Město Chropyně
Náměstí Svobody 29
768 11, Chropyně

Praze dne 12. 2. 2018

Věc: **Žádost o poskytnutí informace podle zákona č. 106/1999 Sb.**

Povinný subjekt:
město Chropyně
se sídlem: Náměstí Svobody 29, 768 11, Chropyně

dále jen jako „*Povinný subjekt*"

Žadatel:
KAMIKA TRADING, s.r.o.
se sídlem: Praha 5 - Smíchov, Holečkova 619/59, PSČ 150 00
IČ: 247 70 078

Znění žádosti:

Vážení,
ráda bych tímto přípisem požádala Povinný subjekt o poskytnutí informací dle zákona č. 106/1999 Sb., o svobodném přístupu k informacím, a to formou odpovědi na níže uvedené otázky:

1. **Jakým způsobem zajišťujete (příp. hodláte zajistit) soulad zpracování osobních údajů s Obecným nařízením o ochraně osobních údajů (Nařízení EP a Rady (EU) č. 2016/679) tzv. GDPR?**

2. **Zadali jste nebo plánujete zadat v rámci zadávacího řízení veřejnou zakázku na dodávku služeb pro zajištění souladu vaší organizace s Obecným nařízením o ochraně osobních údajů?**

3. V případě, že odpověď na otázku č. 2 je kladná, pak:
   a. **Uveďte termín (plánovaný termín), kdy bude zadávací řízení uveřejněno.**

4. V případě, že odpověď na otázku č. 2 je kladná, pak:
   a. **Zajišťujete (hodláte zajistit) soulad zpracování osobních údajů s Obecným nařízením o ochraně osobních údajů pouze pro svůj obecní úřad, nebo i pro příspěvkové organizace, zřízené vaší obcí?**

5. V případě, že již máte vybraného dodavatele služeb pro zajištění souladu vaší organizace (příp. i vámi zřizovaných příspěvkových organizací) s Obecným nařízením o ochraně osobních údajů, pak:
   a. **Kdo je dodavatelem těchto služeb?**
   b. **Byl tento dodavatel vybrán na základě zadávacího řízení veřejné zakázky?**
   c. **Jaká je cena, za kterou jsou tyto služby poskytovány?**
   d. **Žádám o zaslání veškeré smluvní dokumentace, na základě které jsou tyto služby vaší organizaci poskytovány.**

Předem děkuji za kladné vyřízení mé žádosti.

V úctě

KAMIKA TRADING, s.r.o.

MĚSTO CHROPYNĚ

náměstí Svobody 29, 768 11 Chropyně

KAMIKA TRADING, s. r. o.
Holečkova 619/59
150 00 PRAHA 5-SMÍCHOV

IDDS: kguwmyz

VÁŠ DOPIS ZN.:
ZE DNE: 2018-02-12 00:00:00.000
NAŠE ZNAČKA: MCH 1028/2018
SPISOVÁ ZNAČKA:
ID PÍSEMNOSTI: MECHX003ZW35

VYŘIZUJE: Ing. Jiří Rosecký
TEL.: 573500735
E-MAIL: rosecky@muchropyne.cz

DATUM: 21.02.2018

Podání informace

Vážená paní,

dne 12.02.2018 jste požádali o poskytnutí informace podle zákona č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů (dále jen „zákon"). Jako povinný subjekt podle zákona jsme Vaši žádost posoudili a v souladu s ustanovením § 14 odst. 5 písm. d) zákona Vám poskytujeme tyto informace:

ad 1) Soulad zpracování osobních údajů s Obecným nařízením o ochraně osobních údajů zajišťujeme využitím služeb externích dodavatelů služeb.

ad 2) Nezadali jsme ani neplánujeme zadat v rámci zadávacího řízení veřejnou zakázku na dodávku služeb v této věci.

ad 4) Na tuto otázku odpovídáme i přes zápornou odpověď na otázku č. 2, neboť nutnost kladné odpovědi na ni nevnímáme jako důležitou. Město Chropyně zajišťuje soulad zpracování osobních údajů pouze pro Městský úřad Chropyně. Příspěvkové organizace zřízené městem si soulad zpracování osobních údajů s nařízením EU zajišťují samy. Dle nám dostupných informací i ony již mají své dodavatele služeb.

ad 5) Dodavatelem služeb na zajištění souladu zpracování osobních údajů pro město Chropyně je firma I3 Consultants, s. r. o., IČ: 27921344, se sídlem K Trninám 945/34, 163 00 Praha 6-Řepy. S odkazem na odpověď ad 2) doplňujeme, že tato firma byla vybrána v souladu s vnitřní směrnicí města Chropyně o zadávání veřejných zakázek formou poptávkového řízení (4 firmy), na základě průzkumu trhu a výborných zkušeností s touto firmou z jiných měst a obcí. Cena za služby je 113.000 Kč bez DPH. Služby nejsou poskytovány na základě uzavřené smlouvy, ale na základě objednávky (uzavřené v souladu s vnitřní směrnicí města), jejíž nedílnou součástí je nabídka dodavatele, která obsahuje veškeré potřebné informace a závazky dodavatele. Objednávka i nabídka jsou přílohou tohoto poskytnutí informací.

S pozdravem

Ing. Jiří Rosecký
tajemník městského úřadu
podepsáno elektronicky

Digitálně podepsal Ing. Jiří Rosecký
Datum: 2018.02.21 11:28:30 +01'00'

Přílohy

Elektronický podpis - 19.10.2017
Certifikát autora podpisu :
Jméno : Ing. Jiří Rosecký
Vydal : PostSignum Qualified C...
Platnost do : 19.9.2018

MĚSTO CHROPYNĚ

náměstí Svobody 29, 768 11 Chropyně

ČÍSLO OBJEDNÁVKY: OBJ2017/0045

VYŘIZUJE: Rosecký Jiří Ing.
TEL.: 573500735
E-MAIL: rosecky@muchropyne.cz
IDDS: rbsbexq

DATUM TISKU: 17.10.2017

I3 Consultants s.r.o.
K trninám 945/34
16300 PRAHA

Objednávka "Zavedení systému ochrany osobních údajů dle GDPR"

Vážený pane [redacted]

objednáváme u Vás službu "Zavedení systému ochrany osobních údajů dle GDPR" dle Vaší nabídky číslo 64/2017 ze dne 29.09.2017. Uvedená nabídka je nedílnou součástí této objednávky. Počátek realizace zavedení systému je stanoven na 01.11.2017.

