

# SMLOUVA O DÍLO

číslo smlouvy objednatele: 7/18/S/OdIKŘ

číslo smlouvy zhotovitele: 54/2017

*uzavřená v souladu ustanovením § 2586 a následujících zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů (dále jen „smlouva“), mezi smluvními stranami*

## **M&T s.r.o.**

zastoupené: [REDACTED]  
sídlo: Štverákova 2779/9, 193 00 Praha 9  
IČO: 278 94 452  
DIČ: CZ27894452  
bankovní spojení: [REDACTED]  
číslo účtu: [REDACTED]  
kontaktní osoba: [REDACTED]  
tel.: [REDACTED]  
e-mail: [REDACTED]

dále jen „**zhotovitel**“

a

## **Město Šternberk**

zastoupené: [REDACTED]  
se sídlem: Horní náměstí 16, 785 01 Šternberk  
IČ: 00299529  
DIČ: CZ00299529  
bankovní spojení: [REDACTED]  
č. účtu: [REDACTED]  
kontaktní osoba: [REDACTED]  
tel.: [REDACTED]  
e-mail: [REDACTED]

dále jen „**objednatel**“

## **ČLÁNEK 1**

### **PŘEDMĚT SMLOUVY**

1. Předmětem této smlouvy je úprava práv a povinností smluvních stran v souvislosti s “Provedením vstupní a rozdílové analýzy stavu zpracování a ochrany osobních údajů a realizací kroků k uvedení do souladu s požadavky GDPR“ (dále jen „dílo“) pro objednatele

u koncového zákazníka Město Šternberk a 9 jím zřízených příspěvkových organizací, vyjmenovaných v Čl. 3 bod 3.2.

2. Objednatel se zavazuje, že řádně provedené dílo včas převezme a zaplatí za jeho zhotovení zhotoviteli v této smlouvě dohodnutou cenu.
3. Zhotovitel se touto smlouvou zavazuje k řádnému a včasnému provedení díla.

## **ČLÁNEK 2**

### **PŘEDMĚT PLNĚNÍ**

1. Předmětem plnění je “ Provedení vstupní a rozdílové analýzy stavu zpracování a ochrany osobních údajů a realizace kroků k uvedení do souladu s požadavky GDPR“ pro objednatele u koncového zákazníka Město Šternberk a 9 jím zřízených příspěvkových organizací, vyjmenovaných v Čl. 3 bod 3.2.
2. Dílo je rozděleno na dvě části:
  - 2.1 **A.** „Provedení vstupní a rozdílové analýzy stavu zpracování a ochrany osobních údajů a realizace kroků k uvedení do souladu s požadavky GDPR a to včetně analýzy rizik a školení“ pro objednatele u koncového zákazníka Město Šternberk,
  - 2.2 **B.** „Provedení vstupní a rozdílové analýzy stavu zpracování a ochrany osobních údajů a realizace kroků k uvedení do souladu s požadavky GDPR“ u 9 jím zřízených příspěvkových organizací, vyjmenovaných v Čl. 3 bod 3.2.
3. Podrobný rozsah předmětu plnění je uveden v Příloze č. 1 Specifikace předmětu plnění, která je nedílnou součástí této smlouvy.

## **ČLÁNEK 3**

### **DOBA A MÍSTO PLNĚNÍ**

1. Činnosti dle Článku 2 budou zahájeny po podpisu smlouvy oběma stranami a dohodě s objednatelem a koncovým zákazníkem.
2. Průběh realizace se bude řídit harmonogramem realizace, který je Přílohou č. 2 a nedílnou součástí této smlouvy.
3. Místem plnění je Město Šternberk:
  - 3.1. pro část A: budova městského úřadu, Horní náměstí 16, 785 01 Šternberk
  - 3.2. pro část B:
    - ZŠ Svatoplukova, Svatoplukova 7



- 1.4. Fakturovaná cena je celkovou částkou nejvýše přípustnou a obsahuje veškeré náklady zhotovitele, nutné a uznatelné k realizaci předmětu plnění dle Článku 2 této smlouvy.
- 1.5. Dojde-li v průběhu provádění díla ke změně výše příslušné sazby DPH či jiných poplatků stanovených příslušnými právními předpisy, bude účtována DPH k příslušným zdanitelným plněním či jiné poplatky ve výši stanovené novou právní úpravou.

## **2. ZPŮSOB PLATBY**

- 2.1. Cena dle Článku 4 této smlouvy za části A a B bude uhrazena na základě faktur, které budou vystaveny zhotovitelem po ukončení a protokolárním předání a převzetí příslušné části objednatelem.

