



**„Analýza souladu ICT městské části Praha 14  
a vybraných organizací zřízených městskou  
částí Praha 14 s GDPR“**

Nabídka pro: Městskou část Prahy 14

Vypracoval:	
Počet listů:	10
Počet příloh:	0
Verze dokumentu:	ORIGINÁL
Datum podání nabídky:	26. 1. 2018

## Obsah

Upozornění.....	2
1 Identifikační údaje dodavatele.....	3
1.1 Základní údaje společnosti.....	3
1.2 Pobočky společnosti.....	3
1.3 Statutární zástupci společnosti.....	4
1.4 Kontaktní osoby.....	4
2 Úvod.....	5
3 Popis plnění Dodavatele.....	6
3.1 Obecně o nařízení GDPR.....	6
3.2 Porozumění požadavkům Zadavatele.....	6
3.3 Popis plnění požadavků zadavatele.....	7
3.4 Harmonogram.....	9
4 Nabídková cena.....	10

## Upozornění

Tato nabídka obsahuje informace, které nejsou určeny ke zveřejnění mimo Vaši organizaci a nesmí být jako celek ani částečně kopírována, upravována ani jinak využívána k účelům, které nesouvisejí s jejím vyhodnocením. Pokud by tato nabídka vedla k uzavření dohody o vzájemné spolupráci, má Vaše organizace právo ji kopírovat či jinak používat při realizaci předmětné smlouvy.

**©YOUR SYSTEM Copyright, 2018 - All Rights Reserved.**

# 1 Identifikační údaje dodavatele

## 1.1 Základní údaje společnosti

YOUR SYSTEM, spol. s r. o.

Sídlo: Türkova 2319/5b, Praha 4 – Chodov, 149 00

IČ: 00174939

DIČ: CZ00174939

Bankovní spojení: UniCredit Bank Czech Republic, a.s.

Číslo účtu: 381610004/2700

Tel.: +420 277 775 500

Fax: +420 277 775 501

Web: [www.ys.cz](http://www.ys.cz)

E-mail: [obchod@ys.cz](mailto:obchod@ys.cz), [marian-daniel.zak@ys.cz](mailto:marian-daniel.zak@ys.cz)

Základní jmění společnosti: 30 000 000,- Kč

Vlastníci společnosti: OC Holding a.s. 100%

Počet zaměstnanců: 115

YOUR SYSTEM, spol. s r.o., zapsána v obchodním rejstříku vedeném Městským soudem v Praze

18. července 1990, oddíl C, vložka č. 72.

## 1.2 Pobočky společnosti

### **Pobočka Plzeň**

Adresa: Pražská 45, Plzeň 301 00

Tel.: +420 377 236 480

Fax: +420 377 235 661

### **Pobočka Olomouc**

Adresa: Sladkovského 27, Olomouc 772 00

Tel.: +420 585 312 713

Fax: +420 585 313 913

#### Pobočka Brno

Adresa: Hybešova 42 (Millenium Center), Brno 602 00

Tel.: +420 543 128 326

Fax: +420 543 128 247

#### Pobočka Ostrava

Adresa: Razinova 1574/3, Ostrava 700 30

Tel.: +420 595 783 770

Fax: +420 595 783 760

## 1.3 Statutární zástupci společnosti

Jednatel společnosti: RNDr. Jan Huspeka

Jednatel společnosti: Ing. Petr Fiala

Jednatel společnosti: RNDr. Martin Nehasil

## 1.4 Kontaktní osoby

Obchodní manažer: **Miroslav Váňa**

Tel.: +420 277 775 500

Mob: +420 605 234 764

Fax: +420 277 775 501

E-mail: [Miroslav.vana@ys.cz](mailto:Miroslav.vana@ys.cz)

## 3 Popis plnění Dodavatele

### 3.1 Obecně o nařízení GDPR

Nařízení GDPR (dále jako Nařízení) vstoupí v účinnost 25. května 2018 a bude přímo aplikovatelné ve všech členských státech EU. Nahradí tak mimo jiné i zákon č. 101/2000 Sb., o ochraně osobních údajů ("ZOOÚ").

Na zcela obecných základech či principech ochrany osobních údajů Nařízení nic zásadního nemění. Zůstává zachován koncept, kdy primárním právním důvodem ke zpracování osobních údajů má být informovaný a svobodný souhlas subjektu údajů, případně některá z již dnes aplikovaných výjimek, kdy se pro zpracování osobních údajů souhlas subjektu údajů nevyžaduje.