Cena za službu činí 113.000 Kč + 21 % DPH, tedy celkem 136.730 Kč. Jedná se o cenu maximální a nepřekročitelnou.

Objednávku uhradíme na základě Vámi vystavené faktury se splatností 14 dnů. Na faktuře, prosíme, uvádějte číslo objednávky OBJ2017/0045 a celkovou cenu. Město Chropyně není plátcem DPH.

S pozdravem

Ing. Jiří Rosecký
tajemník městského úřadu

I3 Consultants s.r.o., K Trninám 645/34, 163 00 Praha

Dne: 29. září 2017

ČN: 64/2017

Město Chropyně
Nám. Svobody 29
768 11 Chropyně

I3 Consultants
INGENIOSUS INTER INGENIOSI

NABÍDKA

"Zavedení systému ochrany osobních údajů dle GDPR"

1 Souhrn nabídky

1.1 Úvodem

Společnost I3 Consultants s.r.o. si dovoluje předložit nabídku na spolupráci při přechodu města Chropyně do podmínek nové evropské legislativy (*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 – General Data Protection Regulation)*, formou implementace nařízení GDPR na Městském úřadě Chropyně.

V předložené nabídce je popsáno naše pochopení Vašich potřeb a současně náš přístup k jejich zajištění.

Nabízíme pouze ty služby, které jsme schopni plně garantovat a jejich kvalitu prokázat odpovídajícími referencemi, které přesně odpovídají poptávanému a současně nabízenému řešení.

1.2 Představení společnosti

1.2.1 Identifikační údaje

Obchodní název: I3 Consultants s.r.o.
Sídlo: K Trninám 945/34, 163 00 Praha 6 - Řepy
Adresa pobočky společnosti: Scheinerova 1570/6, 628 00 Brno
Tel./fax: +420 233 311 973
Mobil: +420 602 766 240
E-mail: info@i3c.cz
Statutární orgán: Ing. Tomáš Kubínek, jednatel; Ing. Igor Prosecký, jednatel
IČ: 279 21 344
DIČ: CZ 279 21 344
Zapsáno v obchodním rejstříku vedeného Městským soudem v Praze oddíl C, vložka 126634

1.2.2 Profil společnosti

I3 Consultants s.r.o. je konzultační a poradenskou společností, orientující se na poskytování služeb ve všech oblastech bezpečnosti informací s důrazem na oblast ochrany osobních údajů, kybernetické bezpečnosti a implementaci standardů ISMS a ITSM (ISO/IEC 27001 a 20000).

Společnost je držitelem:

- osvědčení podnikatele umožňující přístup k utajované informaci stupně utajení Důvěrné,
- certifikátu systému managementu kvality dle standardu ČSN EN ISO 9001:2009.

1.2.3 Reference a garance kvality

Vybrané referenční zakázky v oblasti bezpečnosti informací a ochrany osobních údajů:

Ministerstvo práce a sociálních věcí ČR
- ✓ zavedení jednotného systému řízení bezpečnosti informací v resortu - 2015

Ministerstvo životního prostředí ČR
- ✓ posouzení stávajícího stavu a zavedení systému ochrany osobních údajů – 2011
- ✓ Bezpečnostní politiky informací ministerstva - 2012

Ministerstvo pro místní rozvoj ČR
- ✓ posouzení stávajícího stavu a zavedení systému ochrany osobních údajů – 2011
- ✓ GAP analýza kybernetické bezpečnosti - 2015
- ✓ zajištění bezpečnostního dohledu MS 2014+ v oblasti řízení bezpečnosti informací a oblasti zpracování a ochrany osobních údajů – 2015 - dosud

Ministerstvo zemědělství ČR, sekce Pozemkové úřady
- ✓ ověření zavedeného systému zpracování osobních údajů a navržení jeho optimalizace, která zajistí plnou shodu zjištěných zpracování osobních údajů s požadavky zákona o ochraně osobních údajů – 2012
  Realizace projektu proběhla u všech 91 organizačních celků ve čtyřech na sobě navazujících etapách:
  - analýza současného stavu ochrany osobních údajů u ÚPÚ,
  - návrh optimalizace činností v oblasti ochrany osobních údajů, sumarizace výstupů z provedené analýzy,
  - implementace opatření zaměřených na optimalizaci systému ochrany osobních údajů,
  - zajištění akreditovaného školení pro zaměstnance ÚPÚ.

Ministerstvo kultury ČR
- ✓ provedení analýzy potřeb bezpečnostních služeb u Ministerstva kultury ČR a jím zřízených příspěvkových organizací, poradenských služeb v oblasti fyzické bezpečnosti při zadávání veřejné zakázky na poskytování bezpečnostních služeb v objektech Ministerstva kultury a jeho příspěvkových organizací a fondů 2012 - 2014
- ✓ posouzení stávající dokumentace ISMS s požadavky zákona o kybernetické bezpečnosti a vypracování nové dokumentace v souladu s požadavky zákona

Generální finanční ředitelství
- ✓ ustavení systému řízení bezpečnosti informací - 2014

Policejní prezidium České republiky – KB
- ✓ ustavení systému řízení bezpečnosti informací - 2016

Český statistický úřad
- ✓ srovnávací analýza souladu systémů s požadavky zákona o kybernetické bezpečnosti – 2015
- ✓ posouzení stávajícího stavu ochrany osobních údajů - 2015

Česká školní inspekce
- ✓ Validace akceptace, ISVS certifikace a implementace pravidel kybernetické bezpečnosti pro informační systém projektu NIQES - 2015
  - implementace požadavků souvisejících s legislativou vztahující se k oblasti kybernetické bezpečnosti, provozu ISVS a ochrany osobních údajů,
  - příprava informačních systémů veřejné správy k atestaci dle zákona č. 365/2000 Sb., včetně zpracování dokumentace,
  - provedení bezpečnostní prověrky s cílem ověřit shodu v oblasti kybernetické bezpečnosti,
  - provedení bezpečnostní prověrky s cílem ověřit shodu v oblasti ochrany osobních údajů - 2015.