## **3. VYSTAVOVÁNÍ FAKTUR**

- 3.1. Celková odměna za plnění předmětu dle Článku 2 této smlouvy bude objednatelem placena na základě řádných daňových dokladů (dílčích faktur), vystavených zhotovitelem v souladu s dalšími podmínkami uvedenými v této smlouvě.
- 3.2. Faktury budou zhotovitelem vystaveny v souladu s § 11 odst. 1 zákona č. 563/1991 Sb., o účetnictví, ve znění pozdějších předpisů a budou obsahovat náležitosti řádného daňového dokladu dle § 29 zákona č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů.
- 3.3. Splatnost každé faktury bude do 14 dnů ode dne jejího doručení objednateli a po splnění podmínek uvedených v této smlouvě.
- 3.4. Objednatel je oprávněn vrátit fakturu před uplynutím lhůty její splatnosti bez zaplacení v případě, že neobsahuje zákonem stanovené a sjednané náležitosti anebo je vystavena na částku, která neodpovídá této smlouvě. Objednatel zároveň uvede důvod takového vrácení. V tomto případě běží nová lhůta splatnosti ode dne doručení opravené faktury objednateli. Zhotovitel v tomto případě nemá právo uplatňovat úrok z prodlení.
- 3.5. Strany se dohodly, že platba bude provedena na číslo účtu uvedené zhotovitelem v úvodu této smlouvy. Povinnost zaplatit je splněna dnem odepsání příslušné částky z účtu objednatele.
- 3.6. Faktura bude uhrazena na účet zhotovitele, který je správcem daně zveřejněn v Registru plátců DPH. Pokud k datu uskutečnění zdanitelného plnění uvedeného na daňovém dokladu bude zhotovitel v Registru plátců DPH uveden jako nespolehlivý plátcce, bude objednatel postupovat v souladu se zákonem o DPH v platném znění.

## **ČLÁNEK 5**

### **PŘEDÁNÍ A PŘEVZETÍ DÍLA**

#### **1. ZPŮSOB PŘEDÁNÍ A PŘEVZETÍ DÍLA**

- 1.1. Zhotovitel se zavazuje v den ukončení příslušné etapy díla předat objednateli provedenou část díla. V případě, že objednatel odmítne provedenou část díla převzít, musí písemně uvést důvod.
- 1.2. Pokud zhotovitel připraví příslušnou etapu díla k odevzdání před sjednaným termínem, zavazuje se objednatel převzít tuto část díla i v nabídnutém, oboustranně akceptovatelném, zkráceném termínu.
- 1.3. Zhotovitel předá dílo v jednom vyhotovení v listinné a digitální podobě, pokud nebude dohodnuto jinak.

## **2. PROTOKOL O PŘEDÁNÍ A PŘEVZETÍ DÍLA**

O předání a převzetí předmětu plnění bude sepsán protokol.

## **3. VLASTNICKÉ PRÁVO K DÍLU A NEBEZPEČÍ ŠKODY**

Veškerá práva k provedenému dílu, a to včetně vlastnického práva, přecházejí na objednatele předáním a převzetím jednotlivých částí, resp. celého díla, ledaže by z povahy věci nebo dohody smluvních stran vyplývalo jiné.

## **ČLÁNEK 6**

### **GARANCE ZHOTOVITELE**

1. Zhotovitel prohlašuje, že je oprávněn k provádění činností dle předmětu této smlouvy v plném rozsahu, zejména, že je držitelem příslušných živnostenských oprávnění pokrývajících celý předmět plnění zhotovitele podle této smlouvy.
2. Zhotovitel se zavazuje, že bude dodržovat a je schopen plnit právní a technické podmínky vyplývající ze závazných platných právních předpisů, vyhlášek a norem.
3. Zhotovitel prohlašuje, že neumožňuje výkon nelegální práce ve smyslu zákona č. 435/2004 Sb. o zaměstnanosti, ve znění pozdějších předpisů, a ani neodebírá žádné plnění od osoby, která by výkon nelegální práce umožňovala. V případě, že se toto prohlášení ukáže v budoucnu nepravdivým a vznikne ručení objednatele ve smyslu ust. § 141a a § 141b zákona č. 435/2004 Sb., má objednatel nárok na náhradu všeho, co za zhotovitele v souvislosti s tímto ručením plnil.
4. Zhotovitel není oprávněn postoupit, převést ani zastavit tuto smlouvu ani jakákoli práva, povinnosti, dluhy, pohledávky nebo nároky vyplývající z této smlouvy bez předchozího písemného souhlasu objednatele.

