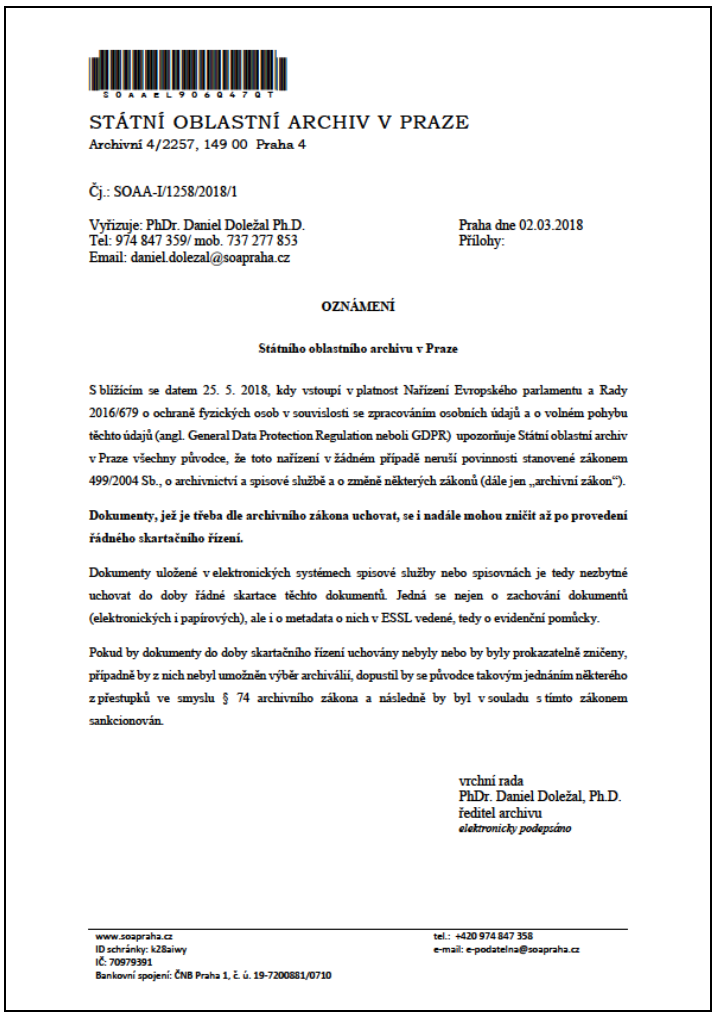
[dotčený odborný útvar]

9. SPISOVÝ A SKARTAČNÍ ŘÁD

9.1 Stanovisko SOA

V rámci analýzy činností zpracování osobních údajů byla řešena otázka aktualizace Spisového a skartačního řádu Správce OÚ, s cílem zajistit soulad s požadavky GDPR.

Bylo vyžádáno stanovisko Státního oblastního archivu, který je v této věci nadřízeným orgánem. Obdržené stanovisko je přiloženo:



SOAAEL90647QT

STÁTNÍ OBLASTNÍ ARCHIV V PRAZE
Archivní 4/2257, 149 00 Praha 4

Čj.: SOAA-I/1258/2018/1

Vyřizuje: PhDr. Daniel Doležal Ph.D.
Tel: 974 847 359/ mob. 737 277 853
Email: daniel.dolezal@soapraha.cz

Praha dne 02.03.2018
Přílohy:

OZNÁMENÍ

Státního oblastního archivu v Praze

S blížícím se datem 25. 5. 2018, kdy vstoupí v platnost Nařízení Evropského parlamentu a Rady 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů (angl. General Data Protection Regulation neboli GDPR) upozorňuje Státní oblastní archiv v Praze všechny původce, že toto nařízení v žádném případě neruší povinnosti stanovené zákonem 499/2004 Sb., o archivnictví a spisové službě a o změně některých zákonů (dále jen „archivní zákon").

Dokumenty, jež je třeba dle archivního zákona uchovat, se i nadále mohou zničit až po provedení řádného skartačního řízení.

Dokumenty uložené v elektronických systémech spisové služby nebo spisovnách je tedy nezbytné uchovat do doby řádné skartace těchto dokumentů. Jedná se nejen o zachování dokumentů (elektronických i papírových), ale i o metadata o nich v ESSL vedené, tedy o evidenční pomůcky.

Pokud by dokumenty do doby skartačního řízení uchovány nebyly nebo by byly prokazatelně zničeny, případně by z nich nebyl umožněn výběr archiválií, dopustil by se původce takovým jednáním některého z přestupků ve smyslu § 74 archivního zákona a následně by byl v souladu s tímto zákonem sankcionován.

vrchní rada
PhDr. Daniel Doležal, Ph.D.
ředitel archivu
elektronicky podepsáno

www.soapraha.cz
ID schránky: k28aiwy
IČ: 70979391
Bankovní spojení: ČNB Praha 1, č. ú. 19-7200881/0710

tel.: +420 974 847 358
e-mail: e-podatelna@soapraha.cz

Vyplývá z něj, že v souvislosti s GDPR není obecně třeba arch. a spisový řád, ani skartační plán Správce OÚ měnit, jen podle GDPR nebude lze ponechat ve spisech ty dokumenty u kterých už podle arch. a spis. řádu mělo proběhnout skartační řízení.

Závěr: Spisový a skartační řád, ani skartační plán, se měnit nutně nemusí pouze kvůli GDPR.

Spisový a skartační řád

vzor

9.2.1 Úvodní ustanovení

Spisový a skartační řád je souhrn předpisů pro vedení spisové služby. Cílem spisového a skartačního řádu je sjednotit manipulaci s dokumenty, vzniklými nebo vyřízenými v xxxxxxxxxxx. Součástí spisového a skartačního řádu je spisový a skartační plán.

Spisový a skartační řád je závazný pro všechny pracovníky xxxxxxxxxxx.

9.2.2 Všeobecná ustanovení

Spisová služba je soubor pravidel a opatření spojených s příjmem, tříděním, zapisováním, oběhem, vyřizováním, vyhotovováním, podepisováním, odesíláním, ukládáním a vyřazováním (skartací) dokumentů.

Spisová služba se řídí:

- zákonem č. 499/2004 Sb., o archivnictví a spisové službě a změně některých zákonů, ve znění pozdějších předpisů, v oblasti výkonu spisové služby a archivnictví dle § 63 odst. 1 písm. d) zákona,
- zákonem č. 563/1991 Sb., o účetnictví v platném znění,
- zákonem č. 582/1991 Sb. o organizaci a provádění sociálního zabezpečení § 35 a odst. 4
- zákonem o volbách č.491/2001 Sb. a vyhláškou č. 59/2002 Sb.

9.2.3 Základní pojmy

Dokument – je každý písemný, obrazový, zvukový, elektronický nebo jiný záznam, ať již v podobě analogové či digitální, který vznikl z činnosti původce.

Podací deník – základní evidenční pomůcka spisové služby, do něhož jsou zapisována v číselném a časovém pořadí podání.

Podání – dokument došlý organizaci nebo v ní vzniklý, návrhy a jiná sdělení včetně vlastního úředního záznamu, který se stává předmětem úředního jednání.

Podatelna – místo, v němž se evidují podání – kancelář obecního úřadu.

Původce – každý, z jehož činnosti dokument vznikl.

Spis – dokument nebo soubor dokumentů vzniklých při úředním jednání k jedné věci.

Spisové znaky – označují jednotlivé skupiny dokumentů podle jejich obsahu.

Skartační znak – vyjadřuje hodnotu dokumentu podle obsahu a označuje způsob, jakým se s dokumentem naloží ve skartačním řízení:

- **znak A** (archiv) – označuje dokument trvalé hodnoty, který bude ve skartačním řízení vybrán jako archiválie k trvalému uložení do archivu,
- **znak S** (stoupa) – označuje dokument bez trvalé hodnoty, jenž bude ve skartačním řízení navržen ke zničení,
- **znak V** (výběr) – označuje dokument bez trvalé hodnoty, jenž bude ve skartačním řízení posouzen a rozdělen mezi dokumenty se skartačním znakem Anebo mezi dokumenty se skartačním znakem S.

Skartační lhůta je doba, po kterou dokument zůstává uložen v organizaci. Tato lhůta je závazná a nelze ji zkracovat.

Spisový plán je schéma pro označování a ukládání vyřízených a vyhotovených dokumentů.

Skartační plán je rozpis věcných druhů dokumentů organizace, doplněný o skartační znaky a lhůty.

Ukládací archiv – archiv, do kterého jsou ukládány archiválie organizace.

9.2.4 Spisový řád

Upravuje úkony spojené s příjmem a tříděním došlých dokumentů se zapisováním došlých dokumentů, s oběhem, vyřizováním, vyhotovováním, podepisováním, odesíláním a ukládáním dokumentů.

9.2.4.1 Příjem dokumentů

Doručené dokumenty se přijímají v místě k tomu určeném – xxxxxxxxxxxxxx (podatelna), popřípadě doručovací adresa dohodnutá s Českou poštou – adresa pracovníka pověřeného k vedení podacího deníku.

Příjem datových zpráv se řídí zvláštním právním předpisem. V podatelně se přijímají veškeré doručené dokumenty bez ohledu na druh odesílatele nebo místo odeslání. Dokument v digitální podobě se považuje za doručený tehdy, je-li dostupný v elektronické podatelně.

Za doručený dokument se považuje také takový dokument, který byl předán osobně mimo podatelnu (kancelář obecního úřadu) nebo byl pořízen záznam o podání učiněném telefonicky nebo ústně. Zaměstnanec, který dokument takto převzal nebo pořídil záznam je povinen zabezpečit jeho neprodlené předání podatelně k evidenci.

Došlý dokument se opatří v den doručení otiskem podacího razítka a po jeho zaevidování se předá k vyřízení. Pokud je dokument doručen v digitální podobě, opatří se identifikátorem elektronické podatelny a předá se k vyřízení.

9.2.4.2 Evidence dokumentů

Všechny dokumenty podléhající evidenci, jsou evidovány v podacím deníku v elektronické spisové službě.

Podací deník je kniha vytvořená přetištěním z elektronické podoby podacího deníku. Do podacího deníku jsou dokumenty zapisovány v pořadí, v němž byly organizaci doručeny. Číselná řada v podacím deníku začíná dnem 1. ledna pořadovým číslem 1 a končí dnem 31. prosince. Každý doručený dokument má své číslo jednací.

9.2.4.3 Rozdělování a oběh dokumentů

Zaevidovaný dokument se předává příslušnému zaměstnanci určenému k vyřízení. Při oběhu dokumentu musí být zabezpečeno sledování jeho předávání a přebírání.

9.2.4.4 Vyřizování dokumentů

Vyřízení doručeného dokumentu je prováděno v listinné podobě nebo elektronicky věcně, stručně a srozumitelně, způsob vyřízení a navrhovaná opatření musí být řádně zdůvodněna. Pokud je dokument vyřizován jinak než v listinné podobě, učiní o tom zaměstnanec záznam. Kopii vyřízení připojuje k vyřízenému dokumentu. Dokumenty, které spolu souvisejí nebo se týkají projednání jedné věci, se spojují a vytvářejí spis. Na dokumenty, na něž se nezpracovává odpověď, se vyznačí poznámka „Vzato na vědomí“, rovněž tak v podacím deníku.

9.2.4.5 Vyhotovování dokumentů

Dokumenty vzniklé z činnosti xxxxxxxxxxxxxxxxxxxxxxx, se označují záhlavím s jeho názvem a sídlem a číslem jednacím. Dalšími náležitostmi dokumentu jsou: datum, přílohy, jméno, příjmení a funkce zaměstnance pověřeného jeho podpisem.

9.2.4.6 Podepisování dokumentu a používání razítek

Dokumenty vzniklé z úřední činnosti podepisuje starosta nebo místostarosta a jsou opatřeny razítkem se státním znakem o průměru 32 mm s textem Obecní úřad xxxxxxxxxxx.

Dokumenty podepisuje statutární zástupce a jsou opatřeny razítkem xxxxxxxxxxx.

9.2.4.7 Odesílání dokumentů

Odesílání dokumentů v listinné podobě poštou nebo elektronicky e-mailem nebo datovou schránkou zajišťuje pověřený zaměstnanec obecního úřadu.

9.2.4.8 Ukládání dokumentů

Ukládacím místem pro vyřízené, ale stále ještě provozně užívané dokumenty včetně kopií, je spisovna. Za řádné uložení spisů, správné označení a zabezpečení dokumentů zodpovídá vedoucí. Dokumenty jsou podle věcného obsahu ukládány do složek. Takto vybavené složky se ukládají do šanonů, na kterých je uveden rok vzniku a nápis, co obsahují.

9.2.5 Skartační řád

Upravuje způsob a průběh skartačního řízení.

9.2.5.1 Předmět skartačního řízení

Dokumenty jsou uloženy ve spisovně obecního úřadu po dobu stanovenou skartační lhůtou, uvedenou ve skartačním plánu. Ta začíná běžet dnem 1. ledna roku následujícího po vyřízení nebo vyhotovení dokumentu. Skartační řízení bude obec provádět průběžně podle skartační lhůty. Skartační řízení je spojeno s výběrem archiválií.

9.2.5.2 Průběh skartačního řízení

K provedení skartačního řízení ustaví obec skartační komisi, jejímž členem je vždy starosta. Ten v rámci skartačního řízení označí v předávacích protokolech položky, kterým uplynula skartační lhůta. Takto zpracovaný seznam dokumentů zn. S, doplněný seznamem dokumentů zn. A s žádostí o schválení

skartace, podepsanou starostou obce, tvoří skartační návrh. Ten bude zaslán Státnímu okresnímu archivu v xxxxxxxxxxxxxxxxxxxxxxxxxxxx.

Na základě skartačního návrhu provede zaměstnanec archivu odbornou archivní prohlídku dokumentů navrhovaných k vyřazení. Archivář posoudí, zda jsou dokumenty správně označeny a uloží skartační komisi sepsat seznam dokumentů určených k uložení v archivu a seznam dokumentů k vyřazení a ke zničení a zároveň dohodne se skartační komisí dobu a způsob předání dokumentů k uložení do archivu. O provedeném skartačním řízení vyhotoví archivář protokol a do jeho přílohy zařadí komisí vypracovaný soupis dokumentů vybraných za archiválie a soupis dokumentů, které lze skartovat.

9.2.5.3 Pravomoc státního archivu

Pověřený státní archiv, kterým je Státní okresní archiv v xxxxxxxxxxxxxxxx, posuzuje a rozhoduje, které dokumenty převezme protokolárně do své péče a které schválí ke zničení.

9.2.6 Závěrečná ustanovení

Tento spisový a skartační řád byl posouzen Státním okresním archivem v xxxxxxxxxxxxx dne 000000000000 a doporučen ke schválení.

Tento Spisový a skartační řád byl schválen xxxxxxxxxxxxxxx dne xxxxxxxxxxxx a nabývá účinnosti dnem xxxxxxxxxxxx.

10. VZOR SMLOUVA O ZPRACOVÁNÍ

Jsou předloženy dvě varianty smlouvy o zpracování OÚ podle GDPR k podkladové smlouvě, a to:

- už je uzavřena smlouva činnostní (podkladová), která už běží a ještě před účinností GDPR se uzavírá zpracovatelská smlouva s ohledem na účinnost, zpracovatel nemá podzpracovatele (a je tu smluvní mechanizmus, podle kterého může být podzpracovatel schválen v budoucnu)
- už je uzavřena smlouva činnostní (podkladová), která už běží a ještě před účinností GDPR se uzavírá zpracovatelská smlouva s ohledem na účinnost, zpracovatel má podzpracovatele
- po účinnosti GDPR se bude uzavírat činnostní (podkladová) smlouva a k ní tato zpracovatelská

10.1 Varianta bez podzpracování (obvyklejší)

SMLOUVA O ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ

podle čl. 28 Obecného nařízení o ochraně osobních údajů[12]

(„**Smlouva**“)

[*zde doplnit právnickou osobu, která je stranou smlouvy*], dále jen

(„**Správce OÚ**“),

zastoupená panem [*doplnit*]

a

společnost [*doplnit obchodní firmu*]

se sídlem [*doplnit*], IČO: [*doplnit*], zapsaná v obchodním rejstříku vedeném *Městským / Krajským* soudem v [*doplnit*], sp. zn. [*doplnit*] („**Dodavatel**“),

zastoupená [*doplnit jméno, příjmení a funkci*] a [*doplnit jméno, příjmení a funkci*],

(Správce OÚ a Dodavatel dále společně jako „**Smluvní strany**“)

se níže uvedeného dne, měsíce a roku dohodli na následujícím:

[12] Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES („**Obecné nařízení**“/“**GDPR**“).

PREAMBULE

Vzhledem k tomu, že:

I. Smluvní strany spolu dne [*doplnit*] uzavřely smlouvu [*doplnit název*] číslo [*doplnit číslo smlouvy*] („**Podkladová smlouva**“) a v rámci plnění této smlouvy Dodavatel zpracovává osobní údaje, jichž je Správce OÚ správcem nebo zpracovatelem, jak je blíže specifikováno níže,

II. Ke dni 25. května 2018 vstoupí v účinnost Obecné nařízení upravující mj. povinnosti správců a zpracovatelů osobních údajů v souvislosti s jejich zpracováním,

III. Smluvní strany mají zájem pokračovat i po 25. květnu 2018 ve vzájemné spolupráci na základě Podkladové smlouvy a dodržovat při ní veškeré legislativní požadavky,

uzavírají spolu Smluvní strany tuto Smlouvu:

I. POSTAVENÍ SMLUVNÍCH STRAN PŘI ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ V SOUVISLOSTI S PODKLADOVOU SMLOUVOU

1.1 Správce OÚ je správcem osobních údajů *zájemců/klientů/občanů obce ve vztahu k produktům/službám Dodavatele* a Dodavatel je ve vztahu k těmto údajům v postavení zpracovatele osobních údajů.

II. PŘEDMĚT a DOBA ZPRACOVÁNÍ

2.1 Dodavatel bude na základě této Smlouvy pro Správce OÚ zpracovávat následující osobní údaje: [*doplnit* kupř. jméno, příjmení adresa bydliště, emailová adresa telefon,…….]

2.2 Dodavatel je oprávněn osobní údaje na základě této Smlouvy zpracovávat *po dobu trvání Podkladové smlouvy*.

III. POVAHA a ÚČEL ZPRACOVÁNÍ

3.1 Dodavatel je na základě této Smlouvy oprávněn osobní údaje zpracovávat pro *účel/y* [*doplnit podle údajů v podkladové smlouvě*].

3.2 Zpracování osobních údajů bude spočívat v jejich:

- sběru,
- zaznamenávání,
- strukturalizaci,
- modifikaci,
- uchovávání,
- extrakci,
- srovnávání,
- likvidaci,
- [*případně doplnit jinou činnost*].

IV. TYP OSOBNÍCH ÚDAJŮ a KATEGORIE SUBJEKTŮ ÚDAJŮ

4.1 Dodavatel na základě této Smlouvy pro Správce OÚ zpracovává osobní údaje následujících kategorií subjektů údajů:

(i) [*doplnit, kupř. zaměstnanci Správce OÚ*];
(ii) *občané*
(iii) [*doplnit osoby vstupující do budov Správce OÚ*]
(iv) [*určit podle podkladové smlouvy*].