Liberecký kraj – Krajský úřad Libereckého kraje
- ✓ zavedení systému řízení bezpečnosti informací dle skupiny norem ČSN ISO/IEC 27000 a zákona č. 181/2014 Sb., o kybernetické bezpečnosti, včetně Nařízení Evropského parlamentu a Rady (EU) 2016/679 (GDPR) - 2017

Jihomoravský kraj – Krajský úřad Jihomoravského kraje
- ✓ posouzení stávajícího stavu a zavedení systému ochrany osobních údajů - 2008

Jihočeský kraj – Krajský úřad Jihočeského kraje
- ✓ posouzení stávajícího stavu a zavedení systému ochrany osobních údajů - 2015

Ústecký kraj – Krajský úřad Ústeckého kraje
- ✓ posouzení stávajícího stavu a zavedení systému ochrany osobních údajů - 2016

Zlínský kraj – Krajský úřad Zlínského kraje
- ✓ zpracování analýzy rizik a bezpečnostní dokumentace dle požadavků zákona o kybernetické bezpečnosti - 2016

Česká republika – Krajské státní zastupitelství Brno
- ✓ posouzení stávajícího stavu a zavedení systému ochrany osobních údajů - 2008
- ✓ ustavení systému řízení bezpečnosti informací – 2008

Česká republika – Krajský soud v Brně
- ✓ ustavení systému řízení bezpečnosti informací ISMS - 2014

Česká republika – Městský soud Praha, Městský soud v Brně, Okresní soud ve Žďáru nad Sázavou, v Kroměříži, v Blansku, v Hodoníně, ve Vyškově a další ...
- ✓ ustavení systému řízení bezpečnosti informací

Hlavní město Praha – Magistrát hlavního města Prahy – Odbor školství, mládeže a tělovýchovy
- ✓ posouzení stávajícího stavu a zavedení systému ochrany osobních údajů ve vybraných školách a školských zařízeních

Statutární město Brno – Magistrát města Brna, Městská policie Brno
- ✓ ustavení systému řízení bezpečnosti informací - 2011
- ✓ posouzení stávajícího stavu a zavedení systému ochrany osobních údajů – 2011
- ✓ outsourcing výkonu role Manažera bezpečnosti informací – 2012 - dosud

Statutární město Olomouc – Magistrát města Olomouc
- ✓ ustavení systému řízení bezpečnosti informací v rozsahu norem ISO 27000 a zákona o kybernetické bezpečnosti 2016 - 2017

Statutární město Kladno – Magistrát města Kladna
- ✓ posouzení stávajícího stavu a zavedení systému ochrany osobních údajů - 2009
- ✓ analýza rizik IS a vypracování návazné dokumentace - 2010

Statutární město Jihlava – Magistrát města Jihlavy
- ✓ posouzení stávajícího stavu a zavedení systému ochrany osobních údajů - 2010

Městský úřad Boskovice, Břeclav, Žďár nad Sázavou, Turnov, Uničov, Kyjov, Moravský Krumlov, Mikulov, Šumperk, Štemberk, Pohořelice a další ...
- ✓ posouzení stávajícího stavu a zavedení systému ochrany osobních údajů

Městská část Praha 1
- ✓ posouzení stávajícího stavu a zavedení systému ochrany osobních údajů - 2010

Městská část Praha 4
- ✓ posouzení stávajícího stavu a zavedení systému ochrany osobních údajů ve vybraných školách a školských zařízeních - 2014

Městská část Praha 5
- ✓ Aktualizace a konsolidace ISMS – 2013 - 2014
- ✓ posouzení současného stavu a zavedení systému ochrany osobních údajů 2013 - 2014
- ✓ posouzení stavu ochrany osobních údajů ve vybraných školách a školských zařízeních - 2013

Městská část Praha 12
- ✓ posouzení stávajícího stavu a zavedení systému ochrany osobních údajů ve vybraných školách a školských zařízeních - 2012

Městská část Praha 15
- ✓ posouzení stávajícího stavu a zavedení systému ochrany osobních údajů - 2012
- ✓ posouzení stávajícího stavu a zavedení systému ochrany osobních údajů ve vybraných školách a školských zařízeních - 2013

Fakultní nemocnice Plzeň
- ✓ Zpracování dokumentace pro ochranu osobních údajů v kamerovém systému včetně podkladů pro registraci - 2012

Fakultní nemocnice Ostrava
- ✓ zpracování návrhu strategie a koncepce bezpečnosti informací - 2011
- ✓ posouzení současného stavu a zavedení systému ochrany osobních údajů – 2011
- ✓ Provedení analýzy současného stavu zpracování a ochrany osobních údajů s cílem vytvořit výchozí podmínky pro implementaci obecného nařízení o ochraně osobních údajů (GDPR) - 2017
- ✓ provedení GAP analýzy požadavků zákona o kybernetické bezpečnosti (ZKB) - 2017
- ✓ provedení GAP analýzy požadavků nařízení Evropského parlamentu a Rady (EU) č. 910/2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu (eIDAS) - 2017

Karlovarská krajská nemocnice a.s.
- ✓ posouzení současného stavu a zavedení systému ochrany osobních údajů – 2011

Masarykův onkologický ústav Brno
- ✓ Ustavení a zavedení systému řízení bezpečnosti informací – 2011

Povodí Vltavy, státní podnik
- ✓ Provedení vstupní a rozdílové analýzy stavu zpracování a ochrany osobních údajů v souvislosti s přípravou k přechodu k GDPR, zpracování interních předpisů a potřebné související řídící dokumentace, včetně implementace systému OOÚ dle GDPR - 2017

Muzeum hl. m. Prahy
- ✓ posouzení současného stavu a zavedení systému ochrany osobních údajů – 2011

Unis a.s.
- ✓ ustavení a zavedení systému řízení bezpečnosti informací – 2010
- ✓ zavedení systému managementu poskytování IT služeb (ITSM) - 2010

Unicontrols a.s.
- ✓ ustavení a zavedení systému řízení bezpečnosti informací - 2017

Panasonic AVC Networks Czech, s.r.o.
- ✓ ustavení a zavedení systému řízení bezpečnosti informací – 2012, Analýza rizik - 2015
- ✓ posouzení současného stavu a zavedení systému ochrany osobních údajů - 2012

ČD-Telematika a.s.