## **ČLÁNEK 7**

### **ODPOVĚDNOST ZA ŠKODU A SANKCE**

## **1. ODPOVĚDNOST ZHOTOVITELE**

- 1.1. Zhotovitel odpovídá za to, že dílo ujednané touto smlouvou je vyhotoveno podle podmínek této smlouvy a že po dobu záruční doby bude mít vlastnosti dohodnuté v této smlouvě.
- 1.2. Zhotovitel nezodpovídá za vady díla, které byly způsobeny použitím podkladů poskytnutých objednavatelem a zhotovitel ani při vynaložení maximální péče, kterou po něm lze oprávněně požadovat, nemohl zjistit jejich nevhodnost, nebo na ně upozornil objednavatele písemně a ten na jejich použití trval.
- 1.3. Záruční doba začíná plynout ode dne předání díla objednateli, tj. ode dne podpisu protokolu o předání a převzetí díla, a trvá 24 měsíců. Záruka se vztahuje na dílo zpracované v souladu s platnými právními předpisy ke dni předání díla objednateli.
- 1.4. Smluvní strany se dohodly pro případ vady díla, že po dobu záruční doby má objednatel právo požadovat a zhotovitel povinnost bezplatného odstranění vady.
- 1.5. Zhotovitel se zavazuje odstranit případnou vadu díla do 14 kalendářních dnů od oprávněné reklamace objednavatele.

## **2. SANKCE**

- 2.1. Bude-li objednatel v prodlení s úhradou faktury, je zhotovitel oprávněn požadovat na objednateli zaplacení úroku z prodlení ve výši 0,05 % z dlužné částky za každý započatý den prodlení, a to až do doby zaplacení dlužné částky, a objednatel je povinen takto požadovaný úrok z prodlení zaplatit.
- 2.2. Bude-li zhotovitel v prodlení s předáním kterékoliv části díla, je objednatel oprávněn požadovat na zhotoviteli zaplacení úroku z prodlení ve výši 0,05 % z ceny za provedení příslušné části díla za každý započatý den prodlení, a to až do doby předání příslušné části díla, a zhotovitel je povinen takto požadovaný úrok z prodlení zaplatit.
- 2.3. Zhotovitel i objednatel se zavazují, že v případě porušení důvěrnosti informací dle Článku 8 této smlouvy zaplatí ten, kdo prokazatelně porušil tento závazek, druhé smluvní straně pokutu ve výši 50 000 Kč (slovy: padesáttisíc korun českých).

## **ČLÁNEK 8**

### **DŮVĚRNOST INFORMACÍ**

1. Smluvní strany jsou si vědomy toho, že v rámci plnění smlouvy:
  - 1.1. si mohou vzájemně poskytnout informace, které budou považovány za důvěrné (dále „důvěrné informace“),
  - 1.2. mohou jejich zaměstnanci získat přístup k důvěrným informacím druhé strany.

2. Veškeré důvěrné informace zůstávají výhradním vlastnictvím předávající strany a přijímající strana vyvine pro zachování jejich důvěrnosti a pro jejich ochranu stejné úsilí, jako by se jednalo o její vlastní důvěrné informace. S výjimkou plnění této smlouvy, se obě strany zavazují nepublikovat žádným způsobem důvěrné informace druhé strany, nepředat je třetí straně ani svým vlastním zaměstnancům a zástupcům s výjimkou těch, kteří s nimi potřebují být seznámeni, aby mohli splnit smlouvu. Obě strany se zároveň zavazují nepoužít důvěrné informace druhé strany jinak než za účelem plnění smlouvy nebo uplatnění svých práv z této smlouvy.
3. Nedohodnou-li se smluvní strany výslovně jinak, považují se za důvěrné implicitně všechny informace, které jsou a nebo by mohly být součástí obchodního tajemství, tj. například ale nejenom popisy nebo části popisů technologických procesů a vzorců, technických vzorců a technického know-how, informace o provozních metodách, procedurách a pracovních postupech, obchodní nebo marketingové plány, koncepce a strategie nebo jejich části, nabídky, kontrakty, smlouvy, dohody nebo jiná ujednání s třetími stranami, informace o výsledcích hospodaření, o vztazích s obchodními partnery, o pracovněprávních otázkách a všechny další informace, jejichž zveřejnění přijímající stranou by předávající straně mohlo způsobit škodu.
4. Pokud jsou důvěrné informace poskytovány v písemné podobě anebo ve formě textových souborů na počítačových médiích, je předávající strana povinna upozornit přijímající stranu na důvěrnost takového materiálu jejím vyznačením alespoň na titulní stránce.
5. Bez ohledu na výše uvedená ustanovení se za důvěrné nepovažují informace, které:
  - 5.1. se staly veřejně známými, aniž by to zavinila přijímající strana,
  - 5.2. měla přijímající strana legálně k dispozici před uzavřením smlouvy, pokud takové informace nebyly předmětem jiné, dříve mezi smluvními stranami uzavřené smlouvy o ochraně informací,
  - 5.3. jsou výsledkem postupu, při kterém k nim přijímající strana dospěje nezávisle a je to schopna doložit svými záznamy nebo důvěrnými informacemi třetí strany,
  - 5.4. jsou zveřejněny a zpřístupněny ve veřejných evidencích.
6. Ustanovení tohoto článku není dotčeno ukončením účinnosti smlouvy z jakéhokoliv důvodu a jeho účinnost skončí nejdříve pět (5) let po ukončení účinnosti této smlouvy.