4.2 Dodavatel na základě této Smlouvy pro Správce OÚ zpracovává následující typy osobních údajů: [*osobní údaje ve smyslu čl. 4 odst. 1 Obecného nařízení / zvláštní kategorie osobních údajů ve smyslu čl. 9 odst. 1 Obecného nařízení / osobní údaje týkající se rozsudků v trestních věcech a trestných činů.*]

V. POVINNOSTI DODAVATELE a SPRÁVCE OÚ

Dodavatel se zavazuje:

5.1 Zpracovávat osobní údaje pouze za účelem definovaným v této Smlouvě, přičemž se výslovně zavazuje, že v žádném případě je nebude zpracovávat pro vlastní účely.

5.2 Zpracovávat osobní údaje pouze v souladu s doloženými pokyny Správce OÚ, včetně předání osobních údajů do třetí země nebo mezinárodní organizaci.

Sjednává se, že pokud Dodavatel dojde k závěru, že některý z pokynů Správce OÚ je v rozporu s Obecným nařízením nebo s jakýmkoli jiným právním předpisem v oblasti ochrany osobních údajů, je povinen Správce OÚ na tuto skutečnost neprodleně písemně upozornit.

Pokud Dodavateli určité zpracování ukládá právo Evropské unie nebo členského státu, které se vztahuje na Dodavatele, je Dodavatel povinen Správce OÚ o tomto právním požadavku písemně informovat před zahájením takového zpracování, ledaže by tyto právní předpisy toto informování zakazovaly z důležitých důvodů veřejného zájmu.

5.3 Vést, písemně (včetně elektronické formy), záznamy o zpracování osobních údajů v souladu s čl. 30 odst. 2 Obecného nařízení, obsahující:

a) [*jméno/obchodní firmu*] a kontaktní údaje Dodavatele a každého správce, pro kterého jedná a případného zástupce správce nebo Dodavatele a pověřence pro ochranu osobních údajů;

b) Kategorie zpracování prováděného pro každého ze správců;

c) Informace o případném předání osobních údajů do třetí země nebo mezinárodní organizaci, včetně identifikace této třetí země či mezinárodní organizace a v případě podle čl. 49 odst. 1 druhého pododstavce Obecného nařízení doložení vhodných záruk;

d) Je-li to možné, obecný popis technických a organizačních bezpečnostních opatření uvedených v čl. 32 odst. 1 Obecného nařízení.

5.4 Nesdělovat osobní údaje třetím osobám, s výjimkou případů, kdy Dodavatel bude mít k tomu předem výslovný pokyn Správce OÚ.

Dodavatel je oprávněn, na základě písemného pokynu Správce OÚ, sdělovat osobní údaje jiným zpracovatelům pověřeným Správcem OÚ. Pokyn Správce OÚ musí obsahovat jasnou identifikaci zpracovatele, rozsah osobních údajů, které mají být předány a prostředky pro zajištění zabezpečení předání osobních údajů.

5.5 Nepověřovat zpracováním osobních údajů na základě této Smlouvy další osoby (dále společně jako „**Další zpracovatel**“).

V případě, že by Dodavatel zamýšlel do zpracování osobních údajů na základě této Smlouvy zapojit Další zpracovatele, je o tom povinen Správce OÚ písemně informovat alespoň 30 pracovních dní před zahájením zamýšlené spolupráce s Dalším zpracovatelem a Správci OÚ sdělit zejména, kterými činnostmi zpracování osobních údajů zamýšlí Dalšího zpracovatele pověřit a identifikační a kontaktní údaje Dalšího zpracovatele a případně další informace či návrh smlouvy, bude-li to Správce OÚ považovat za potřebné k posouzení navrhované spolupráce mezi Dodavatelem a Dalším zpracovatelem. Smlouvu s Dalším zpracovatelem smí Dodavatel uzavřít pouze v případě, že mu Správce OÚ ve lhůtě 14 kalendářních dní od obdržení informace nesdělí nesouhlasnou námitku.

Dodavatel je povinen smluvně zavázat Dalšího zpracovatele k povinnosti plnit Dodavatelovy povinnosti dle této Smlouvy a případné další pokyny Správce OÚ v oblasti ochrany osobních údajů.

Neplní-li Další zpracovatel své povinnosti v oblasti ochrany osobních údajů, odpovídá Správci OÚ za plnění povinností daného Dalšího zpracovatele i nadále Dodavatel.

Dodavatel je rovněž povinen oznámit Správci OÚ ukončení spolupráce s kterýmkoli z Dalších zpracovatelů, a to nejpozději do 3 dnů od ukončení spolupráce.

Nejpozději do 20. května 2018 poskytne Dodavatel Správci OÚ ke schválení vyplněný seznam Dalších zpracovatelů, jehož vzor tvoří přílohu č. 1 této Smlouvy, kteří jsou již zapojeni do zpracování osobních údajů v souvislosti s Podkladovou smlouvou, včetně údajů o dalších zpracovatelích, se kterými případně spolupracují Další zpracovatelé, a to elektronicky na adresu [*doplnit*]. V případě, že od okamžiku poskytnutí tohoto seznamu do 25. května 2018 dojde ke změně v poskytnutých údajích, zavazuje se Dodavatel Správci OÚ bez zbytečného odkladu stejným způsobem zaslat aktualizovaný seznam.

5.6 Udržovat mlčenlivost o zpracovávaných osobních údajích, ke kterým má přístup v souvislosti s Podkladovou smlouvu, resp. touto Smlouvou, a to včetně období po skončení této Smlouvy.

5.7 Zajistit, že jeho pracovníci nakládající s osobními údaji se písemně výslovně zaváží k dodržování mlčenlivosti ohledně zpracovávaných osobních údajů, dodržování stanovených bezpečnostních opatření a podmínek pro zpracování osobních údajů dle této Smlouvy.

5.8 Zajistit kontinuální odpovídající proškolování svých pracovníků nakládajících s osobními údaji v oblasti ochrany osobních údajů.

5.9 Oznámit Správci OÚ jakoukoli změnu zpracovávaných osobních údajů.

5.10 Poskytnout Správci OÚ veškerou součinnost, kterou bude potřebovat pro uskutečnění výkonu práva subjektu údajů:

a) na přístup k osobním údajům, opravu osobních údajů, výmaz osobních údajů, námitku proti zpracování osobních údajů;

b) na omezení zpracování osobních údajů;

c) na přenositelnost osobních údajů;

d) nebýt předmětem automatizovaného rozhodování ve smyslu čl. 22 odst. 1 Obecného nařízení.

Dodavatel je povinen pokynům Správce OÚ v souvislosti s výkonem výše popsaných práv subjektů osobních údajů vyhovět ve lhůtě stanovené Správcem OÚ ve vztahu ke každé individuální žádosti.

V případě, že by subjekt osobních údajů uplatnil některé z výše uvedených práv ve vztahu k Dodavatelem pro Správce OÚ zpracovávaným osobním údajům přímo u Dodavatele a nikoli u Správce OÚ, zavazuje se Dodavatel takovou žádost Správci OÚ zaslat prostřednictvím e-

mailu na adresu [*Doplnit adresu kontaktní osoby Správce OÚ případně též DPO*] a to bez zbytečného odkladu, nejpozději však do 24 hodin od jejího převzetí.

5.11 Pokud je to vzhledem k činnosti Dodavatele vykonávané pro Správce OÚ relevantní, poskytnout subjektům osobních údajů, v souladu s příslušnými ustanoveními Všeobecných podmínek daného produktu, v okamžiku získání osobních údajů, informace Správce OÚ

5.12 o zpracování osobních údajů, a to vždy aktuální a ve formátu stanoveném Správcem OÚ.

5.13 Jakmile zjistí porušení zabezpečení osobních údajů (dále jen „bezpečnostní incident“), ohlásit jej neprodleně, nejpozději však do 24 hodin Správci OÚ a poskytnout mu veškerou součinnost a veškeré informace, které Správce OÚ může potřebovat ke splnění svých zákonných povinností, zejména, nikoli však výlučně:

a) Popis povahy daného případu bezpečnostního incidentu včetně, pokud je to možné, kategorií a přibližného počtu dotčených subjektů údajů a kategorií a přibližného množství dotčených záznamů osobních údajů;

b) Jméno a kontaktní údaje pověřence pro ochranu osobních údajů nebo jiného kontaktního místa, které může poskytnout bližší informace;

c) Popis pravděpodobných důsledků bezpečnostního incidentu;

d) Popis opatření, která Dodavatel přijal nebo navrhuje k přijetí s cílem vyřešit daný bezpečnostní incident, včetně případných opatření ke zmírnění možných nepříznivých dopadů.

Pokud není možné poskytnout Správci OÚ informace podle písm. a) až d) výše současně, mohou být poskytnuty postupně bez dalšího zbytečného odkladu.

Kontaktní osobou pro oznámení bezpečnostních incidentů Správci OÚ a další související komunikaci, nebude-li Správcem OÚ určeno jinak, je: [*doplnit jméno a příjmení*], e-mail [*doplnit*], telefon [*doplnit*]/ pověřenec ochranou osobních údajů Správce OÚ.

Výše uvedené povinnosti Dodavatele se uplatí obdobně, pokud k bezpečnostnímu incidentu dojde u Dalšího zpracovatele nebo dalšího zpracovatele spolupracujícího s Dalším zpracovatelem.

5.14 Poskytnout Správci OÚ veškerou součinnost, která může být pro Správce OÚ nezbytná pro vypracování posouzení vlivu na ochranu osobních údajů ve smyslu čl. 35 Obecného nařízení.

5.15 Poskytnout Správci OÚ veškerou potřebnou součinnost, která může být nezbytná pro uskutečnění předchozích konzultací ve smyslu čl. 36 Obecného nařízení s Úřadem pro ochranu osobních údajů.

5.16 Poskytnout Správci OÚ veškeré informace, které mohou být pro Správce OÚ nezbytné k prokázání plnění svých povinností v roli správce či zpracovatele osobních údajů nebo pro účely jakýchkoli auditů v oblasti ochrany osobních údajů.

5.17 Umožnit Správci OÚ audity ochrany osobních údajů, včetně inspekcí, prováděných Správcem OÚ či jím pověřeným auditorem u Dodavatele, a v rámci těchto auditů a/nebo inspekcí poskytnout Správci OÚ či pověřenému auditorovi veškerou potřebnou součinnost.

5.18 Zavést v souladu s analýzou rizik provedenou [*doplnit*] dne [*doplnit*] alespoň tato následující opatření pro zabezpečení osobních údajů:

a) [*doplnit*];

b) [*doplnit*].

Zavedením výše uvedených opatření se Dodavatel nezbavuje své odpovědnosti zajistit ve vztahu k osobním údajům zpracovávaným na základě této Smlouvy úroveň zabezpečení odpovídající danému riziku. Dodavatel je v každém případě povinen v souladu s čl. 32 Obecného nařízení s přihlédnutím ke stavu techniky, nákladům na provedení, povaze, rozsahu, kontextu a účelům zpracování i k různě pravděpodobným a různě závažným rizikům pro práva a svobody fyzických osob, provést vhodná technická a organizační opatření, aby zajistil úroveň zabezpečení odpovídající danému riziku, případně včetně:

a) Pseudonymizace a šifrování osobních údajů;

b) Schopnosti zajistit neustálou důvěrnost, integritu, dostupnost a odolnost systémů a služeb zpracování;

c) Schopnosti obnovit dostupnost osobních údajů a přístup k nim včas v případě fyzických či technických incidentů;

d) Procesu pravidelného testování, posuzování a hodnocení účinnosti zavedených technických a organizačních opatření pro zajištění bezpečnosti zpracování;

a tato opatření průběžně vyhodnocovat a případně odpovídajícím způsobem upravovat.

5.19 V případě, že je k tomu dle Obecného nařízení povinen, jmenovat pověřence pro ochranu osobních údajů a sdělit Správci OÚ jeho jméno, příjmení a kontaktní údaje.

5.20 Po skončení této Smlouvy vrátit Správci OÚ všechny osobní údaje, včetně, pokud je to relevantní, nosičů, na nichž jsou uloženy a současně tyto osobní údaje vymazat ze všech elektronických zařízení či databází používaných Dodavatelem. / Po skončení této Smlouvy předat osobní údaje zpracovateli určenému Správcem OÚ včetně, pokud je to relevantní, nosičů, na nichž jsou uloženy a současně tyto osobní údaje vymazat ze všech elektronických zařízení či databází používaných Dodavatelem. / Po skončení této Smlouvy osobní údaje do *10 pracovních dnů* zlikvidovat a Správci OÚ do *2 pracovních dnů* od jejich likvidace zaslat písemný protokol o jejich likvidaci.

5.21 Uzavřít a po dobu trvání této Smlouvy udržovat v platnosti pojistnou smlouvu kryjící odpovědnost za případnou újmu, kterou by mohl v souvislosti s výkonem činnosti podle této Smlouvy Správci OÚ způsobit, a to do výše minimálně [*Nutno doplnit s ohledem na rizika u každého dodavatele přiměřeně podle rizik pro práva subjektů OÚ*]. Kopii pojistné smlouvy je Dodavatel Správci OÚ povinen kdykoli na požádání předložit, a to nejpozději do 3 pracovních dnů ode dne výzvy Správce OÚ k jejímu předložení.

5.22 V případě, že Dodavatel bude mít v souvislosti se zpracováním osobních údajů na základě této Smlouvy potřebu konzultace se Správcem OÚ, zavazuje se Správce OÚ poskytnout mu potřebnou součinnost.

5.23 Správce OÚ se zavazuje pro případ, že dle Obecného nařízení jmenuje pověřence pro ochranu osobních údajů sdělit Dodavateli jeho jméno, příjmení a kontaktní údaje do tří pracovních dnů od jmenování, a shodně postupovat v případě změny v osobě pověřence pro ochranu osobních údajů.

VI. ODMĚNA

6.1 Smluvní strany se dohodly, že odměna Dodavatele za plnění povinností dle této Smlouvy je již zahrnuta v odměně Dodavatele sjednané v Podkladové smlouvě. Pro vyjasnění všech

povinností se sjednává, že nad rámec odměny náhrad a plateb sjednaných v Podkladové smlouvě, nebude Správce OÚ Dodavateli hradit ničeho.

VII. ODPOVĚDNOST ZA ÚJMU a SANKCE

7.1 Dodavatel odpovídá za jakoukoli újmu, která Správci OÚ či třetím osobám vznikne porušením jeho povinností na základě této Smlouvy a/nebo Obecného nařízení.

7.2 Dodavatel rovněž odpovídá za jakoukoli újmu, která Správci OÚ či třetím osobám vznikne porušením povinností vyplývajících z této Smlouvy a/nebo z Obecného nařízení Dalším zpracovatelem či s ním spolupracujícím dalším zpracovatelem.

7.3 V případě, že Dodavatel, Další zpracovatel či další zpracovatel spolupracující s Dalším zpracovatelem poruší pravidla nakládání s osobními údaji stanovená v této Smlouvě, resp. Obecným nařízením, může se Správce OÚ domáhat, aby se tohoto jednání zdržel a odstranil závadný stav, resp. aby zajistil, že takto učiní Další zpracovatel či další zpracovatel spolupracující s dalším zpracovatelem. Dále může požadovat smluvní pokutu ve výši 100 000 Kč za každé jednotlivé porušení bez ohledu na to, zda bylo způsobeno Dodavatelem, Dalším zpracovatelem či dalším zpracovatelem spolupracujícím s Dalším zpracovatelem a Dodavatel se zavazuje mu tuto smluvní pokutu uhradit. Úhradou smluvní pokuty dle tohoto odstavce není dotčeno právo Správce OÚ na náhradu újmy ve výši přesahující smluvní pokutu.

VIII. SKONČENÍ SMLOUVY, RESP. PODKLADOVÉ SMLOUVY

8.1 Tato Smlouva skončí:

a) uplynutím sjednané doby trvání, nebo

b) na základě dohody Smluvních stran, nebo

c) ke dni skončení Podkladové smlouvy, nebo

d) odstoupením od Podkladové smlouvy Správcem OÚ, jak je blíže specifikováno v čl. VIII. odst. 8.2 a 8.3 této Smlouvy.

8.2 Smluvní strany tímto sjednávají nový důvod pro odstoupení od Podkladové smlouvy Správcem OÚ. V případě, že:

a) v rámci některého z auditů osobních údajů či inspekcí provedených Správcem OÚ či jím pověřeným auditorem u Dodavatele ve smyslu čl. V odst. 5.16 této Smlouvy budou zjištěny vážné nedostatky v nakládání s osobními údaji Dodavatelem a Dodavatel tyto nedostatky neodstraní do dvou týdnů, nebude-li se Správcem OÚ odsouhlasena jiná lhůta; nebo

b) Správce OÚ zjistí, že Dodavatel porušil některé z ustanovení čl. V. odst. 5.1, 5.2, 5.4, 5.5, 5.6, 5.10, 5.12, 5.15, 5.16, 5.17, 5.18, 5.20 této Smlouvy; nebo

c) Správce OÚ zjistí, že Dodavatel porušil některé z ustanovení čl. V. odst. 5.3, 5.7, 5.8, 5.9, 5.11, 5.13 a 5.14 a na písemnou výzvu Správce OÚ, ve které mu dal přiměřenou lhůtu k nápravě Dodavatel nápravu nezajistil; nebo

d) dojde k jakémukoli úniku osobních údajů zpracovávaných Dodavatelem z jakékoli příčiny (např. zcizení dat pracovníkem Dodavatele; hackerský útok na IT infrastrukturu Dodavatele; nevyhovující způsob likvidace dokumentů obsahujících osobní údaje atd.);

je Správce OÚ oprávněn odstoupit od Podkladové smlouvy. Odstoupení od Podkladové smlouvy je účinné doručením odstoupení Dodavateli, neurčí-li Správce OÚ v textu odstoupení jinak. Dodavatel je v takovém případě povinen neprodleně předat Správci OÚ veškeré zpracovávané osobní údaje ve standardním elektronickém formátu a poskytnout mu veškerou součinnost nutnou pro zachování činnosti Správce OÚ.

8.3 Ustanovení článku VIII. odst. 8.2 této Smlouvy platí obdobně v případě, že by k pochybením dle písm. a) až d) došlo u Dalšího zpracovatele či dalšího zpracovatele, se kterým Další zpracovatel spolupracuje.

IX. ZÁVĚREČNÁ USTANOVENÍ, COMPLIANCE DOLOŽKA

9.1 Smluvní strany níže svým podpisem stvrzují, že v průběhu vyjednávání o této Smlouvě vždy jednaly a postupovaly čestně a transparentně, a současně se zavazují, že takto budou jednat i při plnění této Smlouvy a veškerých činností s ní souvisejících.

