Detailní specifikace předmětu zakázky

Zadavatel požaduje provedení projektových a konzultačních služeb k dosažení shody s požadavky Nařízení Evropského parlamentu a Rady (EU) č. 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů (dále též "GDPR") a navržení způsobu dosažení souladu s těmito požadavky, aby měl zadavatel k datu účinnosti GDPR zavedena pravidla a postupy odpovídající požadavkům tohoto nařízení (dále též jen „služby k dosažení shody" nebo „dílo").

Úřad již má zpracovaný základní sběr informací o zpracování osobních dat, který popisuje současný stav a důvody zpracování osobních údajů. Ten lze poskytnout k dalšímu použití (viz Tabulka č.1 - Vzor sběru informací na odboru ekonomiky).

Zadavatel je zřizovatelem organizačních složek, městské policie a příspěvkových organizací (viz Příloha č.6 – Seznam organizací). Realizace služeb k dosažení shody u těchto organizací je součástí zakázky.

Zakázka bude provedena ve čtyřech etapách, které jsou popsány níže. Výstupy budou zpracovány pro každou organizaci a pro každou etapu zvlášť, s výjimkou školských organizací, u kterých budou provedeny pouze etapy 1 a 2, přičemž etapy 3 a 4 budou zpracovány pouze u dvou školských organizací určených zadavatelem po konzultaci s dodavatelem tak, aby byly získané informace v co nejširší míře aplikovatelné i na ostatní školské organizace. Výstupy ze všech čtyř etap budou v souhrnu tvořit komplexní strategický dokument zahrnující část analytickou (1. srovnávací analýza, 2. posouzení rizik), část návrhovou (3. Plán dosažení souladu s GDPR) a část implementační (4. implementace některých konkrétních GDPR opatření).

1. Srovnávací analýza

V rámci Srovnávací analýzy požaduje zadavatel od uchazeče posoudit úroveň stavu ochrany osobních údajů dle aktuálního rozsahu zpracování těchto údajů v prostředí zadavatele. Skutečnosti zjištěné při srovnávací analýze poskytnou informace o slabinách a nedostatcích v zajištění ochrany osobních údajů zadavatele. Kritéria srovnávací analýzy budou vycházet zejména z požadavků GDPR.

Výstupní dokumenty budou obsahovat souhrnnou přehledovou tabulku hodnocení pro jednotlivé požadavky GDPR se stanovením míry jejich zavedení.

Jako součást srovnávací analýzy musí být provedeny úkony, které povedou ke zjištění stavu souladu s požadavky GDPR:

- identifikace respondentů pro provedení interview;
- analýza dokumentace ochrany osobních údajů;
- provedení rozhovorů a posouzení stavu ochrany osobních údajů na pracovištích zadavatele pomocí různých náhledů:
    - Pohled přes požadavky GDPR bude zpracovaný na základě interview se zaměstnanci ICT a vedoucími zaměstnanci. Výstupem bude přehled plnění jednotlivých požadavků GDPR a hodnocení stávajících opatření pro ochranu osobních údajů (bezpečnostní politika, organizace bezpečnosti, řízení aktiv, bezpečnost lidských zdrojů, fyzická bezpečnost a bezpečnost prostředí, kryptografie, řízení komunikací, řízení provozu, řízení přístupu, akvizice, vývoj a údržba informačních systémů, dodavatelské vztahy, zvládání bezpečnostních incidentů, řízení kontinuity činností organizace a řízení souladu s požadavky);

Evropská unie
Evropský sociální fond
Operační program Zaměstnanost

  - Pohled přes organizační jednotky bude zpracovaný na základě interview se zástupci jednotlivých organizačních jednotek, s cílem identifikovat procesy nakládající s osobními údaji, které nemusí být plně známé centrálnímu ICT a vedení.
  - Pohled přes skupiny informačních aktiv s cílem identifikovat aktiva (skupiny systémů a aplikací) nakládající s osobními údaji, které nemusí být plně pod kontrolou centrálního ICT a vedení;
- analýza zdrojů osobních údajů, právních titulů a účelů k jejich zpracování a způsobu jejich dokumentace;
- analýza kategorizace typů osobních údajů v návaznosti na klasifikaci informací;
- analýza zpracovatelských operací osobních údajů;
- analýza životního cyklu osobních údajů v návaznosti na procesy a datové toky v informačním systému;
- analýza uživatelských přístupů k osobním údajům v informačním systému;
- zpracování záznamu ze srovnávací analýzy popisující míru splnění požadavků GDPR a předání tohoto záznamu zadavateli.
- sestavení jednotného registru zpracování osobních údajů (tj. ucelený seznam zpracování osobních údajů).

