**Část I.**

**Obecné předpoklady předmětu plnění této smlouvy – Výtah z „Koncepce GDPR v prostředí statutárního města Jablonec nad Nisou“**

Rada města Jablonce nad Nisou dne 21. 9. 2017 projednala „Koncepci GDPR v prostředí statutárního města Jablonec nad Nisou včetně Městské policie Jablonec nad Nisou a příspěvkových organizací (seznam je uveden na konci této přílohy) – dále také „Koncepce GDPR SMJN.“

Dne 27. dubna 2016 Evropský parlament schválil Obecné nařízení o ochraně osobních údajů, s účinností od 25. května 2018 – Nařízení EU číslo 2016/679 – General Data Protection Regulation (GDPR).

GDPR je vydán formou přímo účinného nařízení, které není nutné transponovat do právních řádů členských států EU.

Evropská unie si klade za cíl nastolit důvěru, která umožní rozvoj digitální ekonomiky na celém vnitřním trhu EU. Nařízení má také zamezit rozdílům bránícím volnému pohybu osobních údajů v rámci vnitřního trhu EU.

Koncepce ochrany osobních údajů musí být:

* Podrobná a srozumitelná
* Musí umožňovat posouzení souladu s GDPR
* Proveditelná
* Aktuální
* Prezentována (školena) zaměstnancům
* Kontrolovaná

„Koncepce GDPR SMJ“ respektuje následující obecné předpoklady:

**Demingův cyklus (P-D-C-A)**

PDCA (z anglického plan-do-check-act tedy naplánuj-proveď-ověř-jednej) je iterativní (tj. opakující se, cyklická) metoda vedení založená na čtyřech základních krocích. Využívají ji ty organizace, jejichž cílem je dosáhnout neustálého zdokonalování týkajícího se například [procesů](https://cs.wikipedia.org/wiki/Proces), kvality [výrobků](https://cs.wikipedia.org/wiki/V%C3%BDrobek), [služeb](https://cs.wikipedia.org/wiki/Slu%C5%BEba), aplikací atp.

S ohledem na skutečnost, že ochrana (bezpečnost) osobních údajů není (a nemůže být) z pohledu GDPR vnímána jako ochrana (bezpečnost) absolutní, je použití PDCA jedním ze základních stavebních kamenů budování koncepce ochrany (bezpečnosti) osobních údajů v organizaci.



**Jmenování DPO (Pověřenec pro ochranu osobních údajů) a pracovního týmu odpovědného za soulad principů ochrany osobních údajů v prostředí statutárního města Jablonec nad Nisou s GDPR:**

* **DPO** – je osoba, která dohlíží na dodržování GDPR, poskytuje rady a informace ohledně ochrany osobních údajů, spolupracuje s dozorovým úřadem. DPO monitoruje soulad s právem a soulad s koncepcemi (směrnice, pracovní postupy, metodika, apod.)
* **Pracovní tým odpovědný za soulad principů ochrany osobních údajů v prostředí statutárního města Jablonec nad Nisou s GDPR** – úlohou pracovního týmu je připravit a uvést prostředí (fyzická bezpečnost listinných dokumentů, objektová bezpečnost, směrnice, personalistika, ICT bezpečnost, procesy, školení, apod.) statutárního města Jablonec nad Nisou do souladu s GDPR

**Princip Data protection by design**

„Data protection by design“ je princip, jenž počítá s ochranou osobních údajů již od počátku návrhu praktického řešení jejich zpracování (může se jednat o technická řešení typu anonymizace, pseudonymizace a rozdělení oblastí s uloženými daty, nebo personální a organizační opatření).

**Princip Data protection by default**

Princip „Data protection by default“ má potom zajistit, aby v základním nastavení služby byly zpracovávány jen osobní údaje, které jsou zcela nezbytné pro její poskytování.

**Řízení rizik – Risk management**

Řízení rizik (Risk Management) je oblast řízení zaměřující se na analýzu a snížení rizika, pomocí různých metod a technik prevence rizik, které eliminují existující nebo odhalují budoucí faktory zvyšující riziko.

Riziko je všudy přítomným a charakteristickým průvodním jevem fungování organizací v soudobém [turbulentním prostředí](https://managementmania.com/cs/turbulence).