## **ČLÁNEK 9**

### **PLATNOST A ÚČINNOST SMLOUVY**

1. Tato smlouva nabývá platnosti a účinnosti dnem podpisu oprávněnými osobami obou smluvních stran.
2. Tuto smlouvu lze předčasně ukončit:
  - 2.1. dohodou smluvních stran, jejíž součástí je i vypořádání vzájemných závazků a pohledávek,
  - 2.2. odstoupením od smlouvy v případě dále vymezeného podstatného porušení smluvních závazků jednou smluvní stranou.

3. Objednatel je oprávněn odstoupit od této smlouvy v případě podstatného porušení povinností zhotovitelem, které spočívá v prodlení s plněním závazků delším, než 60 kalendářních dnů, přes písemné upozornění zhotovitele na takové prodlení.

## **ČLÁNEK 10**

### **ZÁVĚREČNÁ USTANOVENÍ**

1. Právní vztahy vzniklé z této smlouvy, nebo s touto smlouvou související, se řídí zákonem č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů.
2. Tuto smlouvu lze měnit nebo doplňovat pouze dohodou smluvních stran formou písemného dodatku podepsaného jejich oprávněnými osobami.
3. Smluvní strany se dohodly, že žádná z nich není oprávněna postoupit svá práva a povinnosti vyplývající z této smlouvy třetí straně bez předchozího písemného souhlasu druhé smluvní strany.
4. Smluvní strany se budou snažit veškeré spory vyplývající z této smlouvy řešit nejprve smírnou cestou.
5. Tato smlouva je vyhotovena ve dvou stejnopisech, z nichž každá smluvní strana obdrží jeden stejnopis.
6. Smluvní strany shodně prohlašují, že jsou si vědomy všech právních důsledků touto smlouvou vyvolaných a souhlasí se všemi jejími ustanoveními. Dále prohlašují, že smlouva je uzavřena podle jejich svobodné a pravé vůle, určitě, vážně a srozumitelně a na důkaz toho připojují své podpisy.
7. Smluvní strany souhlasí s tím, že obsah smlouvy není obchodním tajemstvím a smluvní strany mohou smlouvu zveřejnit v rozsahu a za podmínek, jež vyplývají z obecně závazných právních předpisů.
8. Tato smlouva nabývá platnosti dnem podpisu a účinnosti dnem zveřejnění v registru smluv dle příslušných ustanovení zákona č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv (zákon o registru smluv).
9. Smluvní strany se dohodly, že zákonnou povinnost dle § 5 odst. 2 zákona o registru smluv splní objednatel, Město Šternberk.

Doložka platnosti právního jednání dle ustanovení § 41 zákona č. 128/2000 Sb., o obcích (obecní zřízení), ve znění pozdějších předpisů:

Na straně kupujícího rozhodla o uzavření této smlouvy Rada města Šternberka dne 18.12.2017 usnesením č. 2354/63



V Praze.....

Zhotovitel:

.....  
[Redacted]  
[Redacted]  
[Redacted]  
[Redacted]  
**M&T s.r.o.**

Ve Šternberku.....

Objednatel:

.....  
[Redacted]  
[Redacted]  
[Redacted]  
[Redacted]  
**Město Šternberk**

## **A. Provedení vstupní a rozdílové analýzy stavu zpracování a ochrany osobních údajů a realizací kroků k uvedení do souladu s požadavky GDPR u Města Šternberk**

### **1 Etapa 1 – Analýza procesů správy, zpracování a nakládání s osobními údaji**

Cílem etapy je zajistit a vyhodnotit zejména zjištění a vyhodnocení rozsahu a potřebnosti zpracování osobních údajů u jednotlivých organizačních celků a všech realizovaných procesů. V rámci tohoto kroku bude (budou):