Výstupem bude:

Zpráva ze srovnávací analýzy požadavků GDPR - přehledová zpráva o plnění legislativních požadavků GDPR zaměřená na typy osobních údajů spravovaných zadavatelem, procesy a opatření pro jejich ochranu.

Zpráva bude obsahovat přehled plnění jednotlivých požadavků GDPR a hodnocení stávajících opatření pro ochranu osobních údajů (bezpečnostní politika, organizace bezpečnosti, řízení aktiv, bezpečnost lidských zdrojů, fyzická bezpečnost a bezpečnost prostředí, kryptografie, řízení komunikací, řízení provozu, řízení přístupu, akvizice, vývoj a údržba informačních systémů, dodavatelské vztahy, zvládání bezpečnostních incidentů, řízení kontinuity činností organizace a řízení souladu s požadavky);

Dalším výstupem bude registr zpracování osobních údajů.

2. Posouzení rizik

Posouzení rizik bude nezbytné pro návrh vhodných organizačních a technických opatření k zajištění plnění požadavků GDPR. Posouzení rizik bude provedeno pro jednotlivá zpracování identifikovaná v rámci Srovnávací analýzy. Pro posuzování rizikovosti jednotlivých zpracování osobních údajů požaduje zadavatel použít následující postup:

- Identifikace, zda jde o zpracování popsané v čl.35 odst. 3 písm. a), b) nebo c) Nařízení;
- Identifikace, zda je zpracování označené za rizikové dozorovým úřadem;
- Identifikace hrozeb spojených se zpracováním (např. porušení zabezpečení údajů, zpracování údajů v rozporu se základními zásadami GDPR apod.);
- Identifikace potenciální újmy dotčených osob spojené se zpracováním jejich osobních údajů (fyzická, hmotná nebo nehmotná újma způsobená správcem nebo třetí stranou);
- Zhodnocení pravděpodobnosti, že újma vznikne (posouzení slabých míst systémů a procesů zpracování oproti povaze hrozby);

- Zhodnocení závažnosti potenciální újmy, pokud by vznikla (z hlediska citlivosti nebo objemu osobních údajů apod.);
- Vyhodnocení, zda zpracování obsahuje rizikové faktory dle výkladového pokynu WP29 ze dne 4.4.2016 (WP 248);
- Vyhodnocení rizika (vysoké riziko je důvodem k tomu, aby bylo provedeno podrobné Posouzení vlivu na ochranu osobních údajů; naopak nízké riziko může být důvodem pro aplikaci některé výjimky z povinností dle GDPR).

Výstupem bude:

Dokument popisující rizikovost jednotlivých zpracovatelských operací.

3. Plán dosažení souladu s GDPR

V návaznosti na Srovnávací analýzu a Posouzení rizik bude zpracován detailní návrh jednotlivých změn, které je třeba provést před nabytím účinnosti GDPR ke dni 25.5.2018. Cílem Plánu dosažení souladu s GDPR (dále též "Plánu") bude podrobné stanovení dílčích úkolů a postupu jejich realizace pro dosažení souladu s GDPR ke stanovenému datu.

Plán zohlední zjištění ze Srovnávací analýzy a bude zaměřen na sestavení postupu k dosažení následujících cílů:

- redukce rozsahu potřebného zpracování údajů s cílem snížit tak náklady na opatření nezbytné na jeho zabezpečení;
- revize bezpečnostní politiky a další bezpečnostní dokumentace, pokrývající oblast osobních údajů;
- úprava procesů spojených s osobními údaji a jejich ochranou;
- přijetí technických opatření pro zlepšení bezpečnosti osobních údajů;
- revize smluv s externími subjekty, které vstupují do zpracování osobních údajů, případně se kterými jsou osobní údaje vyměňovány na základě zákonné potřeby;
- provedení školení zaměstnanců zadavatele zodpovědných za zajištění bezpečnosti osobních údajů.

Výstupem bude:

Dokument stanovující plán přijetí potřebných opatření k odstranění nesouladu s požadavky GDPR, jejich vzájemnou návaznost a doporučení pro jejich realizaci. Uvedená opatření budou navrhovat změny v oblastech právních, procesních a ICT.