Zásadní pro řízení rizik je jejich analýza. Pomocí analýzy rizik se zjišťuje míra nebezpečí [(hrozba)](https://managementmania.com/cs/hrozba-threat), kterým je [organizace](https://managementmania.com/cs/organizace) vystavena, jak moc jsou její [aktiva](https://managementmania.com/cs/aktiva) vůči těmto hrozbám [zranitelná](https://managementmania.com/cs/zranitelnost-vulnerability), jak vysoká je pravděpodobnost, že hrozba nastane [(zranitelnost)](https://managementmania.com/cs/zranitelnost-vulnerability) a jaký dopad to na [organizaci](https://managementmania.com/cs/organizace) může mít. Základní principy řízení rizik lze shrnout do následujících tvrzení:

* Každá lidská činnost přináší určitá rizika
* Nulové riziko neexistuje

[Odpovědnost](https://managementmania.com/cs/odpovednost) za řízení rizik je v [organizacích](https://managementmania.com/cs/organizace) rozložena v rámci celého [managementu](https://managementmania.com/cs/manazer). Nejvyšší odpovědnost má přirozeně [statutární orgán](https://managementmania.com/cs/statutarni-organ) a nejvyšší management (top management) organizace.

**Využití principu AS-IS, TO-BE**

Přechod od dnešního stavu (AS-IS) do popsaného cílového stavu (TO-BE) bude trvat několik let. Tato změna bude vyžadovat nemalé investiční náklady, personální zdroje, změny mnoha informačních systémů.

**Část II.**

**Implementace GDPR v prostředí statutárního města Jablonec nad Nisou - Výtah z „Koncepce GDPR v prostředí statutárního města Jablonec nad Nisou“**

**1. Etapa – „Naplánuj“ – Inventura zpracování osobních údajů**

Cílem etapy „Naplánuj“ je inventura zpracování osobních údajů včetně komplexního návrhu nápravných opatření k zajištění souladu prostředí správce osobních údajů (statutárního města Jablonec nad Nisou) s GDPR včetně potřebných zdrojů a termínů.

**Plnění této etapy JE předmětem plnění této smlouvy.**

**2. Etapa „Proveď“ – Bezpečnostní procesy – Implementace protiopatření**

Cílem etapy „Proveď“ je implementace nápravných opatření k zajištění souladu prostředí správce osobních údajů (statutárního města Jablonec nad Nisou) s GDPR. Realizace nápravných opatření bude vycházet z výstupů vytvořených v 1. Etapě.

**Plnění této etapy NENÍ předmětem plnění této smlouvy.**

**3. Etapa „Ověř“ – Kontrola – Odchylky implementace od plánu**

Konkrétní podoba, zdroje, termíny a výstupy této etapy budou navrženy a implementovány v 1. a 2. Etapě.

**Plnění této etapy NENÍ předmětem plnění této smlouvy.**

**4. Etapa „Jednej“ – Zdokonalení – Nové bezpečnostní standardy ochrany osobních údajů**

Konkrétní podoba, zdroje, termíny a výstupy této etapy budou navrženy v 1. a 3. Etapě.

**Plnění této etapy NENÍ předmětem plnění této smlouvy.**

**Část III.**

**Předmět plnění této smlouvy – realizace části 1. etapy „Koncepce GDPR v prostředí statutárního města Jablonec nad Nisou“**

V rámci této 1. etapy chce statutární město Jablonec nad Nisou na základě prověření stávajícího stavu zpracování osobních údajů a jejich bezpečnosti stanovit cíle k nápravě zjištěných nedostatků. Součástí plnění je určení nezbytných úkolů, opatření, nástrojů a procesů k dosažení stanovených cílů, to je zajištění souladu zpracování osobních údajů s GDPR.

Cílem 1. etapy „Naplánuj“ je inventura osobních údajů včetně návrhu potřebných změn k zajištění souladu prostředí statutárního města Jablonec nad Nisou s GDPR.