- a) zjišťovány jednotlivé účely zpracování osobních údajů,
  - b) pro každý účel zpracování budou identifikovány veškeré typy zpracovávaných údajů,
  - c) posouzen rozsah a nezbytnost zpracovávaných osobních údajů pro jednotlivé účely, důraz bude položen na typy osobních údajů, které umožňují nepřímou identifikaci subjektu údajů, typicky např. zpracování lokalizačních údajů, IP adres, RFID a řada dalších),
  - d) definovány zdroje osobních údajů u jednotlivých účelů zpracování,
  - e) v součinnosti s objednatelem bude vyhodnocena nezbytná doba uchování zpracovávaných osobních údajů vůči potřebám účelu zpracování,
  - f) u jednotlivých účelů zpracování bude vyhodnocen řádový objem zpracovávaných osobních údajů,
  - g) pro každý účel zpracování bude vyhodnoceno, kdo jej zpracovává, s cílem rozlišit zpracování vlastními zaměstnanci objednatele, zpracovatelem nebo třetí stranou pověřenou správcem nebo zpracovatelem,
  - h) v součinnosti s objednatelem stanoveny právní tituly zpracování osobních údajů pro jednotlivé účely (tj. jejich zákonnost),
  - i) identifikovány osobní údaje předávané jiným správcům nebo do jiných států (pokud jsou předávány) a právní titul k jejich předání.
- 1) Pro každý v bodě 1) identifikovaný účel zpracování budou stanoveny způsoby a prostředky, kterými jsou údaje zpracovávány a kterými jsou minimálně následující:
- a) Listinná podoba vedená v evidencích, kartotékách atd.,
  - b) Agendové IS, jejich moduly, aplikace,
  - c) Ekonomické, provozní, administrativní, docházkové, monitorovací a kamerové a další IS.

- 2) Bude posouzeno dodržování pravidel pro zpracování osobních údajů zpracovávaných v IS, kterých není město správcem (ISEO, ISZR, katastr nemovitostí atd.).
- 3) Posouzení nutnosti a účelnosti provedení datového auditu s cílem zjistit rozsah zpracovávaných osobních údajů, které jsou obvykle mimo kontrolu IT (pevné disky počítačů s uloženými kopiemi dokumentů, dokumentace, programy v podobě např. Excel s makry, ve kterém se zpracovávají osobní údaje a řada dalších...).
- 4) Posouzení prokazatelnosti a kvality souhlasů se zpracováním v případech, kdy zpracování osobních údajů podléhá souhlasu subjektu údajů a současně posouzení plnění informační povinnosti.
- 5) Posouzení smluvních vztahů s dodavateli služeb, kteří jsou zpracovateli ve smyslu zákona o ochraně osobních údajů. V rámci tohoto kroku bude provedena:
  - a) identifikace zpracovatelů,
  - b) posouzení smluvních garancí zpracovatele k zajištění stanovené úrovně ochrany zpracování osobních údajů na základě smlouvy se správcem,
  - c) identifikace případného řetězení zpracovatelů.
- 6) Posouzení smluvních vztahů s dodavateli služeb, kteří nejsou zpracovateli ve smyslu zákona o ochraně osobních údajů. V rámci tohoto kroku bude provedena:
  - a) identifikace dodavatelů,
  - b) posouzení smluvních garancí dodavatele k zajištění ochrany osobních údajů.
- 7) Posouzení rozsahu, efektivity a úrovně přijatých technických a organizačních opatření při zpracování osobních údajů s cílem vyhodnotit úroveň zajištění jejich důvěrnosti, integrity a dostupnosti. V rámci tohoto kroku bude ověřena:
  - a) prokazatelnost a úroveň provedení analýzy rizik,
  - b) opatření v oblasti počítačové, fyzické, personální, administrativní bezpečnosti,
  - c) úroveň a rozsah realizace politiky uchování a mazání/likvidace dat, zpracovávaných automatizovaně i v listinné podobě.
- 8) Posouzení odpovědnosti za zpracování a ochranu osobních údajů v rámci úřadu.
- 9) Posouzení rozsahu a úrovně zpracované bezpečnostní dokumentace k ochraně osobních údajů platné pro listinné i automatizované zpracování osobních údajů, včetně zpracování osobních údajů v kamerových systémech, s cílem ověřit, zda jsou zdokumentovaná pravidla dostatečná pro prokázání zajištění prokazatelnosti záměrné a nezbytné ochrany zpracovávaných osobních údajů.

- 10) Posouzení dostatečnosti, úrovně a rozsahu kontrolní činnosti směrem k zaměstnancům správce, zpracovatelům a dodavatelům.

#### **Výstupy etapy:**

- 1) **Analytická zpráva** - popis současného stavu a identifikace prvků, které nejsou v souladu s požadavky nové legislativy (rozdílová analýza),
- 2) **Záznam o činnostech zpracování osobních údajů** (ke každé skupině zpracovávaných osobních údajů).