Plán bude obsahovat

- popis zadání pro následnou implementaci technických a organizačních opatření;
- odhad náročnosti jednotlivých kroků a doporučení pro postup implementace potřebných opatření do prostředí zadavatele.

4. Implementace některých konkrétních GDPR opatření

V návaznosti na Plán dosažení souladu s GDPR zadavatel požaduje (v nezbytné součinnosti se zadavatelem) úpravu a vytvoření veškerých dodavatelem navržených povinných právních dokumentů a směrnic, zejména:

- vytvořit nový vnitřní předpis ke sjednocení postupů jednotlivých pracovišť zadavatele při sběru a zpracování jednotlivých OÚ
- vytvořit postupy v případě porušení zabezpečení OÚ, vytvořit vzorová oznámení o porušení zabezpečení OÚ, která jsou zasílána dotčených osobám a ÚOOÚ, policejnímu orgánu, vytvořit formuláře pro záznamy o jednotlivých incidentech
- vytvořit postupy pro vypracování záznamů o činnostech zpracování a záznamů o všech kategoriích činností zpracování
- zjistit všechny obecně závazné právní předpisy, které slouží jako podklad pro zpracování OÚ
- vytvořit nový vnitřní předpis upravující práva a povinnosti pověřence
- vytvořit nový vnitřní předpis upravující získávání souhlasu Subjektu údajů, souhlasů dítěte nebo jeho zákonného zástupce a jejich odvolání a archivace, vytvořit vzor souhlasu, získávaného pro všechny možné způsoby zpracování
- vytvořit pravidla pro informování subjektů údajů o jeho právech v souvislosti se zpracováním osobních údajů (práva na přístup, na opravu, na výmaz, na omezení zpracování, na přenositelnost údajů, právo vznést námitku), včetně zavedení postupů pro vyřizování žádostí subjektů údajů o uplatnění jednotlivých práv a námitek proti zpracování, vytvořit vzorová informační oznámení pro jednotlivé druhy subjekty údajů
- vytvořit postupy pro revizi zpracování, které probíhá, byť i částečně, automaticky
- stanovit pravidla pro dobu uchovávání jednotlivých druhů osobních údajů, vč. nastavení postupů pro výmaz údajů v případě uplynutí lhůty nebo odvolání souhlasu se zpracováním

Etapa	Popis	Odhad doby trvání	Předpokládaná realizace
1.	Zpracování srovnávací analýzy	cca 3 týdny	duben 2018
2.	Provedení posouzení rizik	cca 2 týdny	duben 2018 - květen 2018
3.	Plán dosažení souladu s GDPR	cca 2 týdny	květen 2018
4.	Implementace některých GDPR opatření	cca 2 týdny	květen – červen 2018