9.2 Smluvní strany se dále zavazují vždy jednat tak a přijmout taková opatření, aby nedošlo ke vzniku důvodného podezření na spáchání trestného činu či k samotnému jeho spáchání (včetně formy účastenství), tj. jednat tak, aby kterékoli ze smluvních stran nemohla být přičtena odpovědnost podle zákona č. 418/2011 Sb., o trestní odpovědnosti právnických osob a řízení proti nim, nebo nevznikla trestní odpovědnost fyzických osob (včetně zaměstnanců) podle trestního zákoníku, případně aby nebylo zahájeno trestní stíhání proti kterékoli ze smluvních stran, včetně jejích zaměstnanců podle platných právních předpisů.

9.3 Smluvní strany se dále zavazují navzájem si neprodleně oznámit důvodné podezření ohledně možného naplnění skutkové podstaty jakéhokoli z trestných činů, zejména trestného činu korupční povahy, a to bez ohledu a nad rámec případné zákonné oznamovací povinnosti; obdobné platí ve vztahu k jednání, které je v rozporu se zásadami vyjádřenými v tomto článku.

9.4 Tato Smlouva nahrazuje veškerá dřívější ujednání mezi Smluvními stranami ohledně ochrany osobních údajů zpracovávaných Dodavatelem v souvislosti s Podkladovou smlouvou.

9.5 Na vztahy mezi účastníky v této smlouvě výslovně neupravené se přiměřeně použijí ustanovení OZ, jakož i dalších právních předpisů.

9.6 Dodavatel bere na vědomí, že Správce OÚ je povinným subjektem dle § 2 odst. 1 zákona č. 340/2015 Sb., o registru smluv. Smluvní strany dohodly, že pokud to bude k splnění zákonných povinností Správce OÚ nezbytné kupř. v souvislosti se zveřejněním Podkladové smlouvy, uveřejní Správce OÚ tuto smlouvu, a to včetně příloh, dodatků, odvozených dokumentů a metadat v zákonem stanovené lhůtě, v registru smluv. Za tím účelem se smluvní strany zavazují v rámci kontraktačního procesu připravit smlouvu též v otevřeném a strojově čitelném formátu.

9.7 Tato Smlouva nabývá platnosti a účinnosti dnem jejího podpisu oběma Smluvními stranami, resp. účinnosti dnem uveřejnění v registru smluv podle zákona č. 340/2015 Sb., o registru smluv s výjimkou čl. V. odst. 5.10 písm. b), c), d) a odst. 5.13, 5.14 a 5.18, které nabudou účinnosti dne 25. května 2018.

9.8 Tuto Smlouvu lze měnit pouze písemnými dodatky v listinné podobě podepsanými oběma Smluvními stranami.

9.9 Tato Smlouva se řídí a musí být vykládána podle platných ustanovení právního řádu České republiky. Případné spory z této Smlouvy budou řešeny smírnou cestou. Nebude-li dohoda Smluvních stran možná, sjednávají Smluvní strany pro takový případ pro řešení sporů místní příslušnost obecného soudu podle sídla Správce OÚ.

9.10 Pokud jakékoliv ustanovení této Smlouvy je nebo se stane neplatným nebo nevymahatelným jako celek nebo jeho část, je plně oddělitelným od ostatních ustanovení této Smlouvy a taková neplatnost nebo nevymahatelnost nebude mít žádný vliv na platnost a vymahatelnost jakýchkoliv ostatních ustanovení této Smlouvy. V takovém případě Smluvní strany nahradí takové neplatné nebo nevymahatelné ustanovení jiným ustanovením, které bude v nejvyšší možné míře odpovídat obsahu původního ustanovení.

9.11 Tato Smlouva byla podepsána ve dvou vyhotoveních, z nichž každá Smluvní strana obdrží po jednom.

Přílohy:

č. 1 Seznam Dalších zpracovatelů zapojených do zpracování osobních údajů prováděného v souvislosti s Podkladovou smlouvou

Správce OÚ: [doplnit]	**[*Dodavatel: doplnit obchodní firmu*]**
V [doplnit místo] dne _____	V _____ dne _____
_____	_____
[doplnit jméno a funkci]	[*doplnit jméno a funkci, resp. st. orgán*]

Příloha č. 1

Seznam Dalších zpracovatelů zapojených do zpracování osobních údajů prováděného v souvislosti s Podkladovou smlouvou

Seznam dalších zpracovatelů.xlsx

10.2 Varianta bez podzpracování (budoucí)

SMLOUVA O ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ

podle čl. 28 Obecného nařízení o ochraně osobních údajů[13]

(„**Smlouva**“)

[*zde doplnit právnickou osobu, která je stranou smlouvy*], dále jen

(„**Správce OÚ**“),

zastoupená panem [*doplnit*]

a

společnost [*doplnit obchodní firmu*]

se sídlem [*doplnit*], IČO: [*doplnit*], zapsaná v obchodním rejstříku vedeném *Městským / Krajským* soudem v [*doplnit*], sp. zn. [*doplnit*] („**Dodavatel**“),

zastoupená [*doplnit jméno, příjmení a funkci*] a [*doplnit jméno, příjmení a funkci*],

(Správce OÚ a Dodavatel dále společně jako „**Smluvní strany**“)

se níže uvedeného dne, měsíce a roku dohodli na následujícím:

PREAMBULE

Vzhledem k tomu, že:

I. Smluvní strany mají oboustranný úmysl spolu uzavřít smlouvu [*doplnit název*] („**Podkladová smlouva**“) a v rámci plnění této smlouvy Dodavatel bude zpracovávat osobní údaje, jichž je Správce OÚ správcem nebo zpracovatelem, jak je blíže specifikováno níže,

II. Ode dne 25. května 2018 je v účinnosti Obecné nařízení upravující mj. povinnosti správců a zpracovatelů osobních údajů v souvislosti s jejich zpracováním,

III. Smluvní strany uzavírají tuto Smlouvu za účelem dodržování požadavků Obecné nařízení pro ochranu osobních údajů zejm, mj. dodržování povinností správců a zpracovatelů osobních údajů v souvislosti s jejich zpracováním při plnění Podkladové smlouvy a případně před započetím a po končení právních vztahů Smluvních stran dle Podkladové smlouvy.

uzavírají spolu Smluvní strany tuto Smlouvu:

[13] Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES („**Obecné nařízení**“/“**GDPR**“).

IV. POSTAVENÍ SMLUVNÍCH STRAN PŘI ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ V SOUVISLOSTI S PODKLADOVOU SMLOUVOU

4.1 Správce OÚ je správcem osobních údajů *zájemců/klientů/občanů obce ve vztahu k produktům/službám Dodavatele* a Dodavatel je ve vztahu k těmto údajům v postavení zpracovatele osobních údajů.

V. PŘEDMĚT a DOBA ZPRACOVÁNÍ

5.1 Dodavatel bude na základě této Smlouvy pro Správce OÚ zpracovávat následující osobní údaje: [*doplnit* kupř. jméno, příjmení adresa bydliště, emailová adresa telefon,……]

5.2 Dodavatel je oprávněn osobní údaje na základě této Smlouvy zpracovávat *po dobu trvání Podkladové smlouvy*.

VI. POVAHA a ÚČEL ZPRACOVÁNÍ

6.1 Dodavatel je na základě této Smlouvy oprávněn osobní údaje zpracovávat pro *účel/y* [*doplnit podle údajů v podkladové smlouvě*].

6.2 Zpracování osobních údajů bude spočívat v jejich:

- sběru,
- zaznamenávání,
- strukturalizaci,
- modifikaci,
- uchovávání,
- extrakci,
- srovnávání,
- likvidaci,
- [*případně doplnit jinou činnost*].

VII. TYP OSOBNÍCH ÚDAJŮ a KATEGORIE SUBJEKTŮ ÚDAJŮ

7.1 Dodavatel na základě této Smlouvy pro Správce OÚ zpracovává osobní údaje následujících kategorií subjektů údajů:

(v) [*doplnit, kupř. zaměstnanci Správce OÚ*];
(vi) *občané*
(vii) [*doplnit osoby vstupující do budov Správce OÚ*]
(viii) [*určit podle podkladové smlouvy*].

7.2 Dodavatel na základě této Smlouvy pro Správce OÚ zpracovává následující typy osobních údajů: [*osobní údaje ve smyslu čl. 4 odst. 1 Obecného nařízení / zvláštní kategorie osobních údajů ve smyslu čl. 9 odst. 1 Obecného nařízení / osobní údaje týkající se rozsudků v trestních věcech a trestných činů.*]

VIII. POVINNOSTI DODAVATELE a SPRÁVCE OÚ

Dodavatel se zavazuje:

8.1 Zpracovávat osobní údaje pouze za účelem definovaným v této Smlouvě, přičemž se výslovně zavazuje, že v žádném případě je nebude zpracovávat pro vlastní účely.

8.2 Zpracovávat osobní údaje pouze v souladu s doloženými pokyny Správce OÚ, včetně předání osobních údajů do třetí země nebo mezinárodní organizaci.

Sjednává se, že pokud Dodavatel dojde k závěru, že některý z pokynů Správce OÚ je v rozporu s Obecným nařízením nebo s jakýmkoli jiným právním předpisem v oblasti ochrany osobních údajů, je povinen Správce OÚ na tuto skutečnost neprodleně písemně upozornit.

Pokud Dodavateli určité zpracování ukládá právo Evropské unie nebo členského státu, které se vztahuje na Dodavatele, je Dodavatel povinen Správce OÚ o tomto právním požadavku písemně informovat před zahájením takového zpracování, ledaže by tyto právní předpisy toto informování zakazovaly z důležitých důvodů veřejného zájmu.

8.3 Vést, písemně (včetně elektronické formy), záznamy o zpracování osobních údajů v souladu s čl. 30 odst. 2 Obecného nařízení, obsahující:

e) [*jméno/obchodní firmu*] a kontaktní údaje Dodavatele a každého správce, pro kterého jedná a případného zástupce správce nebo Dodavatele a pověřence pro ochranu osobních údajů;

f) Kategorie zpracování prováděného pro každého ze správců;

g) Informace o případném předání osobních údajů do třetí země nebo mezinárodní organizaci, včetně identifikace této třetí země či mezinárodní organizace a v případě podle čl. 49 odst. 1 druhého pododstavce Obecného nařízení doložení vhodných záruk;

h) Je-li to možné, obecný popis technických a organizačních bezpečnostních opatření uvedených v čl. 32 odst. 1 Obecného nařízení.

8.4 Nesdělovat osobní údaje třetím osobám, s výjimkou případů, kdy Dodavatel bude mít k tomu předem výslovný pokyn Správce OÚ.

Dodavatel je oprávněn, na základě písemného pokynu Správce OÚ, sdělovat osobní údaje jiným zpracovatelům pověřeným Správcem OÚ. Pokyn Správce OÚ musí obsahovat jasnou identifikaci zpracovatele, rozsah osobních údajů, které mají být předány a prostředky pro zajištění zabezpečení předání osobních údajů.

8.5 Nepověřovat zpracováním osobních údajů na základě této Smlouvy další osoby (dále společně jako „**Další zpracovatel**“).

V případě, že by Dodavatel zamýšlel do zpracování osobních údajů na základě této Smlouvy zapojit Další zpracovatele, je o tom povinen Správce OÚ písemně informovat alespoň 30 pracovních dní před zahájením zamýšlené spolupráce s Dalším zpracovatelem a Správci OÚ sdělit zejména, kterými činnostmi zpracování osobních údajů zamýšlí Dalšího zpracovatele pověřit a identifikační a kontaktní údaje Dalšího zpracovatele a případně další informace či návrh smlouvy, bude-li to Správce OÚ považovat za potřebné k posouzení navrhované spolupráce mezi Dodavatelem a Dalším zpracovatelem. Smlouvu s Dalším zpracovatelem smí Dodavatel uzavřít pouze v případě, že mu Správce OÚ ve lhůtě 14 kalendářních dní od obdržení informace nesdělí nesouhlasnou námitku.

Dodavatel je povinen smluvně zavázat Dalšího zpracovatele k povinnosti plnit Dodavatelovy povinnosti dle této Smlouvy a případné další pokyny Správce OÚ v oblasti ochrany osobních údajů.

Neplní-li Další zpracovatel své povinnosti v oblasti ochrany osobních údajů, odpovídá Správci OÚ za plnění povinností daného Dalšího zpracovatele i nadále Dodavatel.

Dodavatel je rovněž povinen oznámit Správci OÚ ukončení spolupráce s kterýmkoli z Dalších zpracovatelů, a to nejpozději do 3 dnů od ukončení spolupráce.

Nejpozději do 20. května 2018 poskytne Dodavatel Správci OÚ ke schválení vyplněný seznam Dalších zpracovatelů, jehož vzor tvoří přílohu č. 1 této Smlouvy, kteří jsou již zapojeni do zpracování osobních údajů v souvislosti s Podkladovou smlouvou, včetně údajů o dalších zpracovatelích, se kterými případně spolupracují Další zpracovatelé, a to elektronicky na adresu [*doplnit*]. V případě, že od okamžiku poskytnutí tohoto seznamu do 25. května 2018 dojde ke změně v poskytnutých údajích, zavazuje se Dodavatel Správci OÚ bez zbytečného odkladu stejným způsobem zaslat aktualizovaný seznam.

8.6 Udržovat mlčenlivost o zpracovávaných osobních údajích, ke kterým má přístup v souvislosti s Podkladovou smlouvu, resp. touto Smlouvou, a to včetně období po skončení této Smlouvy.

8.7 Zajistit, že jeho pracovníci nakládající s osobními údaji se písemně výslovně zaváží k dodržování mlčenlivosti ohledně zpracovávaných osobních údajů, dodržování stanovených bezpečnostních opatření a podmínek pro zpracování osobních údajů dle této Smlouvy.

8.8 Zajistit kontinuální odpovídající proškolování svých pracovníků nakládajících s osobními údaji v oblasti ochrany osobních údajů.

8.9 Oznámit Správci OÚ jakoukoli změnu zpracovávaných osobních údajů.

8.10 Poskytnout Správci OÚ veškerou součinnost, kterou bude potřebovat pro uskutečnění výkonu práva subjektu údajů:

e) na přístup k osobním údajům, opravu osobních údajů, výmaz osobních údajů, námitku proti zpracování osobních údajů;

f) na omezení zpracování osobních údajů;

g) na přenositelnost osobních údajů;

h) nebýt předmětem automatizovaného rozhodování ve smyslu čl. 22 odst. 1 Obecného nařízení.

Dodavatel je povinen pokynům Správce OÚ v souvislosti s výkonem výše popsaných práv subjektů osobních údajů vyhovět ve lhůtě stanovené Správcem OÚ ve vztahu ke každé individuální žádosti.

V případě, že by subjekt osobních údajů uplatnil některé z výše uvedených práv ve vztahu s Dodavatelem pro Správce OÚ zpracovávaným osobním údajům přímo u Dodavatele a nikoli u Správce OÚ, zavazuje se Dodavatel takovou žádost Správci OÚ zaslat prostřednictvím e-mailu na adresu [*Doplnit adresu kontaktní osoby Správce OÚ případně též DPO*] a to bez zbytečného odkladu, nejpozději však do 24 hodin od jejího převzetí.

8.11 Pokud je to vzhledem k činnosti Dodavatele vykonávané pro Správce OÚ relevantní, poskytnout subjektům osobních údajů, v souladu s příslušnými ustanoveními Všeobecných podmínek daného produktu, v okamžiku získání osobních údajů, informace Správce OÚ o zpracování osobních údajů, a to vždy aktuální a ve formátu stanoveném Správcem OÚ.

8.12 Jakmile zjistí porušení zabezpečení osobních údajů (dále jen „bezpečnostní incident“), ohlásit jej neprodleně, nejpozději však do 24 hodin Správci OÚ a poskytnout mu veškerou součinnost a veškeré informace, které Správce OÚ může potřebovat ke splnění svých zákonných povinností, zejména, nikoli však výlučně:

e) Popis povahy daného případu bezpečnostního incidentu včetně, pokud je to možné, kategorií a přibližného počtu dotčených subjektů údajů a kategorií a přibližného množství dotčených záznamů osobních údajů;

f) Jméno a kontaktní údaje pověřence pro ochranu osobních údajů nebo jiného kontaktního místa, které může poskytnout bližší informace;

g) Popis pravděpodobných důsledků bezpečnostního incidentu;

h) Popis opatření, která Dodavatel přijal nebo navrhuje k přijetí s cílem vyřešit daný bezpečnostní incident, včetně případných opatření ke zmírnění možných nepříznivých dopadů.

Pokud není možné poskytnout Správci OÚ informace podle písm. a) až d) výše současně, mohou být poskytnuty postupně bez dalšího zbytečného odkladu.

Kontaktní osobou pro oznámení bezpečnostních incidentů Správci OÚ a další související komunikaci, nebude-li Správcem OÚ určeno jinak, je: [*doplnit jméno a příjmení*], e-mail [*doplnit*], telefon [*doplnit*]/ pověřenec ochranou osobních údajů Správce OÚ.

Výše uvedené povinnosti Dodavatele se uplatí obdobně, pokud k bezpečnostnímu incidentu dojde u Dalšího zpracovatele nebo dalšího zpracovatele spolupracujícího s Dalším zpracovatelem.

8.13 Poskytnout Správci OÚ veškerou součinnost, která může být pro Správce OÚ nezbytná pro vypracování posouzení vlivu na ochranu osobních údajů ve smyslu čl. 35 Obecného nařízení.

8.14 Poskytnout Správci OÚ veškerou potřebnou součinnost, která může být nezbytná pro uskutečnění předchozích konzultací ve smyslu čl. 36 Obecného nařízení s Úřadem pro ochranu osobních údajů.

8.15 Poskytnout Správci OÚ veškeré informace, které mohou být pro Správce OÚ nezbytné k prokázání plnění svých povinností v roli správce či zpracovatele osobních údajů nebo pro účely jakýchkoli auditů v oblasti ochrany osobních údajů.

8.16 Umožnit Správci OÚ audity ochrany osobních údajů, včetně inspekcí, prováděných Správcem OÚ či jím pověřeným auditorem u Dodavatele, a v rámci těchto auditů a/nebo inspekcí poskytnout Správci OÚ či pověřenému auditorovi veškerou potřebnou součinnost.

8.17 Zavést v souladu s analýzou rizik provedenou [*doplnit*] dne [*doplnit*] alespoň tato následující opatření pro zabezpečení osobních údajů:

c) [*doplnit*];

d) [*doplnit*].

Zavedením výše uvedených opatření se Dodavatel nezbavuje své odpovědnosti zajistit ve vztahu k osobním údajům zpracovávaným na základě této Smlouvy úroveň zabezpečení odpovídající danému riziku. Dodavatel je v každém případě povinen v souladu s čl. 32 Obecného nařízení s přihlédnutím ke stavu techniky, nákladům na provedení, povaze, rozsahu, kontextu a účelům zpracování i k různě pravděpodobným a různě závažným rizikům pro práva a svobody fyzických osob, provést vhodná technická a organizační opatření, aby zajistil úroveň zabezpečení odpovídající danému riziku, případně včetně:

e) Pseudonymizace a šifrování osobních údajů;

f) Schopnosti zajistit neustálou důvěrnost, integritu, dostupnost a odolnost systémů a služeb zpracování;

g) Schopnosti obnovit dostupnost osobních údajů a přístup k nim včas v případě fyzických či technických incidentů;

h) Procesu pravidelného testování, posuzování a hodnocení účinnosti zavedených technických a organizačních opatření pro zajištění bezpečnosti zpracování;

a tato opatření průběžně vyhodnocovat a případně odpovídajícím způsobem upravovat.