- ✓ ustavení a zavedení systému řízení bezpečnosti informací – 2010, aktualizace ISMS - 2015
- ✓ zavedení systému managementu poskytování IT služeb (ITSM) - 2010

Brněnské komunikace a.s.
- ✓ ustavení a zavedení systému řízení bezpečnosti informací - 2015
- ✓ posouzení stávajícího stavu a zavedení systému ochrany osobních údajů – 2012
- ✓ zabezpečení činností v oblasti bezpečnosti informací a ochrany osobních údajů – 2012 - dosud

Dopravní podnik města Brna, a.s.
- ✓ ustavení systému řízení bezpečnosti informací - 2015
- ✓ posouzení současného stavu a zavedení systému ochrany osobních údajů - 2013
- ✓ příprava registrace vnitřního kamerového systému se záznamem pro dopravní prostředky DPMB – 2013 – 2015

Dopravní podnik hl. m. Prahy, akciová společnost
- ✓ Příprava registrace vnitřního kamerového systému se záznamem pro dopravní prostředky DPP – 2016

Dopravní společnost Zlín – Otrokovice, s.r.o.
- ✓ posouzení současného stavu a zavedení systému ochrany osobních údajů - 2011

Dopravní podnik města Jihlavy, a.s.
- ✓ posouzení současného stavu a zavedení systému ochrany osobních údajů - 2011

Plzeňské městské dopravní podniky, a.s.
- ✓ Příprava registrace vnitřního kamerového systému se záznamem pro dopravní prostředky PMDP, a.s. - 2014

Zdravotnická záchranná služba Jihomoravského kraje, p. o.
- ✓ posouzení stávajícího stavu a zavedení systému ochrany osobních údajů - 2013
- ✓ Příprava registrace kamerových systémů ZZS JmK - 2016

Tchibo ČR
- ✓ posouzení stávajícího stavu a zavedení systému ochrany osobních údajů – 2015

CENTRA a.s.
- ✓ Provedení vstupní a rozdílové analýzy stavu zpracování a ochrany osobních údajů v souvislosti s přípravou k přechodu k GDPR - 2017

2 Informace ke změně legislativy při zpracování a ochraně osobních údajů

Pro sjednocení pravidel ochrany osobních údajů ve všech státech EU bylo dne 4. května 2016 v Úředním věstníku Evropské unie zveřejněno *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 – General Data Protection Regulation)*, dále jen *„GDPR"*.

GDPR bude účinné jednotně v členských zemích EU dnem 25. května 2018. V České republice tak nahradí současnou právní úpravu ochrany osobních údajů, tj. zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů, kterým byly do národního

prostřední transponovány povinnosti k ochraně osobních údajů vyplývající z již výše uvedené směrnice 95/46/ES.

GDPR představuje doposud nejucelenější soubor pravidel na ochranu dat. Nevyhnutně se dotkne každého, kdo shromažďuje nebo zpracovává osobní údaje obyvatel evropských zemí, a to včetně společností a institucí mimo území EU, které na evropském trhu působí. Je zřejmé, že všechny organizace musí reagovat na novou právní úpravu a budou muset upravit způsob zpracovávání osobních údajů.

GDPR rozvíjí a výrazně posiluje práva subjektů údajů (dotčených fyzických osob, kterým osobní údaje patří) s cílem zajistit možnost získat informaci o tom, které jejich údaje a z jakého důvodu jsou zpracovávány a současně mít možnost domáhat se dodržování stanovených pravidel, a to včetně nápravy stavu. Je tedy založeno na vymahatelnosti práv subjektů údajů a povinností správců (subjektů odpovědných za zpracování). Ve srovnání se stávajícím zákonem o ochraně osobních údajů stanovuje preciznější a propracovanější pravidla při zpracování osobních údajů a při jejich ochraně, což přináší zásadní změny a v určitých případech i úplně nová pravidla do stávajícího systému zpracování a ochrany osobních údajů.

Nově se Města Chropyně bude týkat celá řada změn a institutů, ke kterým patří zejména:

Data Protection by Design, by Default (záměrná a nezbytná ochrana)

- ✓ implementace a zajištění prokazatelnosti **záměrné a nezbytné ochrany** („Data Protection by Design, by Default") osobních údajů zpracovávaných v listinné i elektronické podobě, a to ve všech fázích jejich životního cyklu,
  - **„by design"** – návrh vhodných technických a organizačních opatření již při **vývoji, návrhu, přípravě nebo tvorbě účelů a prostředků** zpracování,

  - **„by default" – technická a organizační opatření musí zajišťovat, aby byly zpracovávány pouze nezbytné údaje.**

Data Protection Impact Assessment (posouzení vlivu)

- ✓ nastavení nového způsobu spolupráce s dozorovým úřadem v závislosti na nutnosti provedení **posouzení vlivu** („Data Protection Impact Assessment") na ochranu osobních údajů u některých zpracování a případné vyžádání konzultace s dozorovým úřadem.

Testování kompatibility/proporcionality (zákonnost)

- ✓ nutnost provést u některých zamýšlených účelů zpracování **test** kompatibility/proporcionality s cílem posoudit zákonnost zpracování.

Data Protection Officer (pověřenec)

- ✓ povinnost jmenovat **pověřence pro ochranu osobních údajů** (Data Protection Officer – „DPO"), včetně zavedení všech procesů souvisejících s výkonem jeho působnosti.

Legitimate Interest (oprávněný zájem správce)

- ✓ možnost zpracovávat osobní údaje na základě „ **oprávněného zájmu** „ správce.

Souhlas (subjektu údajů, jako právní titul pro zpracování)

- ✓ nové aspekty pro udělení „souhlasu se zpracováním", vysoká pravděpodobnost **přeformulování** všech doposud udělených souhlasů s cílem získat schopnost doložit, že souhlas byl „Svobodný", „Konkrétní", „Informovaný", „Jednoznačný" a v případě zvláštních kategorií údajů „Výslovný".

Právo na Portabilitu (právo na přenositelnost svých osobních dat)

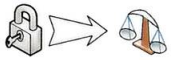
- ✓ možnost **„přenositelnosti"** osobních údajů, zpracovávaných automatizovaně, k jinému správci.

