**Příloha č. 1 - Podrobná specifikace předmětu plnění**

# Základní ustanovení

Předmětem Smlouvy je poskytnutí auditních a navrhovaných služeb, které jsou specifikovány jako soubor služeb poskytnutých Poskytovatelem pro Objednatele vedoucí ke zjištění stávajícího stavu a následnému porovnání s požadavky Nařízení GDPR u Objednatele a návrh opatření vedoucího k souladu s nakládáním s osobními údaji dle nařízení GDPR.

* V souvislosti s výše uvedeným je nutné zmapovat a analyzovat v rámci instituce nakládání s informacemi a osobními údaji u všech organizačních jednotek/útvarů Objednatele s cílem definovat postupy pro naplňování povinností z GDPR vyplývajících. Státní úřad inspekce práce jako Objednatel strukturálně zahrnuje rovněž všechny oblastní inspektoráty práce, které jsou jeho vnitřními organizačními jednotkami. Vzhledem k tomu, že oblastní inspektoráty práce jsou zároveň správními úřady, musí Plnění zahrnout specifické posouzení Objednatelem vybraného min. jednoho oblastního inspektorátu práce.
* Objednatelem vyžadovaný způsobem plnění je výhradně projektové řízení, které povede a bude zajišťovat poskytovatel.
* Součástí Plnění, resp. všech jeho částí, je projektové řízení vedené poskytovatelem, obsahující povinně zajištění zápisů ze společných setkání (zasedání řídících výborů, pracovních skupin apod.) a evidence a vypořádání připomínek, které budou shromážděny v rámci realizace předmětu plnění.
* Veškeré služby dle Smlouvy budou poskytovány a veškeré výstupy dle Smlouvy budou dodány v českém jazyce.
* Plnění (připouští-li to jeho povaha) musí být zpracované písemně, v českém jazyce, ve formátu MS Office vždy v elektronické podobě (na jakémkoli běžném datovém nosiči) a též v listinné podobě, je-li listinná podoba pro daný výstup obvyklá a vhodná. Předávaný výstup je Poskytovatel povinen předat ve dvou kopiích od každé z podob, v níž je vyhotoveno.
* Poskytovatel realizuje relevantní služby a činnosti uvedené v bodě C nejen v sídle Objednatele, ale v rámci výše zmíněného specifického posouzení oblastního inspektorátu práce také v sídle Oblastního inspektorátu práce pro hlavní město Prahu. Pokud Plnění předpokládá a vyžaduje využívání dotazníků, workshopů a rozhovorů s relevantními pracovníky Objednatele, bude toto prováděno také v sídle daného inspektorátu.
* Pokud v průběhu plnění budou identifikovány dopady a opatření, které je možné řešit okamžitě, bude o tom Objednatel informován a relevantní implementační aktivity nastartovány již před dokončením plnění.
* Poskytovatel při realizaci Plnění přiměřeným způsobem přihlédne k obsahu dokumentace, kterou má Objednatel k dispozici v rámci naplnění povinností stanoveným zákonem o kybernetické bezpečnosti.

# Součinnost objednatele

* V rámci součinnosti Objednatele při poskytování služeb Poskytovatelem se Objednatel zavazuje poskytnout zejména následující dokumentaci, ke které je Poskytovatel povinen přihlédnout:

1. bezpečnostní dokumentace,
2. nařízení a směrnice se vztahem k osobním údajům,
3. relevantní dokumentace vzhledem k předmětu plnění,
4. provozní dokumentace a manuály,
5. dokumenty, jimiž Objednatel disponuje po provedení analýzy kybernetické bezpečnosti související s Plněním.

* Objednatel rovněž zajistí:

1. účast vytipovaných uživatelů na interview/pracovní schůzky.
2. účast vytipovaných správců IS na interview/pracovní schůzky.

# Postup plnění – jednotlivé dílčí plnění

## Vstupní analýza - zmapování stávajícího stavu

* Zmapování stávajícího stavu bude zahrnovat a obsahovat zmapování a podrobné zdokumentování výskytu osobních údajů ve všech procesech a systémech objednatele – jaké osobní údaje jsou   
  u objednatele používány, jak jsou osobní údaje získávány, využívány, zpřístupňovány   
  a uchovávány tzn. zejména:

- kde jsou u objednatele sběrné uzly osobních dat (místa sběru);

- jaká je struktura shromažďovaných dat a pomocí jakých nástrojů jsou data shromažďována;

- jaký je formální obsah nástrojů (formát formulářů apod.);

- jak byly a jsou získávány souhlasy ke zpracování osobních dat;

- kdo má přístup k datům a na základě jakého oprávnění;

- jak jsou data uchovávána a chráněna;

- v jakých systémech a aplikacích se s daty pracuje;

- v jakých procesech data figurují a jak probíhá jejich zpracování.