8.18 V případě, že je k tomu dle Obecného nařízení povinen, jmenovat pověřence pro ochranu osobních údajů a sdělit Správci OÚ jeho jméno, příjmení a kontaktní údaje.

8.19 Po skončení této Smlouvy vrátit Správci OÚ všechny osobní údaje, včetně, pokud je to relevantní, nosičů, na nichž jsou uloženy a současně tyto osobní údaje vymazat ze všech elektronických zařízení či databází používaných Dodavatelem. / Po skončení této Smlouvy předat osobní údaje zpracovateli určenému Správcem OÚ včetně, pokud je to relevantní, nosičů, na nichž jsou uloženy a současně tyto osobní údaje vymazat ze všech elektronických zařízení či databází používaných Dodavatelem. / Po skončení této Smlouvy osobní údaje do *10 pracovních dnů* zlikvidovat a Správci OÚ do *2 pracovních dnů* od jejich likvidace zaslat písemný protokol o jejich likvidaci.

8.20 Uzavřít a po dobu trvání této Smlouvy udržovat v platnosti pojistnou smlouvu kryjící odpovědnost za případnou újmu, kterou by mohl v souvislosti s výkonem činnosti podle této Smlouvy Správci OÚ způsobit, a to do výše minimálně [*Nutno doplnit s ohledem na rizika u každého dodavatele přiměřeně podle rizik pro práva subjektů OÚ*]. Kopii pojistné smlouvy je Dodavatel Správci OÚ povinen kdykoli na požádání předložit, a to nejpozději do 3 pracovních dnů ode dne výzvy Správce OÚ k jejímu předložení.

8.21 V případě, že Dodavatel bude mít v souvislosti se zpracováním osobních údajů na základě této Smlouvy potřebu konzultace se Správcem OÚ, zavazuje se Správce OÚ poskytnout mu potřebnou součinnost.

8.22 Správce OÚ se zavazuje pro případ, že dle Obecného nařízení jmenuje pověřence pro ochranu osobních údajů sdělit Dodavateli jeho jméno, příjmení a kontaktní údaje do tří pracovních dnů od jmenování, a shodně postupovat v případě změny v osobě pověřence pro ochranu osobních údajů.

IX. ODMĚNA

9.1 Smluvní strany se dohodly, že odměna Dodavatele za plnění povinností dle této Smlouvy je již zahrnuta v odměně Dodavatele sjednané v Podkladové smlouvě. Pro vyjasnění všech povinností se sjednává, že nad rámec odměny náhrad a plateb sjednaných v Podkladové smlouvě, nebude Správce OÚ Dodavateli hradit ničeho.

X. ODPOVĚDNOST ZA ÚJMU a SANKCE

10.1 Dodavatel odpovídá za jakoukoli újmu, která Správci OÚ či třetím osobám vznikne porušením jeho povinností na základě této Smlouvy a/nebo Obecného nařízení.

10.2 Dodavatel rovněž odpovídá za jakoukoli újmu, která Správci OÚ či třetím osobám vznikne porušením povinností vyplývajících z této Smlouvy a/nebo z Obecného nařízení Dalším zpracovatelem či s ním spolupracujícím dalším zpracovatelem.

10.3 V případě, že Dodavatel, Další zpracovatel či další zpracovatel spolupracující s Dalším zpracovatelem poruší pravidla nakládání s osobními údaji stanovená v této Smlouvě, resp. Obecným nařízením, může se Správce OÚ domáhat, aby se tohoto jednání zdržel a odstranil závadný stav, resp. aby zajistil, že takto učiní Další zpracovatel či další zpracovatel spolupracující s dalším zpracovatelem. Dále může požadovat smluvní pokutu ve výši 100 000 Kč za každé jednotlivé porušení bez ohledu na to, zda bylo způsobeno Dodavatelem, Dalším zpracovatelem či dalším zpracovatelem spolupracujícím s Dalším zpracovatelem a Dodavatel se zavazuje mu tuto smluvní pokutu uhradit. Úhradou smluvní pokuty dle tohoto odstavce není dotčeno právo Správce OÚ na náhradu újmy ve výši přesahující smluvní pokutu.

XI. SKONČENÍ SMLOUVY, RESP. PODKLADOVÉ SMLOUVY

11.1 Tato Smlouva skončí:

e) uplynutím sjednané doby trvání, nebo

f) na základě dohody Smluvních stran, nebo

g) ke dni skončení Podkladové smlouvy, nebo

h) odstoupením od Podkladové smlouvy Správcem OÚ, jak je blíže specifikováno v čl. VIII. odst. 8.2 a 8.3 této Smlouvy.

11.2 Smluvní strany tímto sjednávají nový důvod pro odstoupení od Podkladové smlouvy Správcem OÚ. V případě, že:

e) v rámci některého z auditů osobních údajů či inspekcí provedených Správcem OÚ či jím pověřeným auditorem u Dodavatele ve smyslu čl. V odst. 5.16 této Smlouvy budou zjištěny vážné nedostatky v nakládání s osobními údaji Dodavatelem a Dodavatel tyto nedostatky neodstraní do dvou týdnů, nebude-li se Správcem OÚ odsouhlasena jiná lhůta; nebo

f) Správce OÚ zjistí, že Dodavatel porušil některé z ustanovení čl. V. odst. 5.1, 5.2, 5.4, 5.5, 5.6, 5.10, 5.12, 5.15, 5.16, 5.17, 5.18, 5.20 této Smlouvy; nebo

g) Správce OÚ zjistí, že Dodavatel porušil některé z ustanovení čl. V. odst. 5.3, 5.7, 5.8, 5.9, 5.11, 5.13 a 5.14 a na písemnou výzvu Správce OÚ, ve které mu dal přiměřenou lhůtu k nápravě Dodavatel nápravu nezajistil; nebo

h) dojde k jakémukoli úniku osobních údajů zpracovávaných Dodavatelem z jakékoli příčiny (např. zcizení dat pracovníkem Dodavatele; hackerský útok na IT infrastrukturu Dodavatele; nevyhovující způsob likvidace dokumentů obsahujících osobní údaje atd.);

Správce OÚ je oprávněn odstoupit od Podkladové smlouvy. Odstoupení od Podkladové smlouvy je účinné doručením odstoupení Dodavateli, neurčí-li Správce OÚ v textu odstoupení jinak. Dodavatel je v takovém případě povinen neprodleně předat Správci OÚ veškeré zpracovávané osobní údaje ve standardním elektronickém formátu a poskytnout mu veškerou součinnost nutnou pro zachování činnosti Správce OÚ.

11.3 Ustanovení článku VIII. odst. 8.2 této Smlouvy platí obdobně v případě, že by k pochybením dle písm. a) až d) došlo u Dalšího zpracovatele či dalšího zpracovatele, se kterým Další zpracovatel spolupracuje.

XII. ZÁVĚREČNÁ USTANOVENÍ, COMPLIANCE DOLOŽKA

12.1 Smluvní strany níže svým podpisem stvrzují, že v průběhu vyjednávání o této Smlouvě vždy jednaly a postupovaly čestně a transparentně, a současně se zavazují, že takto budou jednat i při plnění této Smlouvy a veškerých činností s ní souvisejících.

12.2 Smluvní strany se dále zavazují vždy jednat tak a přijmout taková opatření, aby nedošlo ke vzniku důvodného podezření na spáchání trestného činu či k samotnému jeho spáchání (včetně formy účastenství), tj. jednat tak, aby kterékoli ze smluvních stran nemohla být přičtena odpovědnost podle zákona č. 418/2011 Sb., o trestní odpovědnosti právnických osob a řízení proti nim, nebo nevznikla trestní odpovědnost fyzických osob (včetně zaměstnanců) podle trestního zákoníku, případně aby nebylo zahájeno trestní stíhání proti kterékoli ze smluvních stran, včetně jejích zaměstnanců podle platných právních předpisů.

12.3 Smluvní strany se dále zavazují navzájem si neprodleně oznámit důvodné podezření ohledně možného naplnění skutkové podstaty jakéhokoli z trestných činů, zejména trestného činu korupční povahy, a to bez ohledu a nad rámec případné zákonné oznamovací povinnosti; obdobné platí ve vztahu k jednání, které je v rozporu se zásadami vyjádřenými v tomto článku.

12.4 Tato Smlouva nahrazuje veškerá dřívější ujednání mezi Smluvními stranami ohledně ochrany osobních údajů zpracovávaných Dodavatelem v souvislosti s Podkladovou smlouvou.

12.5 Na vztahy mezi účastníky v této smlouvě výslovně neupravené se přiměřeně použijí ustanovení OZ, jakož i dalších právních předpisů.

12.6 Dodavatel bere na vědomí, že Správce OÚ je povinným subjektem dle § 2 odst. 1 zákona č. 340/2015 Sb., o registru smluv. Smluvní strany dohodly, že pokud to bude k splnění zákonných povinností Správce OÚ nezbytné kupř. v souvislosti se zveřejněním Podkladové smlouvy, uveřejní Správce OÚ tuto smlouvu, a to včetně příloh, dodatků, odvozených dokumentů a metadat v zákonem stanovené lhůtě, v registru smluv. Za tím účelem se smluvní strany zavazují v rámci kontraktačního procesu připravit smlouvu též v otevřeném a strojově čitelném formátu.

12.7 Tato Smlouva nabývá platnosti a účinnosti dnem jejího podpisu oběma Smluvními stranami, resp. účinnosti dnem uveřejnění v registru smluv podle zákona č. 340/2015 Sb., o registru smluv s výjimkou čl. V. odst. 5.10 písm. b), c), d) a odst. 5.13, 5.14 a 5.18, které nabudou účinnosti dne 25. května 2018.

12.8 Tuto Smlouvu lze měnit pouze písemnými dodatky v listinné podobě podepsanými oběma Smluvními stranami.

12.9 Tato Smlouva se řídí a musí být vykládána podle platných ustanovení právního řádu České republiky. Případné spory z této Smlouvy budou řešeny smírnou cestou. Nebude-li dohoda Smluvních stran možná, sjednávají Smluvní strany pro takový případ pro řešení sporů místní příslušnost obecného soudu podle sídla Správce OÚ.

12.10 Pokud jakékoliv ustanovení této Smlouvy je nebo se stane neplatným nebo nevymahatelným jako celek nebo jeho část, je plně oddělitelným od ostatních ustanovení této Smlouvy a taková neplatnost nebo nevymahatelnost nebude mít žádný vliv na platnost a vymahatelnost jakýchkoliv ostatních ustanovení této Smlouvy. V takovém případě Smluvní strany nahradí takové neplatné nebo nevymahatelné ustanovení jiným ustanovením, které bude v nejvyšší možné míře odpovídat obsahu původního ustanovení.

12.11 Tato Smlouva byla podepsána ve dvou vyhotoveních, z nichž každá Smluvní strana obdrží po jednom.

Přílohy:

č. 1 Seznam Dalších zpracovatelů zapojených do zpracování osobních údajů prováděného v souvislosti s Podkladovou smlouvou

Správce OÚ: [doplnit]	**[*Dodavatel: doplnit obchodní firmu*]**
V [doplnit místo] dne _____	V _____ dne _____
_____	_____
[doplnit jméno a funkci]	[*doplnit jméno a funkci, resp. st. orgán*]

Příloha č. 1

Seznam Dalších zpracovatelů zapojených do zpracování osobních údajů prováděného v souvislosti s Podkladovou smlouvou

Seznam dalších zpracovatelů.xlsx

11. VZOR ZÁVAZEK MLČENLIVOSTI

11.1 Dohoda o mlčenlivosti zaměstnance

Já, níže podepsaný/podepsaná

Zaměstnanec:

Jméno	příjmení	Nar.	Bydliště

vykonávající:

práci v pracovním poměru/činnost mimo pracovní poměr v pracovněprávním vztahu na základě pracovní smlouvy/ dohody o provedení práce/dohody o pracovní činnosti

u zaměstnavatele, jímž je [*doplnit*] (dále jen „zaměstnavatel“), uzavírám se zaměstnavatelem dohodu o mlčenlivosti a o zachovávání povinností při ochraně osobních údajů u zaměstnavatele a to při vědomí povinností zaměstnanců stanovených zákonem č. 262/2006 Sb. zákoník práce v platném znění (dále jen „zákoník práce“) v ust. §§ 301 až 302, dle nichž s přihlédnutím k charakteru zaměstnavatele, je zaměstnanec zaměstnancem, který je mimo jiné dle zákoníku povinen

a) pracovat řádně podle svých sil, znalostí a schopností, plnit pokyny nadřízených vydané v souladu s právními předpisy a spolupracovat s ostatními zaměstnanci,

b) dodržovat právní předpisy vztahující se k práci jimi vykonávané; dodržovat ostatní předpisy vztahující se k práci jimi vykonávané, pokud s nimi byl řádně seznámen,

c) řádně hospodařit s prostředky svěřenými jemu zaměstnavatelem a střežit a ochraňovat majetek zaměstnavatele před poškozením, ztrátou, zničením a zneužitím a nejednat v rozporu s oprávněnými zájmy zaměstnavatele.

a dále

a) jednat a rozhodovat nestranně a zdržet se při výkonu práce všeho, co by mohlo ohrozit důvěru v nestrannost rozhodování,

b) **zachovávat mlčenlivost o skutečnostech, o nichž se dozvěděl při výkonu zaměstnání a které v zájmu zaměstnavatele nelze sdělovat jiným osobám**; to neplatí, pokud byl této povinnosti zproštěn statutárním orgánem nebo jím pověřeným vedoucím zaměstnancem, nestanoví-li zvláštní právní předpis jinak,

c) v souvislosti s výkonem zaměstnání nepřijímat dary nebo jiné výhody, s výjimkou darů nebo výhod poskytovaných zaměstnavatelem, u něhož jsou zaměstnáni, nebo na základě právních předpisů,

d) zdržet se jednání, které by mohlo vést ke střetu veřejného zájmu se zájmy osobními, **zejména nezneužívat informací nabytých v souvislosti s výkonem zaměstnání ve prospěch vlastní nebo někoho jiného**.

Zavazuji se výslovně **zachovávat mlčenlivost o skutečnostech, o nichž jsem se dozvěděl a v budoucnu dozvím při výkonu zaměstnání, a které v zájmu zaměstnavatele nelze sdělovat jiným osobám. Povinnost zachovávat mlčenlivost, k níž se zavazuji, se vztahuje zejména na informace, jež jsou osobními údaji** ve smyslu čl. 4 odst. 1 obecného nařízení EU o ochraně osobních údajů (Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů), s nimiž při výkonu zaměstnání u zaměstnavatele budu přicházet do styku, bez ohledu na to zda takové osobní údaje jsou ve správě zaměstnavatele dle ve smyslu čl. 4 odst. 7 či zda je zaměstnavatel jejich zpracovatelem dle ve smyslu čl. 4 odst. 8 obecného nařízení EU o ochraně osobních údajů anebo příjemcem dle ve smyslu čl. 4 odst. 9 obecného nařízení EU o ochraně osobních údajů.

Při výkonu práce se zavazuji respektovat a řídit se pokyny vedoucích zaměstnanců a pověřence ochranou osobních údajů (dále jen „DPO“), jenž je u zaměstnavatele ustanoven, zavazuji se též plnit právní povinnosti ochrany informací, jichž se týká mlčenlivost dle této dohody též pokud vyplývají z dalších právních předpisů, a vnitřních předpisů zaměstnavatele, zejména na úseku požární ochrany BOZP a předpisů fyzické bezpečnosti.

Mlčenlivost se zavazuji zachovávat po dobu trvání mého pracovněprávního vztahu a též v době přiměřené po jeho skončení, nejméně však po dobu, kdy bude trvat povinnost zaměstnavatel zachovávat ochranu těchto informací podle obecného nařízení EU o ochraně osobních údajů či dalších právních předpisů.

Uzavřením této dohody výslovně prohlašuji, že jsem byl/a jsem poučen/a o povinnostech při ochraně osobních údajů vyplývajících z obecného nařízení EU o ochraně osobních údajů a ze Směrnice o nakládání s osobními údaji ze dne ……., dle níž je u zaměstnavatele realizována ochrana osobních údajů v jeho správě, a dále o tom, že u mne bylo provedeno ověření znalosti právních povinností zaměstnanců dle těchto právních předpisů.

V [doplnit] dne .....

....

podpis zaměstnance za zaměstnavatele podpis

12. VZOR INFORMAČNÍ MEMORANDUM

Informace o zpracování osobních údajů a poučení o právech subjektu údajů

INFORMAČNÍ MEMORANDUM

Město Příbram

Sídlo městského úřadu Tyršova 108, 261 19 Příbram

IČO: 002 43 132

Ochrana fyzických osob v souvislosti se zpracováním osobních údajů je základním právem. Ustanovení čl. 8 odst. 1 Listiny základních práv Evropské unie a čl. 16 odst. 1 Smlouvy o fungování Evropské unie přiznávají každému právo na ochranu osobních údajů, které se jej týkají. Zpracování osobních údajů fyzických osob („subjektů údajů“) v rámci Správce OÚ je prováděno ve prospěch těchto osob. Právo na ochranu osobních údajů však není právem absolutním; musí být posuzováno v souvislosti se svou funkcí ve společnosti a v souladu se zásadou proporcionality musí být v rovnováze s dalšími základními právy.

Správce OÚ zpracovává osobní údaje a další informace týkající se občanů a dalších subjektů údajů v rámci samostatné a přenesené působnosti. Většina osobních údajů subjektů je tedy zpracovávána na základě povinností, uložených Správci OÚ zvláštními zákony, případně též smlouvami. Na taková zpracování osobních údajů o subjektech údajů se nevztahuje povinnost získat souhlas těchto osob. Pokud jsou některé osobní údaje zpracovávány mimo zákonnou povinnost, pak taková zpracování podléhají souhlasu občanů. Tato zpracování však Správce OÚ provádí jen výjimečně (např. při pořádání akcí, kdy je nutná předchozí registrace).

Ochrana osobních údajů se vztahuje jak na automatizované zpracování osobních údajů, tak na manuální zpracování. V zásadách a pravidlech ochrany fyzických osob, které Správce OÚ uplatňuje v souvislosti se zpracováním osobních údajů subjektu údajů, respektuje Správce OÚ jejich základní práva a svobody, zejména právo na ochranu osobních údajů. Správce OÚ respektuje práva občanů, která jsou jim zaručena zákony, např. právo vědět a být informován zejména o tom, za jakým účelem se osobní údaje zpracovávají, případně období, po které budou uchovávány. Zásady ochrany osobních údajů se uplatňují na všechny informace, týkající se identifikované nebo identifikovatelné fyzické osoby. Správce OÚ zákonně zpracovává osobní údaje, protože je toto zpracování nezbytné pro výkon úkolů vykonávaných ve veřejném zájmu nebo při výkonu veřejné moci kterým je Správce OÚ pověřen,

nebo z důvodu oprávněných zájmů Správce OÚ nebo třetí strany. Správce OÚ zpracovává osobní údaje občanů podle účelů zpracování v souladu s platnou legislativou pro ochranu osobních údajů, především se zákonem č. 101/2000 Sb., o ochraně osobních údajů, v platném znění a s Nařízením EU 2016/679 (Obecné nařízení o ochraně osobních údajů – GDPR). Přesto má každý dotčený subjekt údajů právo, vznést námitku proti zpracování osobních údajů, které se týkají jeho konkrétní situace. Správce OÚ pak subjektu prokáže závažnost a oprávněnost zájmů Správce OÚ, které nezasahují do zájmů nebo základních práv a svobod občana.