## **2 Etapa 2 – Implementace kroků k dosažení souladu**

Cílem této etapy je navrhnout konkrétní podobu chybějících procesů či změny současných a jejich zavedení pro praxe. Bude se jednat zejména o problematiku:

- 1) pověřence pro ochranu osobních údajů (DPO),
  - a) doporučení k možnostem personálního obsazení DPO, případně návrh řešení smluvním partnerem, včetně návrhu jeho kvalifikačních předpokladů,
  - b) návrh katalogu/manuálu činností DPO, návrh jeho práv a povinností,
- 2) procesů k hlášení narušení bezpečnosti osobních údajů s cílem vyhodnotit:
  - a) povahu incidentu,
  - b) stupeň rizika pro dotčené subjekty údajů:
    - bez rizika,
    - riziko,
    - vysoké riziko,
  - c) návrh přijatých opatření,
- 3) rozhodovacího procesu k uplatnění práva subjektů údajů pro každý účel zpracování samostatně,
- 4) rozhodovacího procesu pro realizaci posouzení vlivu na ochranu osobních údajů, včetně zpracování metodiky pro případné posouzení vlivu,
- 5) metodiky a postupu pro realizaci ochrany „by design“,
- 6) metodiky a postupu pro realizaci ochrany „by default“,
- 7) procesů k zajištění pravidelného testování a vyhodnocování účinnosti přijatých technických a organizačních opatření.

#### **Podle potřeby úprava technických a organizačních opatření v těchto oblastech:**

- 1) Úprava formulace a rozsahu stávajících souhlasů subjektů údajů se zpracováním, vzhledem k právnímu základu příslušného účelu zpracování:
  - na rozdíl od stávajícího zákona o ochraně osobních údajů GDPR nepodmiňuje primárně zpracování osobních údajů souhlasem a následnými výjimkami, nýbrž stanovuje jasné a konkrétní podmínky pro zákonné zpracování, kdy souhlas je jen jednou z nich,
  - rozsah souhlasů bude posouzen i z hlediska nového institutu právního základu, který se týká zejména podnikatelských subjektů a kterým je „Oprávněný zájem správce“,

- bude navržena metodika a postup pro případ Odvolání souhlasu subjektem údajů.
- 2) V případě, že jsou zpracovávány citlivé údaje dle stávající terminologie zákona o ochraně osobních údajů, revize všech procesů souvisejících se zpracováním „zvláštní kategorie údajů“ ve smyslu terminologie a požadavků GDPR.
  - 3) Posouzení úrovně Politiky uchování a mazání dat.
  - 4) Revize a návrh úpravy informační povinnosti subjektům údajů s cílem poskytnout explicitně vyžadované informace přehledným a srozumitelným způsobem a do doby 30 dní.
  - 5) Revize a návrh úprav procesů při uplatnění práv subjektů údajů.
  - 6) Návrh úprav smluvních vztahů se Zpracovatelem a Dodavatelem služeb, v rámci kterých jsou zpracovávány osobní údaje.
  - 7) Návrh úprav řešení kontrolní činnosti.

### **3 Etapa 3 – Provedení analýzy informačních rizik, zpracování interních předpisů a potřebné související řídicí dokumentace pro ochranu osobních údajů**

Cílem této etapy je zejména:

- 1) Zpracovat metodiku analýzy rizik, která prokáže odpovídající úroveň požadavků na:
  - Důvěrnost,
  - Integritu,
  - Dostupnost
 zpracovávaných osobních údajů.
- 2) Provedení analýzy rizik s cílem vyhodnotit, posoudit a navrhnout:
  - Hodnotu informačních aktiv obsahující osobní údaje dle metrik stanovených zákonem o kybernetické bezpečnosti,
  - Zranitelnosti a hrozby působící na aktiva,
  - Velikost a závažnost rizik z pohledu jejich dopadů a pravděpodobnosti výskytu,
  - která explicitně definovaná opatření v GDPR jsou relevantní pro eliminaci identifikovaných rizik (pseudonymizace, šifrování, minimalizace atd.),
  - zda stávající technická a organizační opatření jsou vzhledem k závažnosti rizik dostatečná, v případě potřeby navrhnout další potřebná opatření se zohledněním následujících aspektů:
    - povaha a kontext zpracování,
    - náklady,
    - dostupné technologie,
    - rizika zpracování,
  - návrh a odůvodnění akceptovatelných rizik,
  - zpracování plánu zvládnutí rizik,
  - kalkulaci rámcových nákladů na eliminaci zjištěných rizik.
- 3) Vytvoření koncepce/politiky zpracování a ochrany osobních údajů, která umožní prokázat naplnění základních principů GDPR, kterými jsou:
  - a) zákonnost zpracování osobních údajů,

- b) záměrná a standardní ochrana osobních údajů,
  - c) minimalizace zpracovávaných osobních údajů,
  - d) korektnost a transparentnost při zpracování osobních údajů,
  - e) odpovídající důvěrnost, integritu a dostupnost osobních údajů,
  - f) odpovědnost správce osobních údajů.
- 4) Rozpracování koncepce/politiky ochrany osobních údajů do vnitřních předpisů a metodických pokynů organizace (správce).
  - 5) Příprava registračních formulářů pro účely zpracování, které podléhají oznamovací povinnosti ve smyslu § 16 ZOOÚ a tato povinnost doposud nebyla splněna (platnost do 25.5.2018).