Risk Assessment (posouzení rizik)

- ✓ provedení **analýzy/posouzení rizik** zpracování a ochrany osobních údajů, s cílem vyhodnotit závažnost zjištěných rizik a navrhnout opatření k jejich eliminaci,
- ✓ pro posouzení rizik lze využít standardizovaných metodik pro analýzu rizik dle ISO řady 31000 a 27000, je však nutné zohlednit další rizika jakými jsou např. riziko neoprávněného shromažďování, předávání atd.

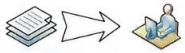
CIA: Confidentality – Integrity - Availability (důvěrnost, integrita a dostupnost osobních údajů)

- ✓ zajištění případné **pseudonymizace** údajů u účelů zpracování, kde toto oddělení určitých informací může vést k vyšší záměrné či standardní ochraně osobních údajů,
- ✓ zajištění dalších opatření k ochraně osobních údajů formou např. **šifrování, minimalizací, obnovou dostupnosti nebo pravidelným testováním a hodnocením účinnosti** k ochraně údajů se schopností odůvodnit, proč byla, respektive nebyla uplatněna výše uvedená opatření, doporučená GDPR,
- ✓ nastavení **politiky uchování a mazání dat** odpovídající uchování a likvidaci dat v listinné podobě – **ZÁSADNÍ PROBLÉM.**



Hlášení incidentů (Ohlašovací povinnost při narušení bezpečnosti údajů)

- ✓ nastavení procesu **ohlašovací povinnosti** v případě narušení bezpečnosti údajů dozorovému orgánu (v určitých případech i subjektu údajů) do časového limitu 72 hodin od okamžiku, kdy bylo toto narušení zjištěno.



Evidence údajů (záznamy o činnostech zpracování)

- ✓ zpracování **záznamů o činnostech** zpracování, které musí být zpracovány pro všechny existující účely zpracování (pokud nebude možné uplatnit výjimku z této povinnosti).

Zcela zásadní změnou je povinnost správce zajistit soulad přijatých a zdokumentovaných technických a organizačních opatření se všemi požadavky GDPR a současně být schopen je aktivně prokázat. Zákon č. 101/2000 Sb. tuto povinnost ukládal jen v rámci technickoorganizačních opatření k zajištění bezpečnosti osobních údajů (§ 13).

Další ze zásadních změn jsou i nepoměrně vyšší sankce za porušení ochrany osobních údajů, kdy oproti stávajícím téměř symbolickým sankcím ve výši do 10 mil. korun bude možno uložit sankce až do výše 20 mil. EUR.

K přípravě na splnění požadavků GDPR je určeno období od dubna 2016, kdy GDPR vstoupilo v platnost, do května 2018, kdy GDPR nabude účinnosti.

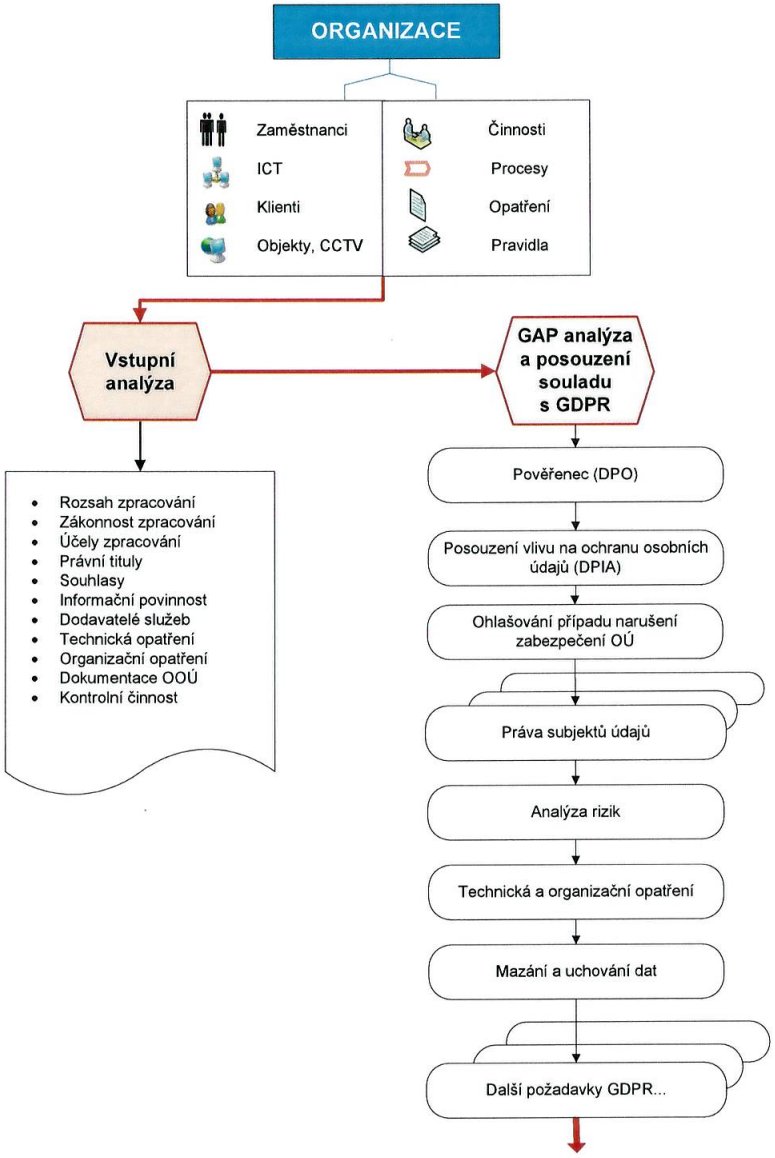
Je zřejmé, že GDPR bude mít značný dopad do stávajících procesů souvisejících se zpracováním a ochranou osobních údajů. Bude tedy nutné nejdříve zrevidovat stávající postupy nakládání s osobními údaji jak v listinné tak i elektronické podobě a vyhodnotit rozsah zpracovávaných osobních údajů. Následně bude nutné porovnat zjištěný stav s požadavky GDPR a navrhnout potřebné změny a definice nových procesů způsobem, který zajistí prokazatelnost platnosti a dodržování stanovených pravidel po celou dobu zpracování osobních údajů.