Mnoho mechanismů, které Nařízení obsahuje, je tak již známo z dosavadní právní úpravy, zejména úpravy v ZOOÚ. Nařízení ovšem zavádí i nové dílčí povinnosti, zpřesňuje či rozšiřuje povinnosti dosavadní, ale také zpřísňuje postihy za nedodržení Nařízení. Nové povinnosti Nařízení ukládá mimo jiné i pro zpracovatele údajů.

Nařízení samotnému a změnám, které přinese, je proto nutné věnovat dostatečnou pozornost. Nařízení se použije celosvětově, na veškeré subjekty, které zpracovávají a budou zpracovávat údaje občanů EU.

Nařízení se neomezí pouze na lokální správce a zpracovatele (ve smyslu ZOOÚ), ale na každou společnost, která nabídku zboží nebo služeb zaměřuje na spotřebitele z EU.

Mezi základní cíle Nařízení patří zejména sjednocení roztržité úpravy ochrany osobních údajů napříč členskými státy EU, které má zamezit rozdílům bránícím ve volném pohybu údajů v rámci vnitřního trhu. Dále Nařízení cílí na snížení administrativní zátěže, umožnění rozvoje digitální ekonomiky a na zajištění účinné kontroly jeho dodržování.

S ohledem na rozsah tohoto Nařízení je nutné očekávat zvýšené nároky na ochranu osobních údajů a dat, kterým bude nutné se přizpůsobit, také v souvislosti se sankcemi, které Nařízení ukládá za jeho porušení, a které jsou mnohonásobně vyšší než doposud.

### 3.2 Porozumění požadavkům Zadavatele

Nabídka analýzy souladu ICT městské části Praha 14 (dále jen „MČP-14“) s nařízením Evropského Parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)(dále jen „GDPR“)

Analýza dopadů bude zaměřena na ICT systémy, které jsou ve správě poskytovatele outsourcingu, dále na systémy, vybraných příspěvkových organizací MČP-14.

Prověření ICT systémů jejich bezpečnostních nastavení, jejich aktuálního stavu a posouzení souladu s požadavky GDPR.

Vypracování analýzy dopadů vyžaduje shromáždění následujících informací a to u každého informačního systému:

- Název systému
- Zpracovávané osobní údaje
- Zpracovávané citlivé údaje
- Citlivé údaje zpracovávají odděleně od ostatních
- Kde jsou ukládána data (lokálně / síť)
- Formát ukládaných dat (Soubor / databáze)
- Jsou uložena data šifrována?

- Umožňuje aplikace vyhledání dat vztahujících se ke konkrétní osobě a provedení operace (vkládání – editace / čtení / výmaz)
- Je přístup k datům omezen na aplikaci, ve které byla pořízena?
- Je přístup k aplikaci omezen pouze na osoby, které s daty potřebují pracovat?
- Je přístup k datům omezen pouze na osoby, které s daty potřebují pracovat?
- Umožňuje aplikace export dat do přenositelného formátu?
- Je export dat sledován / omezen? Jak?
- Aplikaci spravuje organizace / třetí osoba?
- Pokud třetí osoba, má přístup k datům?
- Jsou vedeny záznamy, kdo, kdy a k jakým datům přistupoval? Jaké?
- Jaká oprávnění zahrnují přístupy k aplikacím / datům (vkládání – editace / čtení / výmaz)
- Jsou přístupy omezeny pouze na vnitřní síť / hw vybavení organizace?
- Je povolen vzdálený přístup k datům / aplikacím (popište).
- Je povolen přístup k datům z jiného hw než organizace?
- Je vzdálený přístup / přístup z cizího hw omezen?
- Kdo takový přístup povoluje?
- Jsou data archivována? V jakém formátu? Šifrování?
- Existují směrnice k archivaci dat?
- Kdo rozhoduje o archivaci dat?
- Jsou data uchovávána interně nebo u třetí osoby?

### 3.3 Popis plnění požadavků zadavatele

V rámci analytických postupů bude prováděna komunikace s dodavateli centrálních aplikačních systémů, která povede k návrhu řešení, tak aby byly splněny podmínky nařízení GDPR. Nedílnou součástí je spolupráce s pověřencem pro ochranu osobních údajů, který je jmenován úřadem MČP-14 (dále jen „DPO“).

Výstupem analýzy bude návrh řešení a opatření organizačně technického charakteru, tak aby byly maximálně využity dostupné prostředky úřadu MČP-14.

Návrh opatření bude obsahovat definice systémové bezpečnostní politiky a systémových bezpečnostních opatření pro následující oblasti:

- Active directory
- databáze a datová úložiště
- mail server
- webové portály a webové služby
- datové sítě
- lokální stanice
- antivirová ochrana
- tiskové služby
- ukládání a zálohování dat
- monitoring a logování dat
- CCTV
- řízení přístupů;
- šifrování
- fyzická bezpečnost ICT
- ....