Jak zpracováváme osobní údaje

Zpracování osobních údajů Správcem OÚ je prováděno zákonným a spravedlivým způsobem, je pro subjekty údajů transparentní a informace a všechna sdělení, týkající se zpracování těchto osobních údajů, jsou snadno přístupné, srozumitelné a podávané jasnými a jednoduchými jazykovými prostředky. Při zpracování osobních údajů na základě souhlasu fyzické osoby, jsou tyto osoby upozorněny na případná rizika, vyplývající ze zpracování, a také na pravidla, záruky a práva, která existují v souvislosti se zpracováním jejich osobních údajů. Účely, pro které jsou osobní údaje zpracovávány, jsou jednoznačné a legitimní a jsou stanoveny v okamžiku shromažďování osobních údajů. Rozsah shromažďovaných osobních údajů je vždy přiměřený, relevantní a omezený pouze na údaje nezbytné pro naplnění stanoveného účelu. Rovněž doba, po kterou jsou osobní údaje uchovávány, je omezena na nezbytné minimum. Při veškerém zpracování osobních údajů jsou aplikována opatření, která zaručují náležitou bezpečnost a důvěrnost těchto údajů, (např. zaručující zabránění neoprávněného přístupu k osobním údajům a k zařízení používanému k jejich zpracování).

Správce OÚ, jako správce osobních údajů ve smyslu ust. čl. 4 odst. 7) Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů), má odpovědnost za jakékoliv zpracování osobních údajů a na základě posouzení pravděpodobných a závažných rizik daného zpracování zavedl vhodná a účinná technická a organizační opatření k zajištění ochrany osobních údajů. Součástí opatření pro zabezpečení osobních údajů jsou také pravidelná školení zaměstnanců, kteří zpracovávají osobní údaje. Od zaměstnanců na všech úrovních je vyžadován odpovědný, iniciativní a tvořivý přístup a respektování pravidel systémů zabezpečení osobních údajů.

V souvislosti s přechodem na novou legislativu pro ochranu osobních údajů v EU, tj. Nařízení EU 2016/679 (GDPR), provedl Správce OÚ nové posouzení vlivu všech zpracování na ochranu osobních údajů, s cílem posoudit konkrétní pravděpodobnost a závažnost rizik. Při tomto posouzení zohlednil

Správce OÚ povahu, rozsah, kontext a účely zpracování a zdroje rizik. Opatření k zabezpečení systémů, informací, dat a osobních údajů a konkrétní technická, organizační a bezpečnostní opatření, která Správce OÚ přijal a průběžně zpřesňuje, aby zajistil soulad s Nařízením EU, jsou v této souvislosti nově rozpracována v interních dokumentech a směrnicích Správce OÚ. Součástí těchto opatření je i jmenování pověřence pro ochranu osobních údajů.

Které osobní údaje zpracováváme

Ověřování podpisů a listin dle zákona. 21/2006 Sb., o ověřování ve znění pozdějších předpisů

• Účel zpracování: agenda ověřování podpisů • Kategorie osobních údajů: adresní a identifikační údaje • Kategorie subjektu údajů: zákazníci (klienti) správce • Kategorie příjemců údajů: správce • Doba uchování: 10 let a dále dle Spisového a skartačního řádu včetně Spisového a skartačního

CzechPOINT

• Účel zpracování: vydávání výpisů dle zákona č. 365/2000 Sb., o informačních systémech veřejné správy ve znění pozdějších předpisů • Kategorie osobních údajů: adresní a identifikační údaje • Kategorie subjektu údajů: zákazníci (klienti) správce • Kategorie příjemců údajů: správce • Doba uchování: 10 let a dále dle Spisového a skartačního řádu včetně Spisového a skartačního plánu

Poskytování informací dle zákona č. 106/1999 Sb., o svobodném přístupu k informacím ve znění pozdějších předpisů

• Účel zpracování: poskytování informací občanům na základě zákona č. 106/1999 Sb., o svobodném přístupu k informacím, v platném znění • Kategorie osobních údajů: adresní a identifikační údaje • Kategorie subjektu údajů: zákazníci (klienti) správce • Kategorie příjemců údajů: správce • Doba uchování: 5 let a dále dle Spisového a skartačního řádu včetně Spisového a skartačního plánu

Stížnosti občanů

• Účel zpracování: příjem a vyřizování stížností, dle § 102 odst. 2 písm. n) zákona č. 128/2000 Sb., o obcích • Kategorie osobních údajů: adresní a identifikační údaje • Kategorie subjektu údajů: zákazníci (klienti) správce • Kategorie příjemců údajů: správce • Doba uchování: 5 let a dále dle Spisového a skartačního řádu včetně Spisového a skartačního plánu

Výběrová řízení na pracovní pozici

• Účel zpracování: evidence žadatelů pro výběrová řízení, dle zákona č. 312/2002 Sb., o úřednících územně samosprávných celků a o změně některých zákonů, ve znění pozdějších předpisů a zákon č. 553/1991 Sb., o obecní policii ve znění pozdějších předpisů a u pracovních pozic, kde má Správce OÚ působnost a pravomoc k obsazení pozice • Kategorie osobních údajů: adresní a identifikační údaje;

zvláštní kategorie údajů – trestná činnost, bezúhonnost a jiné údaje • Kategorie subjektu údajů: zákazníci (klienti) správce • Kategorie příjemců údajů: správce • Doba uchování: 5 let a dále dle Spisového a skartačního řádu včetně Spisového a skartačního plánu

Personální, platová a mzdová agenda

• Účel zpracování: zajištění pracovněprávních vztahů a dalších obdobných právních poměrů a všech povinností s nimi spojených dle zákoníku práce a dalších souvisejících nebo navazujících zákonů (zejména daně, sociální a zdravotní pojištění, zákon č. 128/2000 Sb. zákon o obcích (obecní zřízení), zákon č. 586/1992 Sb., o daních z příjmů, zákon č. 187/2006 Sb., o nemocenském pojištění, zákon č. 120/2001 Sb., Exekuční řád, zákon č. 182/2006 Sb., Insolvenční zákon, zákon č. 582/1991 Sb., o organizaci a provádění sociálního zabezpečení, zákon č.148/1997 Sb., o veřejném zdravotním pojištění, zákon č. 589/1992 Sb., o pojistném na sociální zabezpečení a příspěvku na státní politiku zaměstnanosti, zákon č. 155/1995 Sb., o důchodovém pojištění, zákon č. 592/1992 Sb., o pojistném na všeobecné zdravotní pojištění • Kategorie osobních údajů: adresní a identifikační údaje; zvláštní kategorie údajů – zdravotní stav • Kategorie subjektu údajů: zaměstnanci správce, pracovníci na DPP/DPČ + osoby s jiným vztahem ke správci • Kategorie příjemců údajů: správce + oprávněné fyzické a právnické osoby, orgány veřejné moci • Doba uchování: po dobu trvání právního vztahu a dále dle Spisového a skartačního řádu včetně Spisového a skartačního plánu

Střet zájmů - registr oznámení

• Účel zpracování: vedení registru oznámení dle zákona č. 159/2006 Sb., o střetu zájmů, v platném znění • Kategorie osobních údajů: adresní, identifikační a majetkové údaje • Kategorie subjektu údajů: zaměstnanci správce + osoby s jiným vztahem ke správci (veřejní funkcionáři) • Kategorie příjemců údajů: správce, osoby bez vztahu ke správci • Doba uchování: 5 let a dále dle Spisového a skartačního řádu včetně Spisového a skartačního plánu

Krizové a obranné plánování

• Účel zpracování: dokumentace sloužící k ochraně obyvatelstva při vyhlášení krizových stavů, povinnosti ze zákonů č. 240/2000 Sb. ve znění pozdějších předpisů, a 222/1999 Sb. ve znění pozdějších předpisů • Kategorie osobních údajů: adresní a identifikační údaje • Kategorie subjektu údajů: zaměstnanci správce, osoby s jiným vztahem ke správci, osoby bez vztahu ke správci • Kategorie příjemců údajů: správce + oprávněné fyzické a právnické osoby, orgány veřejné moci v rámci • Doba uchování: 5 let a dále dle Spisového a skartačního řádu včetně Spisového a skartačního plánu

Přístup k utajovaným informacím

• Účel zpracování: doložení splnění podmínek k přístupu k utajované informaci, povinnost ze zákona č. 412/2005 Sb. o ochraně utajovaných informací ve znění pozdějších předpisů • Kategorie osobních údajů: adresní a identifikační údaje; zvláštní kategorie údajů zvláštní kategorie údajů – trestná činnost • Kategorie subjektu údajů: zaměstnanci správce • Kategorie příjemců údajů: správce • Doba uchování: 5 let a dále dle Spisového a skartačního řádu včetně Spisového a skartačního plánu

Přísedící soudu

• Účel zpracování: volba přísedících soudu, § 64 odst. 1 zákona č. 6/2002 Sb., o soudech, soudcích, přísedících a státní správě soudů a o změně některých zákonů • Kategorie osobních údajů: adresní a identifikační údaje; zvláštní kategorie údajů – trestná činnost • Kategorie subjektu údajů: osoby bez vztahu ke správci • Kategorie příjemců údajů: správce + oprávněné fyzické a právnické osoby, orgány veřejné moci • Doba uchování: 5 let a dále dle Spisového a skartačního řádu včetně Spisového a skartačního plánu

Petice

• Účel zpracování: příjem a vyřizování petic, dle § 102 odst. 2 písm. n) zákona č. 128/2000 Sb., o obcích • Kategorie osobních údajů: adresní a identifikační údaje • Kategorie subjektu údajů: zákazníci (klienti) správce • Kategorie příjemců údajů: správce • Doba uchování: 10 let a dále dle Spisového a skartačního řádu včetně Spisového a skartačního plánu

Čestné občanství

• Účel zpracování: evidence návrhů na udělení ocenění, dle § 84 odst. 2 písm. s) zákona č. 128/2000 Sb., o obcích ve znění pozdějších předpisů • Kategorie osobních údajů: adresní a identifikační údaje • Kategorie subjektu údajů: zákazníci (klienti) správce + osoby bez vztahu ke správci • Kategorie příjemců údajů: správce • Doba uchování: 5 let a dále dle Spisového a skartačního řádu včetně Spisového a skartačního plánu

Ocenění

• Účel zpracování: evidence návrhů na udělení ocenění, evidence návrhů na udělení ocenění, dle § 84 odst. 2 písm. s) zákona č. 128/2000 Sb., o obcích ve znění pozdějších předpisů • Kategorie osobních údajů: adresní a identifikační údaje • Kategorie subjektu údajů: zákazníci (klienti) správce + osoby bez vztahu ke správci • Kategorie příjemců údajů: správce • Doba uchování: 5 let

Přestupkové řízení

• Účel zpracování: vedení přestupkového řízení zejména dle zákona č. 250/2016 Sb. Zákon o odpovědnosti za přestupky a řízení o nich • Kategorie osobních údajů: adresní a identifikační údaje • Kategorie subjektu údajů: zákazníci (klienti) správce • Kategorie příjemců údajů: oprávněné fyzické a právnické osoby (účastníci řízení), orgány veřejné moci v rámci své působnosti • Doba uchování: 5 let a dále dle Spisového a skartačního řádu včetně Spisového a skartačního plánu

Zprávy o pověsti a spolehlivosti

• Účel zpracování: zprávy o pověsti pro účely trestního řízení a prověrky fyzické osoby a držitele zbrojního průkazu (zákon č.141/1961 Sb., trestní řád, zákon č. 415/2005 Sb., o ochraně utajovaných informací, zákon č. 119/2002 Sb., o střelných zbraních a střelivu ve znění pozdějších předpisů) • Kategorie osobních údajů: adresní a identifikační údaje; zvláštní kategorie údajů – údaje o správním trestání • Kategorie subjektu údajů: zákazníci (klienti) správce • Kategorie příjemců údajů: oprávněné fyzické a právnické osoby (účastníci řízení), orgány veřejné moci v rámci své působnosti • Doba uchování: 5 let a dále dle Spisového a skartačního řádu včetně Spisového a skartačního plánu

Místní referendum

• Účel zpracování: provádění místního referenda dle zákona č. 22/2004 Sb., o místním referendu a o změně některých zákonů, v platném znění • Kategorie osobních údajů: adresní a identifikační údaje • Kategorie subjektu údajů: zákazníci (klienti) správce + osoby bez vztahu ke správci • Kategorie příjemců údajů: správce • Doba uchování: 10 let a dále dle Spisového a skartačního řádu včetně Spisového a skartačního plánu

Evidence místních poplatků

• Účel zpracování: evidence daní a poplatků dle zákona 565/1990, o místních poplatcích a dle zákona č. 280/2009 Sb. daňový řád, ve znění pozdějších předpisů • Kategorie osobních údajů: adresní a identifikační údaje • Kategorie subjektu údajů: zákazníci (klienti) správce • Kategorie příjemců údajů: správce • Doba uchování: po celou dobu přihlášení k poplatkové povinnosti, dále 10 let, v případě vymáhání pohledávek na nedoplatcích 20 let a dále dle Spisového a skartačního řádu včetně Spisového a skartačního plánu

Evidence majetku, pojištění

• Účel zpracování: evidence majetku obce, jeho pojištění dle zákona č. 128/2000 Sb., zákon o obcích, zákona č. 89/2012 Sb., občanský zákoník, zákona č. 563/1991 Sb., zákona o účetnictví, zákona č. 250/2000 Sb., zákon o rozpočtových pravidlech územních rozpočtů, vyhlášky č. 270/2010 Sb. o inventarizaci majetku a závazků ve znění pozdějších předpisů, zákon č. 262/2006 Sb., zákoník práce

• Kategorie osobních údajů: adresní a identifikační údaje, jméno, příjmení, datum narození, titul, trvalé bydliště, místo pobytu, e-mailová adresa, telefonní číslo, ID datové schránky, číslo bankovního účtu, číslo pojistné smlouvy, průkaz totožnosti – kopie, technický průkaz vozidla – kopie, značka spisu pojistné události, podpis • Kategorie subjektu údajů: zákazníci (klienti) správce, občané, zaměstnanci správce, pracovníci na DPP/DPČ, osoby vykonávající veřejnou funkci podle ust. par. 201 zákoníku práce • Kategorie příjemců údajů: správce • Doba uchování: 10 let, a dále dle Spisového a skartačního řádu včetně Spisového a skartačního plánu

Vymáhání pohledávek

• Účel zpracování: evidence a správa finančního majetku obce dle zákona č. 128/2000Sb., zákon o obcích, zákona č. 89/2012 Sb., občanský zákoník, zákona č. 280/2009 Sb., daňový řád ve znění pozdějších předpisů, zákona č. 235/2004 Sb., zákon o dani z přidané hodnoty, zákona č. 220/2013 Sb., vyhlášky o požadavcích na schvalování účetních závěrek některých vybraných účetních jednotek • Kategorie osobních údajů: adresní a identifikační údaje, zvláštní kategorie osobních údajů • Kategorie subjektu údajů: zákazníci (klienti) správce, občané, zaměstnanci správce, pracovníci na DPP/DPČ, osoby vykonávající veřejnou funkci podle ust. par. 201 zákoníku práce, občané, fyzické osoby podnikající, právnické osoby • Kategorie příjemců údajů: správce, osoby vykonávající veřejnou funkci podle ust. par. 201 zákoníku práce, orgány veřejné moci a další oprávněné osoby • Doba uchování: 10 let, a dále dle Spisového a skartačního řádu včetně Spisového a skartačního plánu

Účetnictví a rozpočet

• Účel zpracování: vedení účetnictví obce dle zákona č. 128/2000 Sb., zákon o obcích, zákona č. 89/2012 Sb., občanský zákoník, zákona č. 563/1991 Sb., zákona o účetnictví, zákona č. 250/2000 Sb., zákon o rozpočtových pravidlech územních rozpočtů • Kategorie osobních údajů: adresní a identifikační údaje, zvláštní kategorie údajů • Kategorie subjektu údajů: zákazníci (klienti) správce, zaměstnanci správce, pracovníci na DPP/DPČ, osoby vykonávající veřejnou funkci podle ust. par. 201 zákoníku práce • Kategorie příjemců údajů: správce • Doba uchování: 10 let a dále dle Spisového a skartačního řádu včetně Spisového a skartačního plánu

Agenda hazardních her

• Účel zpracování: povolení k umístění herního prostoru a planění poplatkových povinností dle zákona č. 186/2016 Sb. o hazardních hrách • Kategorie osobních údajů: adresní a identifikační údaje, zvláštní kategorie osobních údajů • Kategorie subjektu údajů: fyzické a právnické osoby • Kategorie příjemců údajů: správce, občané, orgány veřejné moci a další oprávněné osoby • Doba uchování: 5 let a dále dle Spisového a skartačního řádu včetně Spisového a skartačního plánu

Veřejné zakázky • Účel zpracování: realizace zakázky, uzavírání smluv a objednávek • Kategorie osobních údajů: adresní a identifikační údaje • Kategorie subjektu údajů: zákazníci (klienti) správce • Kategorie příjemců údajů: správce • Doba uchování: 10 let a dále dle Spisového a skartačního řádu včetně Spisového a skartačního plánu

Vydávání občanských průkazů

• Účel zpracování: vydávání občanských průkazů • Kategorie osobních údajů: adresní a identifikační údaje • Kategorie subjektu údajů: zákazníci (klienti) správce • Kategorie příjemců údajů: správce + oprávněné fyzické a právnické osoby, orgány veřejné moci v rámci své působnosti • Doba uchování: 20 let a dále dle Spisového a skartačního řádu včetně Spisového a skartačního plánu

Cestovní doklady

• Účel zpracování: vydávání cestovních dokladů • Kategorie osobních údajů: adresní a identifikační údaje • Kategorie subjektu údajů: zákazníci (klienti) správce • Kategorie příjemců údajů: správce + oprávněné fyzické a právnické osoby, orgány veřejné moci v rámci • Doba uchování: 15 let a dále dle Spisového a skartačního řádu včetně Spisového a skartačního plánu

Řidičské průkazy a průkazy profesní způsobilosti řidiče

• Účel zpracování: vydávání řidičských a profesních průkazů řidiče, zkoušky odborné způsobilosti k řízení motorových vozidel, provozovatelů autoškol • Kategorie osobních údajů: adresní a identifikační údaje • Kategorie subjektu údajů: zákazníci (klienti) správce, žadatelé, provozovatelé autoškol • Kategorie příjemců údajů: správce + oprávněné fyzické a právnické osoby + orgány veřejné moci v rámci své působnosti • Doba uchování: po dobu života řidiče plus 1 rok po jeho úmrtí, a dále dle Spisového a skartačního řádu včetně Spisového a skartačního plánu