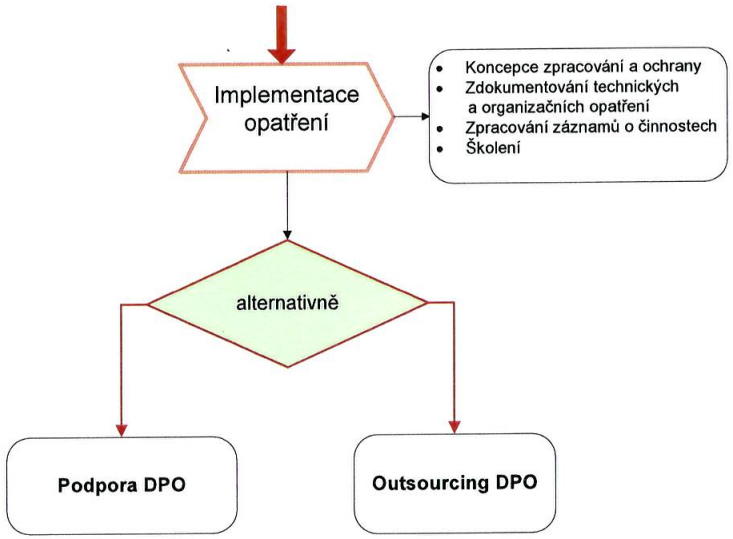
Po provedení revize stávajícího stavu a návrhu definice změnových řízení bude nutné provést implementaci navržených a akceptovaných opatření do podmínek společnosti, což může představovat řadu nových či změněných technických, organizačních a procesních opatření.

Společnost I3 Consultants s.r.o. nabízí pomoc v následujících fázích přípravy a přechodu k GDPR, schematicky znázorněných v následujícím obrázku:

1) provedení revize (vstupní analýzy) stávajícího stavu zpracování a ochrany osobních údajů.

2) Provedení GAP analýzy a posouzení souladu s GDPR a návrh procesních, technických a organizačních opatření nutných pro zajištění souladu s GDPR.
3) Pomoc při implementaci technických a organizačních opatření.
4) Alternativně, na základě zjištěného stavu a reálných podmínek a potřeb objednatele, buď pravidelnou konzultační podporu výkonu role pověřence pro ochranu osobních údajů (DPO) nebo v určitých případech jeho outsourcing.





3 Návrh řešení

3.1 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):

1) zjišťovány jednotlivé **kategorie osobních údajů**
2) zjišťovány jednotlivé **účely zpracování** osobních údajů
   - pro každý účel zpracování budou identifikovány základní typy zpracovávaných údajů,
   - pro každý identifikovaný účel zpracování budou stanoveny způsoby a prostředky, kterými jsou údaje zpracovávány a kterými jsou minimálně následující:
     - listinná podoba vedená v evidencích, kartotékách atd.,
     - agendové IS, jejich moduly, aplikace,
     - ekonomické, provozní, administrativní, docházkové, monitorovací a kamerové a další IS.
3) **souhlasy subjektů údajů**

Posouzení prokazatelnosti a kvality souhlasů se zpracováním v případech, kdy zpracování osobních údajů podléhá souhlasu subjektu údajů a současně posouzení plnění informační povinnosti.

4) určení **příjemci osobních údajů**

5) Zpracována **metodika analýzy rizik**, která prokáže odpovídající úroveň požadavků na:
   - Důvěrnost,
   - Integritu,
   - Dostupnost a odolnost,

   zpracovávaných osobních údajů.

6) **provedení analýzy rizik ve vztahu ke spravovaným osobním údajům** 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 pracování,
     - náklady,
     - dostupné technologie,
     - rizika zpracování,
   - návrh a odůvodnění akceptovatelných rizik,
   - zpracování plánu zvládání rizik,
   - kalkulaci rámcových nákladů na eliminaci zjištěných rizik.

7) **analýza stávajících organizačních a technických opatření k zajištění ochrany osobních údajů**

   - Posouzení rozsahu, efektivity a úrovně přijatých technických a organizačních opatření při zpracování osobních údajů s cílem vyhodnotit úroveň zajištění jejich důvěrnosti, integrity a dostupnosti,
   - na základě závěrů z provedené analýzy rizik návrh na doplnění potřebných technických a organizačních opatření, která budou prokazovat soulad s požadavky GDPR a závěry z analýzy rizik.

8) **analýza smluvních vztahů s dodavateli služeb, kteří mají přístup k osobním údajům správce**
   a) Posouzení smluvních vztahů s dodavateli služeb, kteří jsou zpracovateli ve smyslu GDPR. V rámci tohoto kroku bude provedena:
      - identifikace zpracovatelů,
      - posouzení smluvních garancí zpracovatele k zajištění stanovené úrovně ochrany zpracování osobních údajů na základě smlouvy se správcem,
      - identifikace případného řetězení zpracovatelů.

   b) Posouzení smluvních vztahů s dodavateli služeb, kteří nejsou zpracovateli ve smyslu zákona GDPR. V rámci tohoto kroku bude provedena:
      - identifikace dodavatelů,
      - posouzení smluvních garancí dodavatele k zajištění ochrany osobních údajů.

9) **analýza rozsahu a potřebnosti spravovaných osobních údajů ve vazbě na vykonávané agendy**
   - v součinnosti se zadavatelem bude posouzen rozsah a nezbytnost zpracovávaných osobních údajů pro jednotlivé účely,
   - u jednotlivých účelů zpracování bude vyhodnocen řádový objem subjektů údajů, jejichž údaje jsou v rámci účelu zpracovávány.

10) **analýza legislativních oprávnění pro nakládání s osobními údaji při výkonu svěřených agend**
   - stanoveny právní tituly zpracování osobních údajů pro jednotlivé účely (tj. jejich zákonnost),
   - pro každý účel zpracování bude vyhodnoceno, kdo jej zpracovává, s cílem rozlišit zpracování vlastními zaměstnanci zadavatele, zpracovatelem,
   - identifikovány osobní údaje předávané jiným správcům nebo do jiných států (pokud jsou předávány) a právní titul k jejich předání,
   - bude posouzeno dodržování pravidel pro zpracování osobních údajů zpracovávaných v IS, kterých není město správcem (ISEO, ISZR, katastr nemovitostí atd.),
   - posouzení odpovědnosti za zapracování a ochranu osobních údajů v rámci úřadu.