Plnění předmětu této smlouvy musí respektovat:

* Obecné předpoklady předmětu plnění – Výtah z „Koncepce GDPR v prostředí statutárního města Jablonec nad Nisou“, uvedené v Části I.
* Implementace GDPR v prostředí statutárního města Jablonec nad Nisou - Výtah z „Koncepce GDPR v prostředí statutárního města Jablonec nad Nisou“, uvedené v Části II. Předmětem plnění této smlouvy je pouze 1. etapa „Koncepce GDPR SMJ“.
1. **Oblasti inventury zpracování osobních údajů:**
* Fyzické zabezpečení dat
* HW
* SW
* Sítě (LAN, WAN, MAN)
* Smlouvy (dodavatelské, odběratelské, o zpracování údajů, personální, …)
* Formuláře
* Datové sklady
* Řízení přístupových práv
* Outsourcované služby
* Zálohování dat
* Archivace dat
* Mazání údajů – právo být zapomenut
* Sledování nedovolených přístupů
* Zpracování žádostí subjektu údajů (práva subjektu údajů)
* Zpracování a hlášení incidentů včetně dokumentace incidentů
* Opatření k prokázání souladu s GDPR
* Souhlasy subjektu údajů se zpracováním údajů
1. **Osobní údaje vedené správcem:**
* Listinný dokument
* Elektronický dokument, včetně digitalizovaného listinného dokumentu
* Databáze
* Zálohy a archivace dat – strukturovaná i nestrukturovaná forma osobních údajů
1. **Aktiva**
* Primární
* Podpůrné
1. **Životní cyklus osobních údajů:**
* Vznik
* Změny
* Zpracování
* Likvidace / Anonymizace
1. **Metadata vedených osobních údajů:**
* Účel vedení osobních údajů
* Právní důvod
* Kdo/kde jsou osobní údaje vedeny
* Skupina osobních údajů opatřená o metadata, která umožní řídit celý životní cyklus
* Délka uchování osobních údajů pro jednotlivé účely
* Informace k omezení využívání osobních údajů
* Informace o předávání osobních údajů jiným zpracovatelům
* Možnosti zpracování přístupu
* Historie metadat
1. **Požadované výstupy:**

Všechny výstupy předmětu plnění budou zpracovány samostatně za:

* Magistrát města Jablonec nad Nisou – organizačně je rozdělen do 7 odborů, počet zaměstnanců 212 (data k 17.1. 2017)
* Městskou policii Jablonec nad Nisou – 50 strážníků a zaměstnanců v zázemí (data k 17.1. 2017). Městská policie spravuje kamerový systém.
* Každou jednu příspěvkovou organizaci – 32 organizací, konkrétní seznam příspěvkových organizací je uveden v Části IV.
1. **Inventura zpracovávaní osobních údajů, jejich kategorizace a posouzení souladu s GDPR**

Cílem této aktivity je provedení mapování výchozího stavu zpracování a ochrany osobních údajů v prostředí statutárního města Jablonec nad Nisou včetně Městské policie Jablonec nad Nisou a příspěvkových organizací, tj. všech procesů zpracování a datových toků osobních údajů.

Struktura inventury zpracování osobních údajů musí být plně v souladu s požadavky GDPR.

Konkrétním výstupem této aktivity je dokumentace, která bude obsahovat:

* Zpracování metodiky provedení inventury zpracování osobních údajů – způsob provedení inventury, pravidla komunikace, nástroje komunikace, proškolení na vyplňování formulářů, časový harmonogram, apod.
* Inventuru zpracování osobních údajů – zmapování zpracování osobních údajů.
* Porovnání (srovnávací analýza) provedené inventury zpracování osobních údajů s požadavky GPDR. Z předloženého výstupu bude jasně patrné, je-li konkrétní zpracování osobních údajů v souladu s požadavky GDPR či je-li konkrétní zpracování osobních údajů v nesouladu s požadavky GDPR. U nesouladu s GDPR bude uveden důvod tohoto nesouladu.

Zadavatel předpokládá, že inventura zpracování osobních údajů nebude provedena pouze vzdáleně formou elektronického sběru informací prostřednictvím dotazníků. Zadavatel předpokládá osobní a aktivní účast pracovníků dodavatele při sběru dat, vysvětlení pojmů a návodnost při vyplňování dotazníků a schopnost včasných interakcí při dotazech.