Očekáváme komunikaci minimálně s následujícími dodavateli aplikačních a agentových systémů:

- Gordic (Ginis);
- Marbes (Proxio);

- ICZ (eSpis);
- CDSW(CDSw);
- VITA SW (Vita);
- Datacentrum (Datacentrum SaC)
- MiSYS (Gepro);
- AIPSafe(AipSafe);
- SafeQ(Konica-Minolta);
- Helpdesk (Kaktus SW);

Vzhledem k tomu, že GDPR nestanoví žádné konkrétní vlastnosti či funkce, které by ICT prostředky měly splňovat, tak návrh řešení bude vycházet ze zkušeností dodavatele a aktuálně dostupné praxe tzv. „best practice“. Jako vhodné GDPR uvádí zajištění následujících funkcionalit a zacházení ohledně ICT prostředků:

- a) schopnost pseudoanonymizace a šifrování osobních údajů
- b) schopnost zajistit neustálou důvěrnost, integritu, dostupnost a odolnost systémů a služeb zpracování
- c) schopnost obnovit dostupnost osobních údajů a přístup k nim včas v případě fyzických či technických incidentů
- d) zajištění procesu pravidelného testování, posuzování a hodnocení účinnosti zavedených technických a organizačních opatření pro zajištění bezpečnosti zpracování

Ze znalosti prostředí již nyní můžeme identifikovat nejčastější neshody

- Neznalost rozsahu zpracování osobních údajů (kde jsou uloženy, jak jsou zpracovávány, na základě jakých právních základů)
- paušální, časově nekonkrétní souhlasy
- Nejednotná pravidla pro uzavírání smluv
- Neexistence záznamů
- Neschopnost správně reagovat na požadavky subjektů údajů
- Neexistující nebo neaktuální dokumentace

Očekáváme součinnost nejen s dodavateli aplikačních systémů, ale i se zaměstnanci úřadu MČP-14. Neposkytnutí spolupráce nebo neúplně, či nedostatečné informace může vést ke zvýšení časové i finanční náročnosti projektu.

## 2 Úvod

V návaznosti na poptávku Úřadu městské části Praha 14 předkládá Dodavatel, společnost YOUR SYSTEM, spol. s r. o., následující nabídku na zakázku „Analýza souladu ICT městské části Praha 14 a vybraných organizací zřízených městskou částí Praha 14 s GDPR“.

Nabídka je určena výhradně do rukou pracovníků Zadavatele a obsahuje informace klasifikované jako **OBCHODNÍ TAJEMSTVÍ**.

Dokument ani jakákoli jeho část nesmí být kopírována, reprodukována či zpřístupněna třetím stranám bez písemného svolení firmy YOUR SYSTEM, spol. s r.o.



## 3.4 Harmonogram

Odhadovaná pracnost a harmonogram prací vychází z optimálních reakčních dob všech zainteresovaných subjektů. Reálnost harmonogramu bude upřesňována na pravidelných projektových schůzkách.

popis činnosti	týden 5	týden 6	týden 7	týden 8	týden 9	týden 10	týden 11	týden 12	týden 13	týden 14	týden 15	týden 16	týden 17	týden 18	týden 19	týden 20	týden 21	týden 22	týden 23	týden 24
Analýza dopadů																				
Návrh řešení																				
Konzultace a odsouhlasení návrhu řešení																				
Implementace pilotních nastavení (*)																				
Testování pilotních nastavení (*)																				
Vyhodnocení pilotních nastavení (*)																				
Implementace finálního nastavení (*)																				
Testování finálních nastavení (*)																				
Ověření funkcionality (*)																				

\*Není součástí této nabídky

## 4 Nabídková cena

Popis činnosti	Časový odhad (MD)	Cena 1 MD (člověkodenní)	Cena celkem (činnost)
Projektové řízení	15	10 000 Kč	150 000 Kč
Analytická činnost (garanti oblastí ICT, AD, LAN, backup...)	15	9 000 Kč	135 000 Kč
Konzultační činnost (solution architekt)	8	12 000 Kč	96 000 Kč
Technická podpora (dokumentace, zprávy)	4	8 000 Kč	32 000 Kč
<b>CELKEM</b>	<b>50</b>		<b>413 000 Kč</b>

Součástí nabídky nejsou implementační práce.  
Ceny jsou uvedeny bez platné DPH.

V Praze, dne 26.01.2018

Miroslav Váňa, Obchodní ředitel

YOUR SYSTEM, spol. s r.o.