11) **analýza stávající dokumentace (její úplnost) nezbytné k ochraně osobních údajů (jak pro elektronické, tak i listinné zpracování)**
   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 standardní ochrany zpracovávaných osobních údajů.

12) 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) Podklady pro záznamy o činnostech zpracování osobních údajů (ke každé skupině zpracovávaných osobních údajů).

Použité metody práce:
V rámci realizace etapy bude provedena:
- ✓ analýza dokumentace (u smluv, souladů se zpracováním a další dokumentů s velkým počtem instancí bude použita metoda vzorkování),
- ✓ analýza všech tiskopisů, formulářů, dotazníků atd., v rámci kterých jsou shromažďovány osobní údaje pro potřeby dalšího zpracování,

- ✓ sada interview s odpovědnými zaměstnanci.

3.2 Etapa 2 - Návrh technických a organizačních opatření k dosažení a doložení souladu s GDPR

1) návrh opatření, seznam opatření, harmonogram, priority, náklady, přínosy, rizika, provázanost

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 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, kterým je „Oprávněný zájem správce",
   - bude navržena metodika a postup pro případ Odvolání souhlasu subjektem údajů.
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 Zpracovateli a Dodavateli služeb, v rámci kterých jsou zpracovávány osobní údaje.
5) Návrh úprav řešení kontrolní činnosti.

Výčet výše uvedených změnových řízení vychází z dosavadních 10 letých zkušeností objednatele v auditní a poradenské činnosti v oblasti ochrany osobních údajů a rozhodně není definitivní. Součástí návrhu bude navržení priorit z hlediska možných rizik dopadajících na správce v případě neplnění některých z povinností. Současně bude navržen harmonogram realizace opatření.

2) návrh vhodných technických opatření pro zabezpečení dat v ICT

- budou navržena vhodná technická opatření, vyplývající z analýzy rizik a z analýzy rizikovosti zpracování, jejichž součástí bude doporučení priorit a rámcové finanční nacenění,
- bude zpracován plán zvládání rizik, ve kterém budou uvedena opatření, která není možná realizovat bezprostředně po jejich návrhu z důvodu finančních (nebudou v rozpočtu) a legislativních (zákon o zadávání veřejných zakázek atd.),
- v plánu zvládání rizik budou určeni vlastníci (garanti) těchto opatření.

3) zpracování dokumentace pro ochranu osobních údajů v souladu s GDPR (pravidla nakládání s osobními údaji, interní směrnice, záznamy o činnostech, posouzení vlivu na ochranu osobních údajů, závěrečná zpráva)

a) Vytvoření koncepce/politiky zpracování a ochrany osobních údajů, která umožní prokázat naplnění základních principů GDPR, kterými jsou:
   - zákonnost zpracování osobních údajů,
   - záměrná a standardní ochrana osobních údajů,
   - minimalizace zpracovávaných osobních údajů,
   - korektnost a transparentnost při zpracování osobních údajů,
   - odpovídající důvěrnost, integritu a dostupnost osobních údajů,
   - odpovědnost správce osobních údajů.

b) Rozpracování koncepce/politiky ochrany osobních údajů do vnitřních předpisů a metodických pokynů organizace (správce).

4) pravidla fyzické bezpečnosti osobních údajů budou zapracována do dokumentace zahrnuté v bodě 3 b) a budou zahrnovat minimálně následující:

- případné bezpečnostní zónování v rámci úřadu,
- klíčový režim/duplikáty klíčů,
- návštěvní režim,
- fyzické zabezpečení datových center, serveroven, místností s aktivními prvky sítě, spisoven, archívů a kanceláří, ve kterých jsou zpracovávány osobní údaje,
- kamerové systémy, EZS, docházkový nebo přístupový systém atd.

3.3 Etapa 3 – Diferencované školení k navrženému systému zpracování a ochrany osobních údajů dle GDPR (4 hodiny)

Školení vedoucích zaměstnanců (1 hodina)	
Doporučená účast:	Vedoucí zaměstnanci, v jejichž agendách se zpracovávají osobní údaje
Osnova školení: • Změny v systému ochrany osobních údajů u úřadu • Nové povinnosti vedoucích zaměstnanců	

- Odpovědnost vedoucích zaměstnanců
- Kontrolní činnost vedoucích zaměstnanců
- Prokazování souladu s GDPR

Školení k zabezpečení osobních údajů (2 hodiny)	
Doporučená účast:	Osoby, které jsou odpovědné za realizaci ochrany zpracovávaných osobních údajů ve smyslu GDPR (zejména IT, právní, fyzická bezpečnost, spisovna, interní audit…)

Osnova školení:

- Mechanismus GDPR
- Analýza rizik, řízení rizik
- Návrh opatření k zajištění důvěrnosti, integrity a dostupnosti údajů
- Vhodné nástroje pro zajištění důvěrnosti a integrity v podmínkách úřadu
- Odpovědnost za soulad s GDPR po jednotlivých oblastech

Školení zaměstnanců (1 hodina)	
Doporučená účast:	Všichni zaměstnanci, kteří v rámci své činnosti zpracovávají osobní údaje

Osnova školení:

- Co se změnilo v rámci zpracování osobních údajů
- Co se nedoporučuje a co je zakázáno při zpracování osobních údajů
- Typické nedostatky při zpracování osobních údajů ve veřejné správě

3.4 Zajištění role pověřence pro ochranu osobních údajů

Na základě závěrů ze všech předcházejících etap bude zřejmé, zda je vhodné roli pověřence zajistit externě, nebo vlastním zaměstnancem, kterému smluvní partner zajistí potřebnou podporu. Naše společnost se přiklání na základě dosavadních zkušeností z ochrany osobních údajů z měst Vašeho typu k názoru, že je vhodnějším řešením mít pověřence vlastního, který je schopen zejména evidovat veškeré změny v procesech a v rozhodnutích rady města a zastupitelstva a kterému jsme schopni vytvořit potřebnou odbornou podporu a pomoc na základě definovaného smluvního vztahu.
Přesto předkládáme alternativní nabídku na jeho případný outsourcing, zahrnující jak rozsah zajišťovaných činností tak i cenu za jejich výkon.