## **B. Provedení „vstupní a rozdílové analýzy a implementace kroků k dosažení souladu s GDPR“ u městem zřízených 9 příspěvkových organizací (PO):**

- ZŠ Svatoplukova, Svatoplukova 7
- ZŠ Dr. Hrubého, Dr. Hrubého 319/2
- ZŠ nám. Svobody, nám. Svobody 3
- Základní umělecká škola, Olomoucká 3
- Školní jídelna Šternberk, Svatoplukova 7
- MŠ Nádražní, Nádražní 7
- MŠ Komenského, Komenského 44
- Dům dětí a mládeže, Opavská 14
- Sociální služby Šternberk, Komenského 40

### **Etapa 1 – vstupní a rozdílová analýza**

**Cílem vstupní a rozdílové analýzy je zajistit a vyhodnotit zejména**

- 1) Zjištění a vyhodnocení rozsahu a potřebnosti zpracování osobních údajů u PO a všech realizovaných procesů. V rámci tohoto kroku u každé PO bude (budou):
  - j) zjišťovány jednotlivé účely zpracování osobních údajů,
  - k) posouzen rozsah a nezbytnost zpracovávaných osobních údajů,
  - l) definovány zdroje osobních údajů u jednotlivých účelů zpracování,
  - m) v součinnosti s objednatelem u jednotlivých účelů zpracování bude vyhodnocen řádový objem zpracovávaných osobních údajů,
  - n) pro každý účel zpracování bude vyhodnoceno, kdo jej zpracovává, s cílem rozlišit zpracování vlastními zaměstnanci objednatele nebo zpracovatelem,

- o) v součinnosti s objednatelém stanoveny právní tituly zpracování osobních údajů pro jednotlivé účely (tj. jejich zákonnost),
  - p) v součinnosti s objednatelém identifikovány osobní údaje předávané jiným správcům nebo do jiných států (pokud jsou předávány) a právní titul k jejich předání.
- 2) Pro každý v bodě 1) identifikovaný účel zpracování budou stanoveny způsoby a prostředky, kterými jsou údaje zpracovávány a kterými jsou minimálně následující:
    - d) listinná podoba vedená v evidencích, kartotékách atd.,
    - e) agendové IS, jejich moduly, aplikace,
    - f) ekonomické, provozní, administrativní, docházkové, monitorovací a kamerové a další IS.
  - 3) Bude posouzeno dodržování pravidel pro zpracování osobních údajů zpracovávaných v IS jiných správců.
  - 4) Posouzení prokazatelnosti a znění souhlasů se zpracováním v případech, kdy zpracování osobních údajů podléhá souhlasu subjektu údajů; posouzení plnění informační povinnosti.
  - 5) Posouzení smluvních vztahů s dodavateli služeb, kteří jsou zpracovateli ve smyslu zákona o ochraně osobních údajů. V rámci tohoto kroku bude provedena:
    - d) identifikace zpracovatelů,
    - e) posouzení smluvních garancí zpracovatele k zajištění stanovené úrovně ochrany zpracování osobních údajů na základě smlouvy se správcem,
    - f) identifikace případného řetězení zpracovatelů.
  - 6) Posouzení rozsahu, efektivity a úrovně přijatých technických a organizačních opatření při zpracování osobních údajů s cílem vyhodnotit úroveň zajištění jejich důvěrnosti, integrity a dostupnosti. V rámci tohoto kroku bude ověřena:
    - d) prokazatelnost a úroveň provedení analýzy rizik,
    - e) opatření v oblasti počítačové, fyzické, personální, administrativní bezpečnosti,
    - f) úroveň a rozsah realizace politiky uchování a mazání/likvidace dat, zpracovávaných automatizovaně i v listinné podobě.
  - 7) Posouzení rozsahu a úrovně zpracované bezpečnostní dokumentace k ochraně osobních údajů platné pro listinné i automatizované zpracování osobních údajů, včetně zpracování osobních údajů v kamerových systémech, s cílem ověřit, zda jsou zdokumentovaná pravidla dostatečná pro prokázání zajištění prokazatelnosti záměrné a nezbytné ochrany zpracovávaných osobních údajů.
  - 8) Určení chybějících procesů a opatření, nutných pro dosažení souladu s GDPR.
  - 9) Posouzení dostatečnosti, úrovně a rozsahu kontrolní činnosti.