* Zmapování stávajícího stavu má zahrnovat zejména tyto oblasti:

1. identifikace subjektů údajů a jejich osobních údajů včetně citlivých osobních údajů zpracovávaných objednatelem a třídění osobních údajů s ohledem na:
2. účel a rozsah jejich zpracování,
3. dobu jejich uchovávání,
4. předávání třetím osobám a způsob zpracování;
5. posouzení vztahu správce a zpracovatele osobních údajů při jejich zpracování;
6. zmapování a posouzení stávající dokumentace – dokumenty, vnitřní předpisy a normy objednatele apod.;
7. zmapování procesů při zpracování osobních údajů – získávání osobních údajů, plnění informačních povinností vůči subjektům údajů, souhlas subjektů údajů se zpracováním osobních údajů, právo subjektů údajů odvolat souhlas se zpracováním osobních údajů, bezpečnost zpracování osobních údajů, předávání osobních údajů třetím osobám a do zahraničí, a dále postupů zpracování osobních údajů po skončení jejich (aktivního) zpracování (archivace, likvidace);
8. zmapování dokumentace používané při zpracování osobních údajů (informace subjektům údajů o zpracování jejich osobních údajů, souhlas subjektu údajů se zpracováním osobních údajů, pracovněprávní dokumentace, vnitřní předpisy, smlouvy o zpracování osobních údajů, standardní smluvní doložky, závazná pravidla objednatele atd.);
9. analýza zdrojů osobních údajů, právních titulů a účelů k jejich zpracování (kategorizace typů osobních údajů, a způsobů zpracování a typů zpracovatelských operací a způsobu jejich dokumentace), analýza uživatelů a jejich přístupů;
10. posouzení prokazatelnosti a budoucí využitelnosti již získaných souhlasů se zpracováním   
    v případech, kdy zpracování osobních údajů podléhá souhlasu subjektu údajů a současně posouzení plnění informační povinnosti;
11. zmapování informačních systémů využívaných objednatelem při zpracování osobních údajů, včetně zmapování datových toků osobních údajů jako systematického zachycení toku těch kterých osobních údajů v jednotlivých informačních systémech;
12. posouzení rozsahu, efektivity a úrovně přijatých technických a organizačních opatření zejména s ohledem na požadavky § 13 zákona č. 101/2000 Sb. a GDPR

* Zmapování stávajícího stavu musí být zpracováno s aktivním využitím podrobných dotazníků, workshopů a rozhovorů s relevantními pracovníky objednatele.

## GAP analýza – rozdílová analýza

* GAP analýza bude podrobně identifikovat soulad stávajících procesů s požadavky GDPR, tzn. identifikovat rozdíly a nesoulady stávajícího stavu zpracování a ochrany osobních údajů   
  u objednatele oproti všem požadavkům GDPR (event. i zákona č. 101/2000 Sb.).
* GAP analýza má zahrnovat a obsahovat detailní přehled o nesouladu stávajícího stavu s konkrétními požadavky GDPR a identifikaci klíčových nedostatků, rizik a dopadů. GAP analýza musí obsáhnout také:

- kontrolu smluvních závazků týkajících se osobních dat;

- vazby a smlouvy třetích stran;

- přístup k hodnocení dopadů na soukromí;

- proces řízení bezpečnostních incidentů a schopnosti na ně reagovat.

* GAP analýza bude obsahovat přehled všech z pohledu GDPR neexistujících nebo nevyhovujících procesních, organizačních a technických opatření.
* GAP analýza bude obsahovat posouzení procesů z hlediska nutnosti aplikace posouzení vlivu na ochranu osobních údajů (DPIA) včetně doporučení pro zpracování metodiky pro případné posouzení vlivu.
* GAP analýza musí být zpracována s aktivním využitím podrobných dotazníků, workshopů   
  a rozhovorů s relevantními pracovníky objednatele.