Evidence motorových vozidel

• Účel zpracování: evidence motorových vozidel • Kategorie osobních údajů: adresní a identifikační údaje • Kategorie subjektu údajů: zákazníci (klienti) správce • Kategorie příjemců údajů: správce + oprávněné fyzické a právnické osoby (účastníci řízení), orgány veřejné moci v rámci své působnosti• Doba uchování: 5 let po vyřazení vozidla a dále dle Spisového a skartačního řádu včetně Spisového a skartačního plánu

Povolení na provoz stanic pro měření emisí automobilů

• Účel zpracování: vydávání povolení na provoz stanic pro měření emisí automobilů dle zákona č. 56/2001 Sb., o podmínkách provozu vozidel na pozemních komunikacích ve znění pozdějších právních předpisů • Kategorie osobních údajů: adresní a identifikační údaje žadatelů o povolení

a provozovatelů stanic • Kategorie subjektu údajů: zákazníci (klienti) správce • Kategorie příjemců údajů: správce + oprávněné fyzické a právnické osoby (účastníci řízení), orgány veřejné moci v rámci své působnosti

• Doba uchování: 5 let zániku stanice a dále dle Spisového a skartačního řádu včetně Spisového a skartačního plánu

Postup podle zákona o ochraně ovzduší • Účel zpracování: postup dle zákona č. 201/2012 Sb., o ochraně ovzduší, v platném znění • Kategorie osobních údajů: adresní a identifikační údaje • Kategorie subjektu údajů: zákazníci (klienti) správce • Kategorie příjemců údajů: správce • Doba uchování: 5 let po uzavření spisu a dále dle Spisového a skartačního řádu včetně Spisového a skartačního plánu

Postup podle zákona č. 254/2001 Sb., o vodách a o změně některých zákonů (vodní zákon) v platném znění

• Účel zpracování: vedení správních řízení a další postupy podle zákona č. 254/2001 Sb., o vodách a o změně některých zákonů (vodní zákon), v platném znění • Kategorie osobních údajů: adresní a identifikační údaje • Kategorie subjektu údajů: zákazníci (klienti) správce • Kategorie příjemců údajů: správce • Doba uchování: 5 až 50 let po uzavření spisu a dále dle Spisového a skartačního řádu včetně Spisového a skartačního plánu

Vodoprávní evidence

• Účel zpracování: zpracování údajů dle zákona č. 254/2001 Sb. o vodách a o změně některých zákonů (vodní zákon), v platném znění • Kategorie osobních údajů: adresní a identifikační údaje • Kategorie subjektu údajů: zákazníci (klienti) správce • Kategorie příjemců údajů: správce • Doba uchování: 50 let po uzavření spisu a dále dle Spisového a skartačního řádu včetně Spisového a skartačního plánu

Majetková a provozní evidence vodovodů a kanalizací

• Účel zpracování: postup dle zákona č. 274/2001 Sb., o vodovodech a kanalizacích ve znění pozdějších předpisů • Kategorie osobních údajů: adresní a identifikační údaje • Kategorie subjektu údajů: vlastníci a provozovatelé vodovodů a kanalizací • Kategorie příjemců údajů: správce • Doba uchování: 10 let a dále dle Spisového a skartačního řádu včetně Spisového a skartačního plánu

Postup podle zákona č. 114/1992 Sb., o ochraně přírody a krajiny, v platném znění

• Účel zpracování: vedení správních řízení a další postupy podle zákona č. 114/1992 Sb., o ochraně přírody a krajiny, v platném znění • Kategorie osobních údajů: adresní a identifikační údaje • Kategorie

subjektu údajů: zákazníci (klienti) správce • Kategorie příjemců údajů: správce • Doba uchování: 5 let po uzavření spisu a dále dle Spisového a skartačního řádu včetně Spisového a skartačního plánu

Postup podle zákona č. 185/2001 Sb., o odpadech, v platném znění

• Účel zpracování: vedení správních řízení a další postupy podle zákona č. 185/2001 Sb., o odpadech v platném znění • Kategorie osobních údajů: adresní a identifikační údaje • Kategorie subjektu údajů: zákazníci (klienti) správce • Kategorie příjemců údajů: správce • Doba uchování: 5 let po uzavření spisu a dále dle Spisového a skartačního řádu včetně Spisového a skartačního plánu

Poskytování informací dle zákona č. 123/19989 Sb., o svobodném přístupu k informacím o životním prostředí, v platném znění

• Účel zpracování: poskytování informací občanům na základě zákona č. 123/1998 Sb., o svobodném přístupu k informacím o životním prostředí, v platném znění • Kategorie osobních údajů: adresní a identifikační údaje • Kategorie subjektu údajů: zákazníci (klienti) správce • Kategorie příjemců údajů: správce • Doba uchování: 5 let

Postup podle zákona č. 334/1992 Sb., o ochraně zemědělského půdního fondu, v platném znění

• Účel zpracování: vedení správních řízení a další postupy podle zákona č. 334/1992 Sb., o ochraně zemědělského půdního fondu, v platném znění • Kategorie osobních údajů: adresní a identifikační údaje • Kategorie subjektu údajů: zákazníci (klienti) správce • Kategorie příjemců údajů: správce • Doba uchování: 15 let po uzavření spisu a dále dle Spisového a skartačního řádu včetně Spisového a skartačního plánu

Postup podle zákona č. 246/1992 Sb., na ochranu zvířat proti týrání, v platném znění

• Účel zpracování: vedení správních řízení a další postupy podle zákona č. 246/1992 Sb., na ochranu zvířat proti týrání, v platném znění • Kategorie osobních údajů: adresní a identifikační údaje • Kategorie subjektu údajů: zákazníci (klienti) správce • Kategorie příjemců údajů: správce • Doba uchování: 5 až 10 let po uzavření spisu a dále dle Spisového a skartačního řádu včetně Spisového a skartačního plánu

Postup podle zákona č. 326/2004 Sb., o rostlinolékařské péči a o změně některých souvisejících zákonů, v platném znění:

• Účel zpracování: vedení správních řízení a další postupy dle zákona č. 326/2004 Sb., v platném znění • Kategorie osobních údajů: adresní a identifikační údaje • Kategorie subjektu údajů: zákazníci (klienti) správce • Kategorie příjemců údajů: správce • Doba uchování: 5 let a dále dle Spisového a skartačního řádu včetně Spisového a skartačního plánu

Postup podle zákona č. 99/2004 Sb., o rybníkářství, výkonu rybářského práva, rybářské stráži, ochraně mořských zdrojů rybolovných zdrojů a o změně některých zákonů (zákon o rybářství), v platném znění

• Účel zpracování: vedení správních řízení a další postupy podle zákona č. 99/2004 Sb., o rybářství, v platném znění • Kategorie osobních údajů: adresní a identifikační údaje • Kategorie subjektu údajů: zákazníci (klienti) správce • Kategorie příjemců údajů: správce • Doba uchování: 5 až 10 let po uzavření spisu a dále dle Spisového a skartačního řádu včetně Spisového a skartačního plánu

Postup podle zákona č. 289/1995 Sb., o lesích, v platném znění

• Účel zpracování: vedení správních řízení a další postupy podle zákona č. 289/1995 Sb., o lesích, v platném znění • Kategorie osobních údajů: adresní a identifikační údaje • Kategorie subjektu údajů: zákazníci (klienti) správce • Kategorie příjemců údajů: správce • Doba uchování: 5 až 10 let po uzavření spisu a dále dle Spisového a skartačního řádu včetně Spisového a skartačního plánu

Postup podle zákona č. 149/2003 Sb., o obchodu s reprodukčním materiálem lesních dřevin, v platném znění

• Účel zpracování: vedení správních řízení a další postupy podle zákona č. 289/1995 Sb., o lesích, v platném znění • Kategorie osobních údajů: adresní a identifikační údaje • Kategorie subjektu údajů: zákazníci (klienti) správce • Kategorie příjemců údajů: správce • Doba uchování: 5 až 10 let po uzavření spisu a dále dle Spisového a skartačního řádu včetně Spisového a skartačního plánu

Postup podle zákona č. 449/2001 Sb., o myslivosti, v platném znění

• Účel zpracování: vedení správních řízení a další postupy podle zákona č. 449/2001 Sb., o myslivosti, v platném znění. • Kategorie osobních údajů: adresní a identifikační údaje • Kategorie subjektu údajů: zákazníci (klienti) správce • Kategorie příjemců údajů: správce • Doba uchování: 5 až 10 let po uzavření spisu a dále dle Spisového a skartačního řádu včetně Spisového a skartačního plánu

Řízení vedená podle zákona č. /2006 Sb., zákon o územním plánování a stavebním řádu (stavební zákon)ve znění pozdějších předpisů

• Účel zpracování: regulace stavební činnosti - vedení správních řízení podle zákona č. 183/2006 Sb., zákon o územním plánování a stavebním řádu (stavební zákon), ve znění pozdějších předpisů s fyzickými i právnickými osobami • Kategorie osobních údajů: adresní a identifikační údaje • Kategorie subjektu údajů: zákazníci (klienti) správce • Kategorie příjemců údajů: správce • Doba uchování: trvale - po dobu existence stavby a po jejím odstranění 20 let a dále dle Spisového a skartačního řádu včetně Spisového a skartačního plánu

Přidělování čísel popisných a evidenčních

• Účel zpracování: označování číslování budov dle zákona č. 128/2000 Sb., o obcích (obecní zřízení), ve znění pozdějších předpisů • Kategorie osobních údajů: adresní a identifikační údaje • Kategorie subjektu údajů: zákazníci (klienti) správce • Kategorie příjemců údajů: správce • Doba uchování: po dobu existence budovy

Obecní živnostenský úřad

• Účel zpracování: postupy ve věcech dle zákona č. 455/1991 Sb., o živnostenském podnikání, ve znění pozdějších předpisů • Kategorie osobních údajů: adresní a identifikační údaje • Kategorie subjektu údajů: osoby s jiným vztahem ke správci, zákazníci (klienti) správce • Kategorie příjemců údajů: správce • Doba uchování: 10 let a dále dle Spisového a skartačního řádu včetně Spisového a skartačního plánu

Evidence zemědělských podnikatelů

• Účel zpracování: vydávání osvědčení o zápisu do evidence zemědělského podnikatele nebo vyřazení z evidence zemědělského podnikatele podle zákona č. 252/1997 Sb., o zemědělství, ve znění pozdějších předpisů • Kategorie osobních údajů: adresní a identifikační údaje • Kategorie subjektu údajů: osoby s jiným vztahem ke správci, zákazníci (klienti) správce • Kategorie příjemců údajů: správce • Doba uchování: 10 let a dále dle Spisového a skartačního řádu včetně Spisového a skartačního plánu

Agenda trhů a tržních prodejů

• Účel zpracování: pro organizaci a řízení trhů a tržních akcí • Kategorie osobních údajů: adresní a identifikační údaje • Kategorie subjektu údajů: osoby s jiným vztahem ke správci, zákazníci (klienti) správce • Kategorie příjemců údajů: správce • Doba uchování: 5 let a dále dle Spisového a skartačního řádu včetně Spisového a skartačního plánu

Sociální kuratela

• Účel zpracování: péče o osoby ohrožené sociálním vyloučením z důvodu předchozí ústavní nebo ochranné výchovy nebo výkonu trestu, osoby, jejichž práva a zájmy jsou ohroženy trestnou činností jiné osoby, a osoby, jejichž způsob života může vést ke konfliktu se společností zákon č. 108/2006 Sb., o sociálních službách, zákon č. 111/2006 Sb., - o pomoci v hmotné nouzi; zákon č. 110/2006 Sb., o existenčním minimu; zákon č. 169/1999 Sb. o výkonu trestu odnětí svobody; zákon č. 345/1999 Sb., řád výkonu trestu odnětí svobody; zákon č. 293/1993 Sb., o výkonu vazby; zákon č. 109/1999 Sb., řád výkonu vazby; zákon č. 129/2008 Sb., o výkonu zabezpečovací detence; v platném znění • Kategorie osobních údajů: adresní a identifikační údaje (zvláštní kategorie údajů: trestná činnost, informace týkající se umístění v institucionální péči - ústavní a ochranná výchova, výkon vazby a výkon trestu, výkon zabezpečovací detence, jiné osobní údaje), jiné osobní údaje • Kategorie subjektu údajů: zákazníci (klienti) správce • Kategorie příjemců údajů: správce, oznamovatel, oprávněné fyzické

a právnické osoby, orgány veřejné moci v rámci • Doba uchování: 5 let a dále dle Spisového a skartačního řádu včetně Spisového a skartačního plánu

Sociálně-právní ochrana dětí

• Účel zpracování: agenda vedená dle zákona č. 359/1999 Sb., o sociálně-právní ochraně dětí, v platném znění • Kategorie osobních údajů: adresní a identifikační údaje, zvláštní kategorie údajů, jiné osobní údaje • Kategorie subjektů údajů: zákazníci (klienti) správce, osoby s jiným vztahem k oznamovateli, osoby bez vztahu k oznamovateli • Kategorie příjemců údajů: správce, oznamovatel, oprávněné fyzické a právnické osoby, orgány veřejné moci v rámci • Doba uchování: 15 let a dále dle Spisového a skartačního řádu včetně Spisového a skartačního plánu

Sociální práce

• Účel zpracování: agenda vedená dle zákona č. 111/2006 Sb., o pomoci v hmotné nouzi, v platném znění a zákona č. 108/2006 Sb., o sociálních službách, v platném znění • Kategorie osobních údajů: adresní a identifikační údaje, citlivé osobní údaje • Kategorie subjektů údajů: zákazníci (klienti) správce • Kategorie příjemců údajů: správce, oznamovatel, oprávněné fyzické a právnické osoby, orgány veřejné moci v rámci • Doba uchování: 10 let a dále dle Spisového a skartačního řádu včetně Spisového a skartačního plánu

Zvláštní příjemce dávek důchodového pojištění

• Účel zpracování: agenda vedená dle zákona č. 582/1991 Sb., o organizaci a provádění sociálního zabezpečení, v platném znění • Kategorie osobních údajů: identifikační a adresné údaje • Kategorie subjektů údajů: zákazníci (klienti) správce, osoby s jiným vztahem k oznamovateli • Kategorie příjemců údajů: oznamovatel, oprávněné fyzické a právnické osoby, orgány veřejné moci v rámci • Doba uchování: 10 let a dále dle Spisového a skartačního řádu včetně Spisového a skartačního plánu

Parkovací průkazy

• Účel zpracování: agenda vedená dle zákona č. 361/2000 Sb., o provozu na pozemních komunikacích, v platném znění • Kategorie osobních údajů: adresní a identifikační údaje • Kategorie subjektů údajů: zákazníci (klienti) správce • Kategorie příjemců údajů: správce, oznamovatel • Doba uchování: 10 let a dále dle Spisového a skartačního řádu včetně Spisového a skartačního plánu

Veřejné opatrovnictví

• Účel zpracování: agenda veřejného opatrovnictví u osob omezených ve svéprávnosti, vedená podle zákona č. 89/2012 Sb., občanský zákoník, v platném znění • Kategorie osobních údajů: adresní a identifikační údaje, zvláštní kategorie údajů, jiné osobní údaje • Kategorie subjektů údajů: zákazníci

(klienti) správce, osoby s jiným vztahem k oznamovateli • Kategorie příjemců údajů: správce, oznamovatel, jiní příjemci (právnické a fyzické osoby v ČR) • Doba uchování: 5 let a dále dle Spisového a skartačního řádu včetně Spisového a skartačního plánu

Zástup při uzavírání smluv o poskytování sociální služby

• Účel zpracování: agenda vedená dle zákona č. 108/2006 Sb., o sociálních službách, v platném znění • Kategorie osobních údajů: adresní a identifikační údaje • Kategorie subjektů údajů: zákazníci (klienti) správce • Kategorie příjemců údajů: správce, oznamovatel, jiní příjemci (právnické a fyzické osoby ČR) • Doba uchování: 10 let a dále dle Spisového a skartačního řádu včetně Spisového a skartačního plánu

Sociální pohřby

• Účel zpracování: agenda vedená na základě zákona č. 256/2001 Sb., o pohřebnictví, v platném znění • Kategorie osobních údajů: adresní a identifikační údaje • Kategorie subjektů údajů: osoby s jiným vztahem k oznamovateli • Kategorie příjemců údajů: správce, jiní příjemci (právnické osoby ČR, fyzické osoby ČR) • Doba uchování: 5 let a dále dle Spisového a skartačního řádu včetně Spisového a skartačního plánu

Stanovení úhrady za stravu a péči

• Účel zpracování: agenda vedená na základě zákona č. 108/2006 Sb., o sociálních službách, v platném znění • Kategorie osobních údajů: adresní a identifikační údaje • Kategorie subjektů údajů: zákazníci (klienti) správce, členové oznamovatele • Kategorie příjemců údajů: správce, klienti správce, právnické nebo fyzické osoby v ČR • Doba uchování: 5 let a dále dle Spisového a skartačního řádu včetně Spisového a skartačního plánu

Nálezy věcí a zvířat

• Účel zpracování: evidence a přihlášení nálezu věci nebo zvířete dle zákona č. 89/2012 Sb., občanský zákoník, v platném znění • Kategorie osobních údajů: adresní a identifikační údaje • Kategorie subjektu údajů: zákazníci (klienti) správce • Kategorie příjemců údajů: správce • Doba uchování: 3 roky a dále dle Spisového a skartačního řádu včetně Spisového a skartačního plánu

Zpracování případů protiprávního jednání

• Účel zpracování: řešení přestupků a zpracování podkladů pro příslušné orgány, dle č. 250/2016 Sb. Zákon o odpovědnosti za přestupky a řízení o nich a dle zákona č. 251/2016 Sb. o některých přestupcích a dle zákona č. 553/1991 Sb., o obecní policii, v platném znění • Kategorie osobních údajů: adresní a identifikační údaje; zvláštní kategorie údajů – přestupkové jednání, údaje o správním trestání • Kategorie subjektu údajů: zákazníci (klienti) správce • Kategorie příjemců údajů: správce, oprávněné

fyzické a právnické osoby, orgány veřejné moci v rámci • Doba uchování: 3 roky a dále dle Spisového a skartačního řádu včetně Spisového a skartačního plánu

Pořizování obrazových a zvukových záznamů z veřejných prostranství a zákroků

• Účel zpracování: dokladování protiprávního jednání, prevence, identifikace osob, dle § 24b zákona č. 553/1991 Sb., o obecní policii, v platném znění • Kategorie osobních údajů: adresní a identifikační údaje; zvláštní kategorie údajů – přestupkové jednání, údaje o správním trestání • Kategorie subjektu údajů: zákazníci (klienti) správce • Kategorie příjemců údajů: správce + oprávněné fyzické a právnické osoby, orgány veřejné moci v rámci • Doba uchování: 1 měsíc a dále dle Spisového a skartačního řádu včetně Spisového a skartačního plánu