Zadavatel požaduje před započetím vlastního sběru dat fyzické proškolení všech dotčených osob zadavatele na metodiku provedení inventury zpracování osobních údajů (statutární město Jablonec nad Nisou – cca 20 osob, Městská policie Jablonec nad Nisou – cca 5 osob, příspěvkové organizace – cca 30 osob). Proškolení a sběr dat nesmí být ve větších skupinách než 15 osob.

1. **Analýza rizik včetně návrhu nápravných opatření z pohledu subjektu údajů**

Cílem této aktivity je využití výstupů z předchozí inventury zpracování osobních údajů (dle bodu a) pro ohodnocení dopadů požadavků GDPR na jednotlivé oblasti činností správce. Je nezbytné posoudit bezpečnostní rizika, která zpracování osobních údajů představuje, z pohledu subjektu údajů. Nařízení GDPR vyžaduje, aby správce osobních údajů individuálně uzpůsoboval organizační a technická opatření tomu, jak vysoké bezpečnostní riziko jejich zpracování představuje.

V rámci této aktivity je také požadováno zjištění, zdali je správce povinen vždy jmenovat pověřence pro ochranu osobních údajů (DPO).

Analýza bezpečnostních rizik bude provedena z pohledu subjektu údajů.

Zadavatel předpokládá, že každé bezpečnostní riziko bude škálovatelné v rozsahu – nízké, střední, vysoké a kritické.

Konkrétním výstupem této aktivity je dokumentace, která bude obsahovat:

* Seznam bezpečnostních rizik – konkrétní výčet možných rizik
* Přiřazení a ohodnocení míry bezpečnostního rizika konkrétním výstupům z inventury zpracování osobních údajů
* Návrh (doporučení) nápravných opatření ke snížení míry bezpečnostního rizika při zpracování osobních údajů u konkrétních bezpečnostních rizik ohodnocených kategorií střední, vysoké či kritické. Návrhem je míněno doporučení uchazeče ke snížení míry bezpečnostního rizika vč. obecné specifikace typu opatření.
1. **Návrh organizačních opatření zajišťující soulad s GDPR včetně systému vzdělávání (školení) zaměstnanců. V rámci systému vzdělávání (školení) zaměstnanců bude zohledněna také možnost vytvoření e-learningových kurzů**

Cílem této aktivity je sumarizace předchozích aktivit z pohledu organizačních opatření (doporučení systémové regulace formou vnitřních předpisů, vzdělávání, apod.), která jsou uchazečem doporučeny realizovat, tak aby zpracování osobních údajů bylo v souladu s GDPR, případně bylo sníženo bezpečnostní riziko zpracování osobních údajů.

Každému jednomu doporučenému organizačnímu nápravnému opatření bude přiřazena priorita v rozsahu 1 až 3, kde 1 je „realizovat okamžitě“, 2 je „realizovat v horizontu měsíců“ a 3 je „realizovat v horizontu roků“.

Návrhem je míněno pouhé doporučení dodavatele. Zadavatel u  návrhu organizačních opatření nepředpokládá podrobný popis konkrétního návrhu organizačního opatření (např. není požadováno zpracování konkrétního návrhu směrnice), ale pouze doporučení, že oblast je třeba regulovat a jak. Konkrétním výstupem této aktivity je dokumentace, která bude obsahovat:

* Seznam doporučených organizačních opatření – konkrétní výčet doporučených organizačních opatření včetně určení priority.
1. **Návrh technických opatření zajišťující soulad s GDPR**

Cílem této aktivity je sumarizace předchozích aktivit z pohledu technických opatření (hardware, software, vybavení kanceláře, objektová bezpečnost, apod.), která jsou uchazečem doporučeny realizovat, tak aby zpracování osobních údajů bylo v souladu s GDPR, případně bylo sníženo bezpečnostní riziko zpracování osobních údajů.

Každému jednomu doporučenému technickému nápravnému opatření bude přiřazena priorita v rozsahu 1 až 3, kde 1 je „realizovat okamžitě“, 2 je „realizovat v horizontu měsíců“ a 3 je „realizovat v horizontu roků“.

Návrhem je míněno pouhé doporučení uchazeče. Zadavatel u  návrhu technických opatření nepředpokládá podrobný popis konkrétního návrhu technického opatření (např. není požadováno zpracování konkrétního technické specifikace hardware), tato aktivita bude předmětem plnění 2. etapy „Koncepce GDPR SMJ“.