## Impact analýza – dopadová analýza

* V rámci impact analýzy bude provedena analýza zjištěných nedostatků a navržena možná řešení včetně určení souvisejících rizik a odhadu nákladů na jejich realizaci. Budou zpracovány podrobné analytické dokumenty, kde u každého zjištěného nesouladu (příp. skupiny nesouladů) mezi činností objednatele a požadavky GDPR budou určena z toho plynoucí rizika (včetně možných sankcí či jiné újmy) bude vyhodnocena závažnost daného nesouladu a navrženo možné řešení včetně vyhodnocení náročnosti nápravného opatření.
* Impact analýza bude zahrnovat a obsahovat také revizi smluvní dokumentace, souhlasů   
  a informační povinnosti.
* V závislosti na výsledcích GAP analýzy se jednotlivé dopady mohou týkat například informační povinnosti, zabezpečení osobních údajů, zajištění práv subjektů, změn ve smlouvách s externími subjekty, změn v oblasti vnitřních norem nebo dalších činností objednatele
* Impact analýza bude dále zahrnovat a obsahovat návrh změn a opatření, která odpovídajícím způsobem modifikují stávající procesní, technická a organizační opatření objednatele v oblasti zpracování osobních údajů, nebo jej doplní. Může se jednat (zvláště v případě GAP analýzou identifikovaných nevyhovujících či chybějících procesů, nebo jejich zdokumentování) zejména o:

1. identifikaci nových účelů zpracování, kterými mohou být zejména údaje umožňující nepřímou identifikaci subjektu údajů;
2. formulaci a vymezení rozsahu souhlasů subjektů údajů se zpracováním, vzhledem   
   k právnímu základu příslušného účelu zpracování:
3. navržení metodiky a postupu pro případ odvolání souhlasu subjektem údajů;
4. posouzení úrovně zpracování analýzy rizik ve vztahu k dopadům GDPR;
5. v případě zpracování citlivých údajů podle stávající terminologie zákona č. 101/2000 Sb. revize všech procesů souvisejících se zpracováním „zvláštní kategorie údajů“ ve smyslu terminologie a požadavků GDPR;
6. posouzení úrovně politiky uchování a mazání dat;
7. revize a návrh úpravy informační povinnosti vůči subjektům údajů s cílem poskytnout explicitně vyžadované informace přehledným a srozumitelným způsobem;
8. revize a návrh úprav procesů při uplatnění práva subjektu údajů na přístup k jeho údajům;
9. návrh úprav smluvních vztahů se zpracovateli a poskytovateli služeb, v rámci kterých jsou zpracovávány osobní údaje spravované objednatelem;
10. detailní přehled dopadů do informačních systémů a technologií objednatele.

## Návrh implementačního plánu

* Na základě dílčích výsledků plnění dle bodu C1 – C3 vyhotoví poskytovatel návrh Implementačního plánu.
* Implementační plán by měl při zohlednění:

1. objednateli dostupného objemu zdrojů finančních a personálních a časových možností potřebných k naplnění požadavků GDPR;
2. časových možností potřebných k naplnění požadavků GDPR;
3. dosud učiněných zjištění, jejich významnosti a pracnosti a analýzy časového vynakládání zdrojů,;

obsahovat zejména:

1. stanovení akčního plánu (včetně identifikace směrů/cílů, stanovení jejich významnosti, jejich prioritizaci) a časové osy (harmonogramu implementace);
2. vyhotovení prioritizační mapy, matice (či jiný obdobný nástroj) zahrnující jednotlivé dopady, ze které vyplyne, které dopady je třeba řešit prioritně, a které později;
3. vytvoření plánu činností pro zajištění souladu s nařízením GDPR s ohledem na prioritizaci jednotlivých dopadů;
4. identifikaci klíčových úloh a milníků;
5. upozornění na účelnost či nezbytnost konzultační a schvalovací činnosti u ÚOOÚ.

* Poskytovatelem připravený návrh Implementačního plánu bude projednán s objednatelem a jeho finální podoba podléhá odsouhlasení objednatelem.

## Prezentace výsledků

* Provedení základního seznámení s nařízením GDPR a s obsahem výstupů C1 – C4 vedení a vybrané osoby objednatele (cca 20 osob) v sídle Objednatele – cca 20 osob.
* Min. rozsah prezentace 5 hodin (1 hodina = 60 min) v sídle Objednatele.
* Poskytovatel zajistí prezenční listinu z prezentace a tisk prezentačních materiálů všem zúčastněným.
* Prostory pro prezentaci a nutná technika v běžném rozsahu (NTB, dataprojektor, projekční plátno, …) bude zajištěna ze strany Objednatele v sídle Objednatele.
* Objednatel nepožaduje žádné občerstvení.
* Minimální obsahová náplň prezentace:

1. co je GDPR, co mění a co přináší,
2. co je to osobní údaj a jeho zpracování v pojetí GDPR,
3. zákonnost zpracování,
4. odpovědnost vedoucích zaměstnanců,
5. kontrolní činnost,
6. GDPR v podmínkách Objednatele - výstupy C1 – C4.