Evropská unie
Evropský sociální fond
Operační program Zaměstnanost

Tabulka č.1 – Vzor sběru informací na odboru ekonomiky

ČÁST 1	Vymáhání pohledávek	Rozpočet	Účtárna	Správní řízení	Dotační řízení	Pokladna
Proč?	z. 280/2009 Sb. z. 565/1990 Sb. Vyhlášky o místních poplatcích	odpadá	smluvní vztahy (smlouvy, objednávky)	z. 500/2004	z. 250/2000 Sb., smlouva, rozšířený formulář žádosti o dotaci	z. 563/1990 Sb., z. 320/2001 Sb.
O kom?	daňový subjekt, poplatník, osoba, které byla uložena platební povinnost za přestupek, osoba, která se dopustila PRK	odpadá	smluvní strana	osoba, se kterou je vedeno správní řízení	žadatel o dotaci (jeho statutární zástupce, popř. též zmocněná kontaktní osoba)	osoba, která platbu hradí či osoba, jejímž jménem je platba přijímána
Co?	legislativa – výčet níže + registrace k vyrozumívání	odpadá	smlouva	legislativa – výčet níže	legislativa, smlouva, souhlas	legislativa
Kdy?	- poté, co se osoba stane poplatníkem (odpady – trvalé bydliště – přistěhování, narození), nebo poté co splní podmínky pro placení poplatku (stane se držitelem psa, ohlásí zábor, platí pobytové poplatky apod.) - poté, kdy je osobě uložena pravomocná sankce za přestupek - v případě řízení PRK Doba vymáhání až 20 let, skartace S5 (pět let po ukončení)	odpadá A10	po uzavření smluvního vztahu (smlouva, objednávka, fakturace) A10, S10	v případě zahájení správního řízení S5	již v případě přijetí žádosti o dotaci /i pokud není dotace přiznána/ v případě poskytnutí dotace + smlouva a kontrola vyúčtování dotace V10	pokladní doklady S5
Jak?	síťové programy: SW GINIS eSPIS sms.chomutov.cz lokální stanice: excel, word – při hromadném vymáhání Fyzické spisovny V případě sankcí dělená správa (odpady ukládají, OE vymáhá)	odpadá	SW GINIS, ProfiBanka (někdy IČ a název)	SW GINIS	SW eGranty, SW GINIS, SW eSPIS SW form.flow.server	SW GINIS
Kdo	oprávněná úřední osoba, nadřízený, tajemník, primátor, kontrolní orgán (ÚK) Podatelna Hybridní pošta??	odpadá	účetní, nadřízený, primátor, audit (interní i externí)	oprávněná úřední osoba, nadřízený, tajemník, primátor, kontrolní orgán (ÚK) Podatelna	Administrátor dotací, tajemníci komisí, členové komisí, RM, ZM (některé údaje jsou i na webu města) Podatelna	Pokladní, nadřízený, primátor

Evropská unie
Evropský sociální fond
Operační program Zaměstnanost

ČÁST 2	Vymáhání pohledávek	Rozpočet	Účtárna	Správní řízení	Dotační řízení	Pokladna
Obecné osobní údaje						
Jméno	ANO	NE (výjimky)	ANO	ANO	ANO	ANO
Pohlaví	nepřímo lze zjistit, účelově nesledujeme					
Věk	nepřímo lze zjistit, účelově nesledujeme					
Datum narození	ANO	NE	NE (výjimečně)	ANO	ANO	ANO
Rodné číslo	ANO	NE	NE	ANO	ANO	ANO
IP adresa	NE	NE	NE	NE	zřejmě v systému eGranty stopa existuje	NE
Fotografický záznam	NE	NE	NE	NE	NE	NE
Organizační údaje						
e-mailová adresa	ANO (pokud se subjekt zaregistruje)	NE	NE	NE	ANO	NE
Telefonní číslo	ANO (pokud se subjekt zaregistruje)	NE	NE	NE	ANO	NE
Identifikační údaje vydané státem	ANO	NE	ANO	ANO	ANO	ANO
Citlivé údaje						
Rasový, etnický původ	NE	NE	NE	NE	NE	NE
politické názory	NE	NE	NE	NE	NE	NE
náboženství	NE	NE	NE	NE	NE	NE
filozofické vyznání	NE	NE	NE	NE	NE	NE
členství v odborech	NE	NE	NE	NE	NE	NE
zdravotní stav	ANO – držitel průkazu ZTP/P má zadarmo odpady a i psa (nárok na úlevu má, pokud skutečnost doloží) Umístění v léčebně, dětském domově či domově pro seniory, klokánku apod. – úleva od poplatku za odpady	NE	NE	NE	NE (výjimka již jsme se setkali s grantem na nákup automobilu pro vozíčkáře), zahrnu sem i sbírku CHOMUTOV POMÁHÁ	Nepřímo – viz sloupec vymáhání pohledávek (údaje však neeviduje)
ČÁST 3	**Vymáhání pohledávek**	**Rozpočet**	**Účtárna**	**Správní řízení**	**Dotační řízení**	**Pokladna**
sexuální orientace	NE	NE	NE	NE	NE	NE
trestní delikty	ANO (sankce za delikty přímo vymáháme)	NE	NE	ANO (pokud řízení přímo vedeme (zákon o loteriích nebo porušení rozpočtové= kázně)	Nepřímo – ten kdo poruší RK je vyloučen z dotačního řízení	NE

Evropská unie
Evropský sociální fond
Operační program Zaměstnanost

pravomocná odsouzení	ANO – osoba ve výkonu trestu nebo ve vazbě má nárok na prominutí poplatku za odpady	NE	NE	NE	NE	NE
genetické, biometrické údaje a osobní údaje dětí	NE	NE	NE	NE	NE	NE

Evropská unie
Evropský sociální fond
Operační program Zaměstnanost