#### **Výstupem bude:**

- 1) **Analytická zpráva** – popis současného stavu s pojmenováním skutečností, které nejsou v souladu s požadavky legislativy,
- 2) **Záznamy o činnostech zpracování osobních údajů** v rozsahu čl. 30 GDPR,
- 3) **Návrhy nových/chybějících procesů.**

#### **Způsob realizace:**

V rámci realizace etapy budou provedeny (bude provedena):

- řízené pohovory s odpovědnými a/nebo určenými zaměstnanci PO,
- analýza dokumentace, tj. vnitřních normativních aktů a poskytnutých smluv (pozn.: v případě velkého počtu smluv u jednoho subjektu bude použita metoda vzorkování).

## **Etapa 2 - Implementace kroků k dosažení souladu**

Cílem této etapy je navrhnout konkrétní podobu chybějících procesů či změny současných a jejich zavedení pro praxe. Bude se jednat zejména o problematiku:

- 1) pověřence pro ochranu osobních údajů (DPO),
  - c) doporučení k možnostem personálního obsazení DPO, případně návrh řešení smluvním partnerem, včetně návrhu jeho kvalifikačních předpokladů,
  - d) návrh katalogu/manuálu činností DPO, návrh jeho práv a povinností,
- 2) procesů k hlášení narušení bezpečnosti osobních údajů s cílem vyhodnotit:
  - d) povahu incidentu,
  - e) stupeň rizika pro dotčené subjekty údajů:
    - bez rizika,
    - riziko,
    - vysoké riziko,
  - f) návrh přijatých opatření,
- 3) rozhodovacího procesu k uplatnění práva subjektů údajů pro každý účel zpracování samostatně,
- 4) metodiky a postupu pro realizaci záměrné ochrany,
- 5) metodiky a postupu pro realizaci standardní ochrany,
- 6) procesů k zajištění pravidelného testování a vyhodnocování účinnosti přijatých technických a organizačních opatření.

### **Podle potřeby úprava technických a organizačních opatření v těchto oblastech:**

- 1) Úprava formulace a rozsahu stávajících souhlasů subjektů údajů se zpracováním, vzhledem k právnímu základu příslušného účelu zpracování:
- 2) Revize a návrh úpravy informační povinnosti subjektům údajů s cílem poskytnout explicitně vyžadované informace přehledným a srozumitelným způsobem a do doby 30 dní.
- 3) Revize a návrh úprav procesů při uplatnění práv subjektů údajů.
- 4) Návrh úprav smluvních vztahů se Zpracovatelem a Dodavatelem služeb, v rámci kterých jsou zpracovávány osobní údaje.
- 5) Návrh úprav řešení kontrolní činnosti.

## **Etapa 3 - Pomoc při implementaci technických a organizačních opatření**

Cílem této etapy je zejména:

- 1) Vytvoření koncepce/politiky zpracování a ochrany osobních údajů, která umožní prokázat naplnění základních principů GDPR, kterými jsou:
  - g) zákonnost zpracování osobních údajů,
  - h) záměrná a standardní ochrana osobních údajů,



- i) minimalizace zpracovávaných osobních údajů,
  - j) korektnost a transparentnost při zpracování osobních údajů,
  - k) odpovídající důvěrnost, integritu a dostupnost osobních údajů,
  - l) odpovědnost správce osobních údajů.
- 2) Vypracování nebo úprava vnitřních předpisů pro řízení systému ochrany osobních údajů.

## Příloha č. 2 smlouvy o dílo – Harmonogram realizace

### 1. Harmonogram realizace – Město Šternberk

| Etapa   | Činnost  | Období  |
|---------|--|---|
| Etapa 1 | Vstupní a rozdílová analýza  | do 90 dní od podpisu smlouvy a zahájení realizace |
| Etapa 2 | Implementace kroků k dosažení souladu  | do 30 dní od ukončení etapy 1                     |
| Etapa 3 | Zpracování interních předpisů a potřebné související řídicí dokumentace pro ochranu osobních údajů | do 30 dní od ukončení etapy 2                     |

### 2. Harmonogram realizace – příspěvkové organizace

| Etapa   | Činnost   | Období  |
|---------|---|---|
| Etapa 1 | Vstupní a rozdílová analýza                                 | do 90 dní od podpisu smlouvy a zahájení realizace |
| Etapa 2 | Implementace kroků k dosažení souladu                       | do 30 dní od ukončení etapy 1                     |
| Etapa 3 | Pomoc při implementaci technických a organizačních opatření | do 30 dní od ukončení etapy 2                     |