Oznámení od občanů (veřejnosti)

• Účel zpracování: evidence oznámení (podnětů) od občanů, dle zákona č. 553/1991 Sb., o obecní policii, v platném znění • Kategorie osobních údajů: adresní a identifikační údaje • Kategorie subjektu údajů: zákazníci (klienti) správce • Kategorie příjemců údajů: správce + oprávněné fyzické a právnické osoby, orgány veřejné moci v rámci • Doba uchování: 3 roky a dále dle Spisového a skartačního řádu včetně Spisového a skartačního plánu

Zjišťování totožnosti osoby při právním zájmu jiného občana

• Účel zpracování: poskytnutí totožnosti osoby při právním zájmu další osoby, dle §12 odst. 2 písm. e), f) zákona č. 553/1991 Sb., o obecní policii, v platném znění • Kategorie osobních údajů: adresní a identifikační údaje • Kategorie subjektu údajů: zákazníci (klienti) správce • Kategorie příjemců údajů: správce, fyzická osoba v ČR i v zahraničí • Doba uchování: 3 roky a dále dle Spisového a skartačního řádu včetně Spisového a skartačního plánu

Žádosti o podání vysvětlení od občana

• Účel zpracování: využití oprávnění požadovat vysvětlení, dle §12 odst. 2 písm. c) zákona č. 553/1991 Sb., o obecní policii, v platném znění • Kategorie osobních údajů: adresní a identifikační údaje; zvláštní kategorie údajů – trestná činnost • Kategorie subjektu údajů: zákazníci (klienti) správce • Kategorie příjemců údajů: správce + oprávněné fyzické a právnické osoby, orgány veřejné moci v rámci • Doba uchování: 3 let a dále dle Spisového a skartačního řádu včetně Spisového a skartačního plánu

Hlášení pobytu obyvatel

• Účel zpracování: evidence, přihlášení, změny a zrušení trvalého pobytu • Kategorie osobních údajů: adresní a identifikační údaje • Kategorie subjektu údajů: zákazníci (klienti) správce • Kategorie příjemců údajů: správce + oprávněné fyzické a právnické osoby, orgány veřejné moci v rámci • Doba uchování: 50 let, u poskytnutí údajů z informačního systému EO 5 let a dále dle Spisového a skartačního řádu včetně Spisového a skartačního plánu

Matrika

• Účel zpracování: vedení matrik, změny jména a příjmení • Kategorie osobních údajů: adresní a identifikační údaje • Kategorie subjektu údajů: zákazníci (klienti) správce • Kategorie příjemců údajů: správce + oprávněné fyzické a právnické osoby, orgány veřejné moci i • Doba uchování: narození – 100 let, manželství, úmrtí – 75 let, změna jména a příjmení 10 let a dále dle Spisového a skartačního řádu včetně Spisového a skartačního plánu

Volební agenda - volební seznamy

• Účel zpracování: stálý seznam voličů, zvláštní seznam voličů, registrace kandidátů v případě komunálních a senátních voleb • Kategorie osobních údajů: adresní a identifikační údaje • Kategorie subjektu údajů: zákazníci (klienti) správce • Kategorie příjemců údajů: správce • Doba uchování: seznam voličů: stále - seznam je průběžně aktualizován, registrace kandidátů: 10 let a dále dle Spisového a skartačního řádu včetně Spisového a skartačního plánu

Volební agenda - Okrskové volební komise

• Účel zpracování: zajištění voleb • Kategorie osobních údajů: adresní a identifikační údaje • Kategorie subjektu údajů: osoby s jiným vztahem k oznamovateli • Kategorie příjemců údajů: správce • Doba uchování: 5 let a dále dle Spisového a skartačního řádu včetně Spisového a skartačního plánu

Volební agenda - Vydávání voličských průkazů

• Účel zpracování: zajištění voleb - vydávání voličských průkazů • Kategorie osobních údajů: adresní a identifikační údaje • Kategorie subjektu údajů: zákazníci (klienti) správce • Kategorie příjemců údajů: správce • Doba uchování: 5 let a dále dle Spisového a skartačního řádu včetně Spisového a skartačního plánu

Postup podle zákona č. 111/1994 Sb., o silniční dopravě, v platném znění

• Účel zpracování: postup podle zákona č. 111/1994 Sb., o silniční dopravě, v platném znění • Kategorie osobních údajů: adresní a identifikační údaje • Kategorie subjektu údajů: zákazníci (klienti)

správce • Kategorie příjemců údajů: správce • Doba uchování: 5 až 15 let po uzavření spisu a dále dle Spisového a skartačního řádu včetně Spisového a skartačního plánu

Centrální registr dopravců (CRD)

• Účel zpracování: zpracování údajů dle zákona č. 111/1994 Sb., o silniční dopravě v platném znění • Kategorie osobních údajů: adresní a identifikační údaje • Kategorie subjektu údajů: zákazníci (klienti) správce • Kategorie příjemců údajů: správce • Doba uchování: po dobu platnosti oprávnění k podnikání

Postup podle zákona č. 361/2000 Sb., o provozu na pozemních komunikacích, v platném znění

• Účel zpracování: vedení správních řízení a další postupy podle zákona č. 361/2000 Sb., o provozu na pozemních komunikacích, v platném znění, v platném znění, včetně vydávání výjimek z dopravního značení a stanovování jak přechodnou, tak místní úpravy provozu • Kategorie osobních údajů: adresní a identifikační údaje • Kategorie subjektu údajů: zákazníci (klienti) správce • Kategorie příjemců údajů: správce • Doba uchování: po dobu existence stavby a po jejím odstranění dvacet let a dále dle Spisového a skartačního řádu včetně Spisového a skartačního plánu

Soudní řízení

• Účel zpracování: sporná a nesporná řízení před soudy, návrhy, žaloby, exekuce, odvolání • Kategorie osobních údajů: adresní a identifikační údaje • Kategorie subjektu údajů: zákazníci (klienti) správce • Kategorie příjemců údajů: správce + oprávněné fyzické a právnické osoby, orgány veřejné moci • Doba uchování: 10 let a dále dle Spisového a skartačního řádu včetně Spisového a skartačního plánu

Smlouvy o kulturním vystoupení, o spolupráci, o dílo, o vytvoření díla

• Účel zpracování: smlouvy o kulturním vystoupení, smlouvy o spolupráci, smlouvy o dílo, smlouvy o vytvoření díla a jeho dalším užití, zákon č. 121/2000 Sb., autorský zákon v platném znění • Kategorie osobních údajů: adresní a identifikační údaje • Kategorie subjektu údajů: zákazníci (klienti) správce • Kategorie příjemců údajů: správce • Doba uchování: 5 let

Smlouvy, jejichž předmětem jsou majetkoprávní dispozice s majetkem města - nájemní, pachtovní, kupní, darovací, směnné, o výpůjčce a jiné

• Účel zpracování: realizace majetkoprávních dispozic s majetkem obce v souladu se specifickými zákonnými požadavky, administrace žádostí o uzavření smlouvy • Kategorie osobních údajů: adresní a identifikační údaje • Kategorie subjektu údajů: zákazníci (klienti) správce • Kategorie příjemců údajů: správce, oprávněné fyzické a právnické osoby, orgány veřejné moci • Doba uchování: 10 let a dále dle Spisového a skartačního řádu včetně Spisového a skartačního plánu

Výkon práva shromažďovacího

• Účel zpracování: zajištění možnosti výkonu shromažďovacího práva dle zákona č. 84/1990 Sb. o právu shromažďovacím, vedení seznamu svolavatelů shromáždění • Kategorie osobních údajů: adresní a identifikační údaje • Kategorie subjektu údajů: svolavatelé shromáždění • Kategorie příjemců údajů: správce • Doba uchování: 5 let a dále dle Spisového a skartačního řádu včetně Spisového a skartačního plánu

Spisová služba

• Účel zpracování: zajištění výkonu spisové služby dle zákona č. 499/2004 Sb., o archivnictví a spisové službě a o změně některých zákonů, ve znění pozdějších předpisů • Kategorie osobních údajů: adresní a identifikační údaje • Kategorie subjektu údajů: fyzické a právnické osoby • Kategorie příjemců údajů: správce • Doba uchování: 5 let a dále dle Spisového a skartačního řádu včetně Spisového a skartačního plánu

Veřejnoprávní smlouva o poskytnutí účelové dotace z rozpočtu města Příbram

• Účel zpracování: veřejnoprávní smlouva o poskytnutí účelové dotace z rozpočtu města Příbram podle zákona č. 250/2000 Sb., o rozpočtových pravidlech územních rozpočtů a podle zákona č. 89/2012 Sb., občanský zákoník • Kategorie osobních údajů: adresní a identifikační údaje • Kategorie subjektu údajů: zákazníci (klienti) správce • Kategorie příjemců údajů: správce • Doba uchování: 5 let a dále dle Spisového a skartačního řádu včetně Spisového a skartačního plánu

Systém prostupného bydlení (sociální bydlení)

• Účel zpracování: žádosti a jejich administrace podle „Směrnice Města Příbram č.1/2018/MěÚ Pravidla pro pronájem a směnu bytů ve vlastnictví města Příbram“ na základě zákona č. 128/2000 Sb., o obcích • Kategorie osobních údajů: adresní a identifikační údaje, zvláštní kategorie údajů, jiné osobní údaje • Kategorie subjektu údajů: zákazníci (klienti) správce • Kategorie příjemců údajů: správce • Doba uchování: 10 let a

Bytové domy zvláštního určení (DPS, KoDuS)

• Účel zpracování: žádosti a jejich administrace podle „Směrnice Města Příbram č.1/2018/MěÚ Pravidla pro pronájem a směnu bytů ve vlastnictví města Příbram“ na základě zákona č. 128/2000 Sb., o obcích • Kategorie osobních údajů: adresní a identifikační údaje, zvláštní kategorie údajů, jiné osobní údaje • Kategorie subjektu údajů: zákazníci (klienti) správce • Kategorie příjemců údajů: správce • Doba uchování: 10 let

Evidence a hlášení pracovních úrazů

• Účel zpracování:stanovený postup dle zákona č. 262/2006 Sb., zákoník práce, v platném znění, nařízení vlády č. 201/2010 Sb., v platném znění • Kategorie osobních údajů: adresní a identifikační údaje, zvláštní kategorie údajů – zdravotní stav, lékařské zprávy • Kategorie subjektů údajů: zaměstnanci správce a osoby s jiným vztahem ke správci • Kategorie příjemců údajů: správce a oprávněné orgány • Doba uchování: 10 let a dále dle spisového a skartačního řádu

Jednotky požární ochrany

• Účel zpracování: stanovený postup dle zákona č. 262/2006 Sb., zákoník práce, v platném znění, zajištění pracovně právních vztahů • Kategorie osobních údajů: adresní a identifikační údaje, zvláštní kategorie údajů -zdravotní a profesní způsobilost • Kategorie subjektů údajů: zaměstnanci • Kategorie příjemců údajů: správce, HZS ČR • Doba uchování: 5 let a dále dle spisového a skartačního řádu

Pověřenec pro ochranu osobních údajů čili DPO

Správce OÚ zřídil funkci Pověřence pro ochranu osobních údajů (dále jen „pověřenec“/“DPO“). Kontakty na pověřence jsou zveřejněny na www.pribram.eu.

Aktualizace

Toto informační memorandum průběžně kontrolujeme a můžeme jej příležitostně měnit (především aby byl dodržen soulad s právními předpisy a postupy ochrany osobních údajů).

Poslední změna byla provedena dne

13. VZOR Technické požadavky na SW

13.1 Dopad GDPR na stávající software

V souvislosti s novými právy subjektů osobních údajů vznikly Správci OÚ nové povinnosti. Na tyto povinnosti musí výrobci a dodavatelé softwarů reagovat a implementovat ve svých softwarech požadavky GDPR.

Dále jsou uvedeny minimální technické požadavky na software používané Správcem OÚ, jejichž splnění je nezbytné k tomu, aby Správce byl schopen dostát svým povinnostem, vyplývajícím z GDPR.

Zapracování minimálně uvedených technických požadavků Správce projedná s dodavatelem software a vhodnou formou (prohlášením výrobce, dodatkem ke smlouvě, změnou obchodních podmínek a podobně) zajistí jejich realizaci.

Protože Správce OÚ má povinnost dokladovat Úřadu pro ochranu osobních údajů, že zpracování probíhá v souladu s GDPR, je vhodné, aby Správce OÚ ve spolupráci se svým DPO splnění technických požadavků zajistil smluvně a jejich funkčnost ověřoval.

13.2 Technické požadavky na úpravu software

13.2.1 Vymazání osobních údajů

Ve všech případech, kdy dochází k vymazání osobních údajů (zejména v případech, když pominul účel zpracování, kdy je to nařízeno zákonem nebo když subjekt údajů úspěšně uplatnil právo na výmaz), je nutno:

- veškeré údaje, které jsou předmětem výmazu, trvale a neobnovitelně smazat, případně nevratně anonymizovat;
- pro účely evidence a dokladování, založit záznam o tom, kdy a v jakém rozsahu byly údaje vymazány (anonymizovány).

13.2.2 Omezení zpracování osobních údajů

Ve všech případech, kdy dochází k omezení zpracování osobních údajů (zejména v případech, když pominul nebo se zúžil účel zpracování, kdy je to nařízeno zákonem nebo když subjekt údajů úspěšně uplatnil námitku založenou na oprávněném zájmu), je nutno:

- veškeré údaje, jejichž zpracování je třeba omezit, trvale a neobnovitelně smazat, případně nevratně anonymizovat;
- pro účely evidence a dokladování, založit záznam o tom, kdy a v jakém rozsahu bylo zpracování osobních údajů omezeno (anonymizovány).

13.2.3 Přenositelnost osobních údajů

Ve všech případech, kdy má subjekt právo na přenositelnost osobních údajů (zejména v případech, kdy údaje poskytl správci sám subjekt údajů a současně zpracování je založeno na souhlasu či smlouvě), je nutno:

- veškeré údaje, které jsou předmětem předání, poskytnout ve strukturovaném a běžně používaném elektronickém formátu (například XML, JSON či jiném), s možností uložení na vhodné záznamové médium;
- pro účely evidence a dokladování, založit záznam o tom, kdy a v jakém rozsahu byly údaje exportovány;

13.2.4 Zamezení automatizovaného rozhodování

Ve všech případech, kdy dochází k automatizovanému rozhodování, které má či může mít právní a nebo obdobné důsledky (neuzavření smlouvy, stanovení úrokové sazby u úvěru), není použití plně automatizovaného rozhodování dovoleno. Výjimky jsou možné, pokud je to nezbytné k uzavření nebo plnění smlouvy, pokud je to dovolené zákonem anebo pokud subjekt údajů dá výslovný souhlas:

- ve všech případech, kdy plně automatizované zpracování není dovoleno, je nutno buď umožnit ruční vstup do rozhodovacího procesu, nebo změnit algoritmus zpracování;
- pro účely evidence a dokladování, založit záznam o tom, kdy a v jakém rozsahu byly údaje zpracovány ručně;

13.2.5 Logování přístupů

Přestože to GDPR přímo nenařizuje, v zájmu všeobecné prevence kybernetické bezpečnosti je vhodné:

- pro účely evidence a dokladování, vytvářet a ukládat záznamy o tom, kdo a kdy přistupoval k osobním údajům osob, zejména pak ke zvláštním kategoriím osobních údajů.

14. METODICKÝ POSTUP PŘI UPLATNĚNÍ PRÁV OBČANŮ

14.1 Uplatnění práv občanů podle GDPR

Podání by měla přicházet standardní cestou, například přes podatelnu a měla by obsahovat alespoň základní údaje (např. kdo, co a kdy žádá). Pokud podání jde nestandardní cestou (např. při osobním jednání), je třeba o uplatnění práva sepsat stručný zápis aby bylo možno doložit, že podání bylo vyřízeno včas. Podání se běžným postupem doručí vedoucímu odboru, kterého se věc týká.

14.2 Práva podle GDPR

Vedoucí odboru v první řadě určí, o jaké právo subjektu se jedná. Podle GDPR může subjekt uplatnit následující práva:

1. **Právo na informace, přístup k osobním údajům a na jejich opravu.** Nejčastěji půjde o dotaz, jaké údaje, proč a po jakou dobu úřad o subjektu shromažďuje. Většinou postačí odkaz na informační memorandum na https://pribram.eu/mesto-pribram/OchranaOU.html. Pokud subjekt chce znát konkrétní obsah údajů o sobě, je potřeba mu vyhovět. V případě, že požaduje provést opravu, nezapomeňte opravu provést jak v elektronické, tak i v listinné dokumentaci. V každém případě je potřeba stručně zaznamenat, jak a kdy bylo podání vyřízeno (kvůli pozdějšímu dokazování).
2. **Právo na výmaz („právo být zapomenut“)**. Toto právo může subjekt uplatnit jen v určitých konkrétních případech, zejména:
   (a) když subjekt údajů odvolal svůj souhlas a neexistuje žádný další právní důvod pro zpracování,
   (b) když subjekt údajů vznesl námitky proti „zpracování na základě oprávněného zájmu“ a jeho námitce bylo vyhověno,
   (c) když osobní údaje musí být vymazány ke splnění právní povinnosti.

   V ostatních případech se OÚ zpravidla nevymazávají. Zejména je **nelze vymazat**, když jsou údaje nezbytné ke splnění zákonné povinnosti, pro výkon práva na svobodu projevu a informace, z důvodu veřejného zájmu na ochranu zdraví, z důvodu archivace, pro určení, výkon nebo obhajobu právních nároků.

Vedle toho samozřejmě nastává také automatické vymazávání osobních údajů vždy, když osobní údaje již nejsou potřebné pro účely, pro které byly shromážděny nebo jinak zpracovány – toto je řízeno Spisovým a skartačním řádem.

3. **Právo na omezení zpracování**. Někdy je možno se subjektem dohodnout, že osobní údaje, které by správně měly být vymazány, ve skutečnosti vymazány nebudou, ale jen bude omezen přístup k nim. Takovým omezením například může být, že spis se zapečetí a uloží na vhodné místo u vedoucího. Využití práva na omezení zpracování je spíše výjimečné a přísně individuální. V každém případě je nutno zaznamenat souhlas subjektu.
4. **Právo vznést námitku**. Subjekt může vznést námitku proti zpracování, ale výlučně jen v případě, že je zpracování nezbytné pro účely oprávněných zájmů příslušného správce či třetí strany. **V ostatních případech subjekt není oprávněn vznést námitku**.
5. **Právo na přenositelnost**. Tímto právem se myslí, že subjekt má právo, aby mu MěÚ zadarmo (!) nakopíroval na vhodné médium (CD, USB flash paměť apod.) osobní údaje, které o něm zpracovává. Toto právo ovšem lze uplatnit pouze v případě, že jsou současně splněny dvě následující podmínky.

   Musí platit tyto dvě podmínky současně:

   (a) zpracování musí být založené na právním důvodu „souhlas“ nebo „smlouva“,

   (b) zpracování se musí provádět automatizovaně.