Konkrétním výstupem této aktivity je dokumentace, která bude obsahovat:

* Seznam doporučených technických opatření – konkrétní výčet doporučených technických opatření včetně určení priority

**Část IV.**

**Seznam orgánů a organizací**

**Orgány města:**

1. Statutární město Jablonec nad Nisou – Magistrát města Jablonec nad Nisou;
2. Statutární město Jablonec nad Nisou – Městská policie Jablonec nad Nisou;

**Další organizace:**

1. Centrum sociálních služeb Jablonec nad Nisou, p.o.;
2. [Dům dětí a mládeže Vikýř, Jablonec nad Nisou, Podhorská 49, příspěvková organizace](http://www.mestojablonec.cz/redakce/index.php?lanG=cs&clanek=303&slozka=23&detaildb=27&);
3. [Městská knihovna Jablonec nad Nisou, p.o.](http://www.mestojablonec.cz/redakce/index.php?lanG=cs&clanek=303&slozka=23&od=20&detaildb=26&)

**Mateřské školy:**

1. [Mateřská škola Jablonec nad Nisou - Jablonecké Paseky, Tichá 19, příspěvková organizace](http://www.mestojablonec.cz/redakce/index.php?lanG=cs&clanek=303&slozka=23&detaildb=1821&)
2. [Mateřská škola Jablonec nad Nisou - Kokonín, Dolní 3969, příspěvková organizace](http://www.mestojablonec.cz/redakce/index.php?lanG=cs&clanek=303&slozka=23&detaildb=1820&)
3. [Mateřská škola Jablonec nad Nisou - Mšeno, Josefa Hory 31, příspěvková organizace](http://www.mestojablonec.cz/redakce/index.php?lanG=cs&clanek=303&slozka=23&detaildb=1822&)
4. [Mateřská škola Jablonec nad Nisou - Mšeno, Mechová 10, příspěvková organizace](http://www.mestojablonec.cz/redakce/index.php?lanG=cs&clanek=303&slozka=23&detaildb=1819&)
5. [Mateřská škola Jablonec nad Nisou - Rýnovice, Československé armády 37, příspěvková organizace](http://www.mestojablonec.cz/redakce/index.php?lanG=cs&clanek=303&slozka=23&detaildb=1818&)
6. [Mateřská škola Jablonec nad Nisou – Mšeno, Arbesova 50, příspěvková organizace](http://www.mestojablonec.cz/redakce/index.php?lanG=cs&clanek=303&slozka=23&od=10&detaildb=1888&)
7. [Mateřská škola Jablonec nad Nisou, 28. října 16, příspěvková organizace](http://www.mestojablonec.cz/redakce/index.php?lanG=cs&clanek=303&slozka=23&od=10&detaildb=1885&)
8. [Mateřská škola Jablonec nad Nisou, Havlíčkova 4, příspěvková organizace](http://www.mestojablonec.cz/redakce/index.php?lanG=cs&clanek=303&slozka=23&od=10&detaildb=1143&)

ch) [Mateřská škola Jablonec nad Nisou, Hřbitovní 10, příspěvková organizace](http://www.mestojablonec.cz/redakce/index.php?lanG=cs&clanek=303&slozka=23&od=10&detaildb=1887&)