3.4.1 Rozsah zajišťovaných činností pověřence pro ochranu osobních údajů

1. Pro zabezpečení komunikace zajistit:
    a. kontaktní místo pro subjekty údajů (v rámci i mimo město),

    b. komunikaci s dozorovým úřadem, zpracovateli, jinými správci a třetími stranami, včetně dozorových úřadů cizích zemí.
2. V rámci trvalého monitoringu souladu s GDPR a dalšími souvisejícími právními předpisy upravujícími ochranu osobních údajů:
    a. ověřovat relevantnost vyhodnocení rizik pro práva a svobody subjektů údajů pro prováděné zpracovatelské operace,
    b. podílet se na testování účinnosti přijatých technických a organizačních opatření a připravovat návrhy nezbytných změnových řízení,
    c. v součinnosti s vedením města:
        i. hodnotit efektivitu a účinnost přijatých organizačních a technických opatření a připravovat nezbytná změnová řízení,
        ii. řídit výkon práv subjektů údajů a zajišťovat jejich informovanost o průběhu a řešení jejich požadavku na uplatnění práva do stanovené lhůty.
        iii. Zajistit ohlašování případů porušení zabezpečení osobních údajů dozorovému úřadu,
        iv. oznamování případů porušení zabezpečení osobních údajů subjektu údajů.
    d. vést dokumentaci o všech případech porušení zabezpečení osobních údajů,
    e. informovat, radit a vydávat doporučení v oblasti zpracování a ochrany osobních údajů vedení a ostatním vedoucím zaměstnancům města,
    f. řídit kontrolní činnost zaměřenou na zpracování a ochranu osobních údajů.
3. Při dohledu nad zpracovatelskými operacemi:
    a. vést a dle potřeby aktualizovat záznamy o činnostech zpracování,
    b. při vzniku potřeby nové zpracovatelské operace, nebo změny již existující, připravit návrh procesů a podklady pro rozhodnutí vedení města související s:
        i. dodržením zásad zpracování osobních údajů a zvláštních kategorií osobních údajů uvedených v čl. 5 – čl. 11 GDPR, zejména analyzovat a prověřovat právní soulad zpracovatelských činností,
        ii. přípravou smlouvy o zpracování osobních údajů v případě, že zpracovatelskou operaci nebo její část bude pro město provádět zpracovatel.
        iii. vyhodnocovat rizika pro práva a svobody subjektů údajů:
            1. v případě, že riziko bude vyhodnoceno jako vysoké, posoudit právní základ nového zpracování a vyjádřit se k nutnosti zda provést či neprovést posouzení vlivu na ochranu osobních údajů,

2. v případě kladného vyjádření ve spolupráci s odpovědnými zaměstnanci města provést posouzení vlivu zamýšlené operace zpracování na ochranu osobních údajů a případně zahájit konzultační činnost s dozorovým úřadem,
3. o rozhodnutí dozorového úřadu neprodleně informovat vedení města.

iv. kontrolovat požadavky na zabezpečení osobních údajů.

c. při zániku zpracovatelské operace, nebo jakékoli její části, připravit návrh procesů a podklady pro rozhodnutí správce, související s:

i. dobou uchování osobních údajů za účelem archivace, pokud není určena platným Spisovým a skartačním plánem,

ii. rozsahem a typy osobních údajů, které budou pro případnou archivaci uchovány.

4. Rozvíjet znalosti a provádět vzdělávání zaměstnanců zpracovávajících osobní údaje z problematiky ochrany osobních údajů.

5. Poskytovat poradenství a informace vedení a ostatním vedoucím zaměstnanců města, a to zejména:

c. formou helpdesku na vyžádání,

d. formou trvalého monitoringu informací z dostupných zdrojů (stanoviska dozorového úřadu a evropských orgánů, judikáty, rozhodovací praxe atd.), jejich následného vyhodnocení a předání návrhů pro případné zlepšení či aktualizaci,

e. formou ad hoc konzultací s dozorovým úřadem.

4 Nabídková cena

	Cena v Kč bez DPH
Etapa 1 - Analýza procesů správy, zpracování a nakládání s osobními údaji	58.000
Etapa 2 – Návrh technických a organizačních opatření k dosažení a doložení souladu s GDPR	49.000
Etapa 3 - Školení k navrženému systému zpracování a ochrany osobních údajů dle GDPR (4 hodiny)	6.000
Celková nabídková cena za etapy 1-3	113.000

	Cena v Kč bez DPH
Zajištění role pověřence pro ochranu osobních údajů	15.000/měsíc

Nabídková cena je uvedena jako absolutní a nepřekročitelná částka za provedení celkové zakázky a obsahuje veškeré náklady se zakázkou spojené.

5 Harmonogram plnění

Práce budou zahájeny do 14 dnů od podpisu smlouvy o dílo a uveřejnění smlouvy o dílo v centrálním registru smluv nebo uveřejnění/vystavení objednávky.

Etapa	Činnost	Období
1.	Analýza procesů správy, zpracování a nakládání s osobními údaji	do 120 dnů po podpisu smlouvy
2.	Návrh technických a organizačních opatření k dosažení a doložení souladu s GDPR	do 150 dnů po podpisu smlouvy
3.	Školení k navrženému systému zpracování a ochrany osobních údajů dle GDPR	Podle požadavků zadavatele po ukončení Etapy 2
	Zajištění role pověřence	Od 1. května 2018

6 Prohlášení o mlčenlivosti

Společnost I3 Consultants s.r.o. se tímto, a následně prostřednictvím smlouvy o dílo zavazuje, že neprozradí žádné třetí straně informace týkající se objednatele nebo souvisejících organizací, které se její zaměstnanci budou mít možnost dozvědět v souvislosti s prováděním služeb pro objednatele.

Společnost se zavazuje obeznámit všechny své zaměstnance se závazky zde a následně ve smlouvě učiněnými, a že učiní vše, aby jeho zaměstnanci dostáli těmto závazkům.

7 Závěr

Vážíme si skutečnosti, že jsme pro Vás mohli připravit tuto nabídku a věříme, že naše nabídka splňuje Vaše případné požadavky.

V případě nejasností či případných dalších požadavků nás prosím neváhejte kontaktovat.

Těšíme se na případnou spolupráci s Vámi.

Ing. Igor Prosecký
jednatel
I3 Consultants s.r.o.
K Tminám 945/34
163 00 Praha 6 - Řepy
Tel.:+420 233 311 973, Mobil: +420 733 510 780, www.i3c.cz