   V podmínkách MěÚ to připadá v úvahu jen naprosto výjimečně, protože se agendy zpracovávají ručně, nanejvýš semiautomaticky.
6. **Právo nebýt předmětem automatizovaného zpracování**. Z výše uvedeného důvodu prakticky nepřichází v úvahu.
7. **Právo na stížnost dozorovému úřadu, na žalobu (vůči dozorovému úřadu/ správci nebo zpracovateli)**. Tato práva jsou natolik speciální a současně nebezpečná, že by je žádný vedoucí neměl řešit bez spolupráce s právníkem a DPO.

14.3 Řešení

Pokud subjekt uplatní některé ze svých práv, vedoucí odboru případ vyřeší v pracovním pořádku. V každém případě je potřeba o řešení provést nějakou formu záznamu.

14.4 Zásadní doporučení

V případě, že vedoucí bude mít jakékoliv pochybnosti, nejistotu nebo si jen bude chtít ověřit správnost svého postupu, může kontaktovat **pověřence pro ochranu osobních údajů** (aktuální kontakt je uveden na https://pribram.eu/mestsky-urad/kontakty-meu/ing-barbora-bahnikova.html) a postupovat v souladu s jeho doporučením.

PŘÍLOHY

15. PŘEHLED POUŽITÝCH ZNAČEK A ZKRATEK

AIS	Agendový informační systém
ČR	Česká republika
ČSN	Česká státní norma
DDoS	Distributed Denial of Service
DLP	Data loss protection
DMZ	Demilitarized Zone
ESLP	Evropský soud pro lidská práva
EU	Evropská unie
FDE	Full Disk Encryption
FES	File Encryption System
GDPR	Nařízení Evropského parlamentu a Rady EU 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)
GPS	Global Positioning System
HTTPS	Zabezpečený Hypertext Transfer Protocol
IDS	Intruder Detection Systems
IP	Internet Protocol
IPS	Intrusion Prevention Systems
IPsec	IP security
IS	Informační systém
ISVS	Informační systém veřejné správy
IT	Informační technologie
ITIL	IT infrastructure Library
LAN	Local Area Network
MAC	Media Access Control
MDM	Mobile Device Management
OÚ	Osobní údaje
PIN	Personal Identification Number
Rada	Rada Evropské unie
SIEM	Security Information and Event Management
SIM	Subscriber Identity Module

SSL	Secure Socket Layer
SÚ	Subjekt údajů
ÚOOÚ	Úřad pro ochranu osobních údajů
ÚS	Ústavní soud
USB	Universal Serial Bus
WPA2	Wi-Fi Protected Access verze 2
WP29	Pracovní skupina zřízená podle článku 29 směrnice 95/46/ES
ZKB	Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších přepisů (také jako „zákon o kybernetické bezpečnosti)

16. FORMULÁŘE

16.1 Formulář F01

Oblast	Příklad zjištění	Poznámka
V jakých procesech jsou získávány OÚ?	Všechny agendy odboru ve vztahu k občanům. OÚ občanů - dle požadavků zákonů. Nejsou shromažďovány OÚ u agend zajišťujících chod úřadu.	Živnostenský úřad výkon jednotlivých agend dle zák. č. 455/1991 Sb.
Kde probíhá shromažďování a zpracovávání OÚ? Centrálně, pobočky atd.? Jak organizace vypadá?	Vše je na jednom místě. OÚ se nikam neexportují, kromě zákonných povinností (přenesená působnost).	Živnostenský úřad - pracoviště slouží jako centrální registrační místo.
Je definována zodpovědnost za ochranu OÚ? Je řešeno v pracovní smlouvě nebo nějakou doložkou?	Není explicitně definováno, je dáno požadavkem mlčenlivosti úředníka. Požadavek mlčenlivosti je součástí pracovní smlouvy.	Minimálně dle zákona č. 312/2002 Sb. §16odst. 1 písm. j
Shromažďujete a zpracováváte OÚ jen občanů ČR nebo i jiných zemí EU?	I z jiných zemí EU, zejména v případě agendy Živnostenského úřadu.	
Předáváte nějaké OÚ do zahraničí? Kam, komu, důvod?	Ne, není důvod.	
V jaké podobě jsou shromažďovány jednotlivé OÚ jednotlivými odděleními / organizačními jednotkami?	V listinné podobě, ale i elektronicky.	
Jaké jsou důvody pro shromažďování OÚ?	Jsou definovány zákony nebo potřebou naplnit smlouvu.	Živnostenský úřad dle zák. č. 455/1991 Sb. Jsou používány formuláře MPO.
Jsou shromažďovány OÚ, "protože by se mohly někdy hodit"?	Nejsou, všechny OÚ by měly mít stanovený důvod.	
Jsou shromažďovány OÚ zvláštní kategorie? Pokud ano důvod?	Ne.	
Jsou shromažďovány OÚ zvláštní kategorie? Pokud ano jaké?	Ne.	
Je shromažďování OÚ vyžadováno zákonem nebo právem ČR nebo EU?	Ano.	
Je získáván souhlas se shromažďováním OÚ?	Ne není.	Souhlas je získáván v případě pořizování fotografií a jejich publikace např. vítání občánků.
Jakým způsobem je získáván souhlas ke shromažďování jednotlivých OÚ jednotlivými	Není získáván.	U výše uvedených fotografií neformalizovaný způsob,

Oblast	Příklad zjištění	Poznámka
odděleními/organizačními jednotkami? Popis.		není postup pro uchování souhlasu.
Získáváte OÚ i z jiných zdrojů (komerčně nabízené databáze atd.)? Jakým způsobem jsou subjekty informovány?	Ne jen a pouze z veřejně dostupných zdrojů. Nejsou pořizovány komerční databáze.	
Jakým způsobem jsou jednotlivé OÚ jednotlivými odděleními/organizačními jednotkami ukládány? Popis. Dochází ke spojování informací získaných za různým účelem?	Ukládání v rámci aplikace, databáze, pošta a souborový systém. Ano informace se spojují.	
Jsou OÚ nějak klasifikovány? Jsou OÚ vůbec nějak označovány?	Není prováděna klasifikace dat a informací, která by umožňovala následně nastavovat bezpečnostní opatření.	Riziko ohledně GDPR!
Je pro každý jednotlivý případ u jednotlivých oddělení/organizačních jednotek definován účel shromáždění OÚ?	Ano, ale není formalizováno.	Riziko ohledně GDPR!
Je pro každý jednotlivý případ u jednotlivých oddělení/organizačních jednotek definována doba shromáždění a zpracování OÚ? Jak dlouho jsou drženy?	Jsou dodržovány lhůty ze zákona.	
Je subjekt OÚ informován o shromažďování OÚ? Zná subjekt účel zpracování a dobu, po kterou budou OÚ zpracovávány?	Ano, není však formalizováno. Předpokládá se, že subjekt má povědomí o účelech shromažďování OÚ.	Riziko ohledně GDPR!
Jakým způsobem je subjekt OÚ informován o shromažďování OÚ?	Předpokládá se, že subjekt má povědomí o účelech shromažďování OÚ. Základní informace o zpracování OÚ v pracovní smlouvě, dohodách o pracích konaných mimo pracovní poměr.	Riziko ohledně GDPR!
Jakým způsobem se provádí na jednotlivých odděleních/organizačních jednotkách aktualizace a upřesňování OÚ?	Aktivně není prováděno.	
Mají subjekty možnost získat přístup ke svým OÚ? Náhled co se zpracovává a jak, kopie zpracovávaných OÚ?	Není proces a není tedy postup.	Riziko ohledně GDPR!

Oblast	Příklad zjištění	Poznámka
Může subjekt vznést námitku proti shromažďování a zpracovávání dat? Co se stane? Má to nějaký dopad?	Není stanoven proces a postup - ad hoc.	Riziko ohledně GDPR!
Jakým způsobem může subjekt vznést námitku proti shromažďování a zpracovávání dat? Popis, technologie, postup.	Není stanoven proces a postup - ad hoc.	Riziko ohledně GDPR!
Existuje politika/směrnice pro uchovávání a mazání OÚ?	Není definován způsob a popis vlastní skartace.	Riziko ohledně GDPR!
Jsou definovány bezpečnostní incidenty? Existuje politika/směrnice pro řízení bezpečnostních incidentů? Vznikají záznamy řízení incidentů? Je možné nějaký takový záznam získat/vidět?	Není momentálně nic takového. Ad hoc podle situace.	Riziko ohledně GDPR!
Kdo přiděluje práva a přístup k OÚ? K datům obecně, popis procesu.	Rozhodují jednotliví vedoucí.	
Jak se autentizují jednotliví uživatelé s přístupem k OÚ?	Jméno a heslo.	
Je implementována pseudonymizace OÚ?	Není implementováno.	
Jakým způsobem jsou OÚ v listinné podobě likvidovány? Popis, postup, technologie, protokoly? Co se děje s archívy?	Skartovačka. Mazání v PC jeho systémovými prostředky.	

16.2 Metodika vyplňování formulářů

Odbor	Příklad: Městský úřad XXXX, Obecní živnostenský úřad
Název činnosti zpracování	Příklad: Poskytování informací dle zákona č. 106/1999 Sb.
Podrobný popis datové sady	Zde se uvádí agenda, oblast či proces odpovídající příslušné oblasti působnosti, při níž jsou zpracovávány osobní údaje. Může se jednat o agendy v přenesené působnosti státu (např. stavební povolení, evidence obyvatel, cestovní doklady, rybářské lístky, vedení obecní kroniky atd.), Samostatná působnost (např. Správa bytových fondů, pronájem nebytových prostor, těžba a prodej dřeva), Interní procesy úřadu (např. personalistika, zúčtování mezd, kamerové systémy, GPS lokace vozidel pracovníků). Níže uvedené části dotazníku bude odpovědná osoba vyplňovat pro každou agendu, proces či oblast samostatně.
Oblast působnosti agendy či procesu	Vyberte jednu ze tří možností: □ Přenesená působnost státu (státní správa), jedná se o přenesenou působnost státu dle Hlavy III zákona č. 128/2000 Sb. o obcích; □ Samostatná působnost (samospráva), jedná se o samostatnou působnost dle Hlavy II zákona č. 128/2000 Sb. o obcích; □ Interní procesy úřadu.
OÚ obsažené v agendě	Zde se uvádí taxativní výčet druhu zpracovávaných osobních údajů, např. Jméno, Příjmení, Rok narození, Telefon atd. U kategorie zvláštních osobních údajů, dle článku č. 9 GDPR, se jedná o následující prvky: □ rasový či etnický původ; □ politické názory; □ náboženské vyznání; □ filozofické přesvědčení; □ členství v odborech; □ genetické údaje; □ biometrické údaje za účelem jedinečné identifikace fyzické osoby; □ údaje o zdravotním stavu; □ údaje o sexuálním životě; □ údaje o sexuální orientaci.
Zpracovávané kategorie osobních údajů	Položka slouží k výběru kategorií zpracovávaných osobních údajů týkající se uvedené agendy. □ Osobní údaje - osobní údaje dle čl. 4 Nařízení Evropského parlamentu a Rady (EU) 2016/679 jsou definovány takto "veškeré informace o identifikované nebo identifikovatelné fyzické osobě (dále jen „subjekt údajů“); identifikovatelnou fyzickou osobou je fyzická osoba, kterou lze přímo či nepřímo identifikovat, zejména odkazem na určitý identifikátor, například jméno, identifikační číslo, lokační údaje, sítový identifikátor nebo na jeden či více zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity této fyzické osoby."; □ Zvláštní kategorie osobních údajů – zvláštní kategorie osobních údajů je charakterizovány článkem č. 9 GDPR takto: " Osobní údaje, které vypovídají o rasovém či etnickém původu, politických názorech, náboženském vyznání či filozofickém přesvědčení nebo členství v odborech, a zpracování genetických údajů, biometrických údajů za účelem jedinečné identifikace fyzické osoby a údajů o zdravotním stravu či o sexuálním životě nebo sexuální orientaci fyzické osoby." □ Genetické údaje – Nařízení evropského parlamentu a Rady (EU) 2016/679 definuje genetické údaje takto "Osobní údaje týkající se zděděných nebo získaných genetických znaků fyzické osoby, které poskytují jedinečné informace o její fyziologii či zdraví a které vyplývají zejména z analýzy biologického vzorku dotčené fyzické osoby"; □ Biometrické údaje – biometrické údaje dle čl. 4 Nařízení evropského parlamentu a Rady (EU) 2016/679 jsou definovány takto "Osobní údaje vyplývající z konkrétního technického zpracování týkající se fyzických či fyziologických znaků nebo znaků chování fyzické osoby, které umožňuje nebo potvrzuje jedinečnou identifikaci, například zobrazení obličeje nebo daktyloskopické údaje"
Vztah subjektu údajů ke správci či Kolektivu osobních údajů	Uvedení vztahu subjektu údajů ke správci či Kolektivu osobních údajů nebo kategorie subjektů osobních údajů. Kolektiv uvádí vybrané kategorie subjektu údajů: □ Občan – přenesená působnost;

	□ Občan – samostatná působnost; □ Zaměstnanec; □ Dodavatel; □ Kategorie zvláště zranitelných subjektů údajů – nezletilý.
Právní základ zpracování	Uvedení právního základu zpracování osobních údajů, na základě článku č. 6 GDPR. Kolektiv uvádí příklady právních základů a to: □ Oprávněný zájem správce; □ Plnění právní povinnosti; □ Plnění smlouvy nebo jednání o jejím uzavření; □ Souhlas se zpracováním osobních údajů pro jeden či více konkrétních účelů; □ Veřejný zájem, výkon veřejné moci; □ Ochrana životně důležitých zájmů subjektu údajů nebo jiné fyzické osoby.
Účel zpracování	Popis důvodu, na základě kterého dochází ke zpracování osobních údajů. Uvedení výčtu právních předpisů, na jejichž základě dochází ke zpracování osobních údajů. Jedná se o zákony, vyhlášky či případně interní akty řízení.
Přenositelnost	ano/ne
Námitka	ano/ne
Archivní doba	Příklady: 84 Poskytování informací, styk s veřejností 84.1 Poskytování informací ze zákona S5 možnosti jsou Archivovat, Skartovat, Výběr
Kdy a jak datová sada vzniká	Příklad: 1. Nejčastějším způsobem vzniku datové sady je osobní kontakt. Při něm žadatel podá žádost osobně při jednání s úředníkem. Identifikaci subjektu provede úřadník podle platných osobních dokladů. Přitom místnost je uspořádána tak, že žadatel sedí naproti úředníkovi a nevidí na monitor jeho počítače. Údaje se zadávají rovnou do počítače. 2. Další možností je, že žadatel přinese dokument žádosti a předá jej v podatelně. Odtud dokument postupuje standardní spisovou službou. 3. Je možné žádost podat prostřednictvím formuláře na internetu – formulář funguje v zabezpečeném režimu SSL, 4. Teoreticky lze formulář žádosti přijmout i prostřednictvím datové schrány úřadu.
Jak se sada zpracovává	Příklad: Všechny údaje z žádosti se vloží do počítače, a to do veřejných rejstříků (živnostenský rejstřík podle 455/1991 Sb. Živnostenský zákon, ve znění pozdějších předpisů, obchodní rejstřík podle 304/2013 Sb. Zákon o veřejných rejstřících právnických a fyzických osob ve znění pozdějších předpisů a další.) Rejstříky jsou vedeny Ministerstvem průmyslu a obchodu – MěÚ je z hlediska osobních údajů jen Kolektivum, správcem je MPO. Rozpracovaný podnět zůstává v oddělení až do jeho vyřízení. V některých případech (žádost o licenci) ŽÚ potřebuje doklady, např. doklady o kvalifikaci. Tyto může postoupit dalším úřadům, a to na základě zvláštních zákonů.
Co se stane po skončení života datové sady	Příklad: Život datové sady končí s ukončením živnostenského podnikání, zejména při smrti subjektu nebo při ukončení živnosti. V takovém případě úřad vyčká pravomocného rozhodnutí (např. na skončení dědického řízení, nebo na pravomocné rozhodnutí o ukončení činnosti). Potom je proveden postup podle spisového a skartačního řádu, a to ve lhůtách a se skartačním znakem, určeným tímto řádem. Papírové dokumenty se předávají do spisovny (odkud mohou být

	přemístěny do archívu nebo být skartovány). Elektronické údaje se neskartují, protože existují jen ve veřejných rejstřících, u kterých MěÚ není správcem
Osoba odpovědná za datovou sadu	uveďte též spojení
Kategorie subjektů osobních údajů	Uvedení vztahu subjektu údajů ke správci či Kolektivu osobních údajů nebo kategorie subjektů osobních údajů. Kolektiv uvádí vybrané kategorie subjektu údajů: □ Občan – přenesená působnost; □ Občan – samostatná působnost; □ Zaměstnanec; □ Dodavatel; □ Kategorie zvláště zranitelných subjektů údajů – nezletilý.
Specifikace listinného úložiště	Popište způsob, jakým jsou uloženy listinné dokumenty
Specifikace elektronického nestrukturovaného úložiště	Specifikace elektronického nestrukturovaného úložiště: lokální disky, email, sdílené disky pokud není, ponechte prázdné
Specifikace elektronického strukturovaného úložiště	Specifikace elektronického strukturovaného úložiště: databáze, informační systém pokud není, ponechte prázdné
Kategorie příjemců včetně příjemců mimo EU	Dle článku č. 4 GDRP je Příjemcem fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, kterým jsou osobní údaje poskytnuty, ať už se jedná o třetí stranu, či nikoli. Uvedení všech kategorií příjemců osobních údajů a to: □ Interní příjemce – uvedení rolí pracovníků úřadu; □ Externí příjemce – uvedení všech možných externích příjemců osobních údajů včetně příjemců mimo EU.
Využívání spolupráce se Kolektivum OÚ	Kolektiv je fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který zpracovává osobní údaje pro správce. Jedná se zpravidla o třetí stranu, která poskytuje službu úřadu. Jedná se o typicky outsourcing. Může se jednat o vedení účetnictví, zpracování mezd apod.
Způsob kontroly zpracování OÚ	Popis způsobu kontroly zpracování OÚ - např. roční audit, kontrola třetí stranou.
Připravenost na uplatňování práv ze strany subjektů OÚ	Dle GDPR, informace o přijatých opatřeních musí být poskytnuta bez zbytečného odkladu a do jednoho měsíce od obdržení žádosti. Činí se tak pouze v odůvodněných případech a bezplatně. Uvedení připravenosti vybraných obcí na uplatňování těchto práv.
Další požadované dokumenty	Vyžádejte si dokumenty, které se k této agendě nějak vztahují a uveďte je zde. Například: □ Organizační struktura posuzovaného subjektu / úřadu; □ Organizační řád; □ Spisový a skartační řád včetně vnitřních předpisů v oblasti archivace listinných dokumentů (Směrnice o archivaci); □ Vnitřní předpisy mající vztah k problematice osobních údajů a k problematice řízení bezpečnosti informací; □ Vzorové smlouvy k problematice zpracování osobních údajů nebo k činnostem, jejichž předmětem je zpracování osobních údajů.

17. OBSAH