1. [Mateřská škola Jablonec nad Nisou, Husova 3, příspěvková organizace](http://www.mestojablonec.cz/redakce/index.php?lanG=cs&clanek=303&slozka=23&od=10&detaildb=1886&)
2. [Mateřská škola Jablonec nad Nisou, Jugoslávská 13, příspěvková organizace](http://www.mestojablonec.cz/redakce/index.php?lanG=cs&clanek=303&slozka=23&od=10&detaildb=1817&)
3. [Mateřská škola Jablonec nad Nisou, Lovecká 11, příspěvková organizace](http://www.mestojablonec.cz/redakce/index.php?lanG=cs&clanek=303&slozka=23&od=10&detaildb=1815&)
4. [Mateřská škola Jablonec nad Nisou, Nová Pasířská 10, příspěvková organizace](http://www.mestojablonec.cz/redakce/index.php?lanG=cs&clanek=303&slozka=23&od=10&detaildb=1889&)
5. [Mateřská škola Jablonec nad Nisou, Slunečná 9, příspěvková organizace](http://www.mestojablonec.cz/redakce/index.php?lanG=cs&clanek=303&slozka=23&od=10&detaildb=1890&)
6. [Mateřská škola Jablonec nad Nisou, Střelecká 14, příspěvková organizace](http://www.mestojablonec.cz/redakce/index.php?lanG=cs&clanek=303&slozka=23&od=10&detaildb=1816&)
7. [Mateřská škola Jablonec nad Nisou, Švédská 14, příspěvková organizace](http://www.mestojablonec.cz/redakce/index.php?lanG=cs&clanek=303&slozka=23&od=20&detaildb=1891&)
8. [Mateřská škola Montessori Jablonec nad Nisou, Zámecká 10, příspěvková organizace](http://www.mestojablonec.cz/redakce/index.php?lanG=cs&clanek=303&slozka=23&od=20&detaildb=1630&)
9. [Mateřská škola speciální Jablonec nad Nisou, Palackého 37, příspěvková organizace](http://www.mestojablonec.cz/redakce/index.php?lanG=cs&clanek=303&slozka=23&od=20&detaildb=892&)

**Základní školy:**

1. [Základní škola Jablonec nad Nisou - Mšeno, Arbesova 30, příspěvková organizace](http://www.mestojablonec.cz/redakce/index.php?lanG=cs&clanek=303&slozka=23&od=20&detaildb=894&)
2. [Základní škola Jablonec nad Nisou - Mšeno, Mozartova 24, příspěvková organizace](http://www.mestojablonec.cz/redakce/index.php?lanG=cs&clanek=303&slozka=23&od=20&detaildb=897&)
3. [Základní škola Jablonec nad Nisou - Kokonín, Rychnovská 216, příspěvková organizace](http://www.mestojablonec.cz/redakce/index.php?lanG=cs&clanek=303&slozka=23&od=30&detaildb=895&)
4. [Základní škola Jablonec nad Nisou - Rýnovice, Pod Vodárnou 10, příspěvková organizace](http://www.mestojablonec.cz/redakce/index.php?lanG=cs&clanek=303&slozka=23&od=30&detaildb=901&)
5. [Základní škola Jablonec nad Nisou, 5. května 76, příspěvková organizace](http://www.mestojablonec.cz/redakce/index.php?lanG=cs&clanek=303&slozka=23&od=30&detaildb=893&)
6. [Základní škola Jablonec nad Nisou, Liberecká 26, příspěvková organizace](http://www.mestojablonec.cz/redakce/index.php?lanG=cs&clanek=303&slozka=23&od=30&detaildb=896&)
7. [Základní škola Jablonec nad Nisou, Na Šumavě 43, příspěvková organizace](http://www.mestojablonec.cz/redakce/index.php?lanG=cs&clanek=303&slozka=23&od=30&detaildb=898&)
8. [Základní škola Jablonec nad Nisou, Pasířská 72, příspěvková organizace](http://www.mestojablonec.cz/redakce/index.php?lanG=cs&clanek=303&slozka=23&od=30&detaildb=899&)
9. [Základní škola Jablonec nad Nisou, Pivovarská 15, příspěvková organizace](http://www.mestojablonec.cz/redakce/index.php?lanG=cs&clanek=303&slozka=23&od=30&detaildb=900&)
10. Základní umělecká škola, Jablonec nad Nisou, Podhorská 47, příspěvková organizace.

**Specifické organizace:**

Jablonecká dopravní a.s.

*Pozn. Zde jde o nově založený podnik pro zajištění dopravní obslužnosti. Podnik zatím nevyvíjí žádnou činnost; cílem analýzy je jen definovat jeho povinnosti na úseku GDPR a navrhnout seznam opatření, které je třeba provést, aby plnil svije povinnosti.*

*Bližší údaje o všech organizacích (vyjma Jablonecké dopravní) jsou na: http://www.mestojablonec.cz/redakce/index.php?lanG=cs&clanek=303&slozka=23&*

V Jablonci nad Nisou dne: ………….. V Liberci dne: 8.2.2018

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

statutární město Jablonec nad Nisou Liberecká IS, a.s.

Ing. Petr Beitl Ing. Jaroslav Bureš, MBA

primátor statutární ředitel