**Příloha č. 2**

**Technická specifikace předmětu plnění**

Předmětem zakázky je:

1. Kontrola záznamů o činnostech zpracování osobních údajů

*Požadavek na realizaci: formou řízených pohovorů s vedoucími odborů a oddělení a obhlídky prostorů a technologií ve vazbě na zpracování osobních údajů. V minimálním rozsahu 2 hodin u jednotlivými odborů a oddělení v prostorách zadavatele.*

* 1. Posouzení rozsahu zpracovávaných osobních údajů
  2. Posouzení relevance právního základu zpracování osobních údajů dle GDPR v jednotlivých agendách
  3. Posouzení oprávněnosti zpracování osobních údajů klasifikovaných jako oprávněný zájem správce
  4. Ověření metodiky postupu při vzniku nového účelu zpracování dat a ověření souladu s požadavky GDPR (realizace zásad „By default“ a „By design“)

1. Kontrola stavu právní ochrany osobních údajů předávaných nebo zpřístupňovaných dalším subjektům dle platné legislativy

*Požadavek na realizaci: dle odstavce č. 1. technické specifikace*

1. Zhodnocení stavu přijatých organizačních a technických opatření k zabezpečení osobních údajů
   1. Kontrola stavu vnitřních předpisů vztahujících se ke zpracování osobních údajů statutárním městem
   2. Kontrola komplexnosti, praktické závaznosti a vymahatelnosti povinností stanovených vnitřními předpisy dle odst. a)
   3. Kontrola souladu vnitřních předpisů s metodikami, výklady a stanovisky dozorového úřadu a resortních ministerstev
2. Kontrola plnění poskytování informací o zpracování osobních údajů v podmínkách výkonu státní správy a samosprávy a v pracovněprávních vztazích

*Požadavek na realizaci: dle odstavce č. 1. technické specifikace*

* 1. Zhodnocení obecných a dílčích informací s ohledem na jejich soulad s GDPR a zákonem č. 110/2019 Sb. – rozsah, úplnost, způsoby poskytování

1. Kontrola dodržování zásad anonymizace osobních údajů
   1. Posouzení shody se zásadami stanovenými GDPR
   2. Způsob anonymizace ve specifických případech – výkon povinností nebo uplatnění práv dle zvláštních právních předpisů, zejména s ohledem na zákony č. 340/2015 Sb., 106/1999 Sb. a č. 128/2000 Sb.
2. Zhodnocení stavu přijatých opatření fyzické bezpečnosti
   1. Posouzení pravidel klíčového režimu (nastavení oprávnění, evidence a uložení klíčů atd.)
   2. Ověření pravidel pro vstup zaměstnanců na pracoviště mimo pracovní dobu
   3. Posouzení pravidel pro pohyb návštěv v objektech
   4. Kontrola stanoveného režimu pro pracovníky úklidu
   5. Kontrola režimových opatření spisovny
   6. Ověření vybavení pracovišť úschovnými uzamykatelnými objekty a pravidel pro jejich užívání
   7. Zhodnocení způsobu a rozsahu zajištění fyzické a elektronické ostrahy objektu a vstupu do něj
3. Kontrola úrovně zajištění ochrany dat při jejich zpracování externím zpracovatelem

*Požadavek na realizaci: dle odstavce č. 1. technické specifikace*

* 1. Kontrola provedení identifikace externích zpracovatelů osobních údajů
  2. Kontrola doložitelnosti smluv o zpracování osobních údajů
  3. Posouzení shody předložených smluv s požadavky GDPR

1. Kontrola systému řízení přístupů do informačních systémů jiných správců
   1. Posouzení systému přidělování přístupových oprávnění
   2. Kontrola dodržování pravidel stanovených jiným správcem
2. Kontrola stanovených postupů a právních základů při předávání osobních údajů do třetích zemí

*Požadavek na realizaci: dle odstavce č. 1. technické specifikace*

1. Posouzení zpracování osobních údajů v personální oblasti

*Požadavek na realizaci: dle odstavce č. 1. technické specifikace*

* 1. Zpracování osobní dat v rámci obsazování volných pracovních míst
  2. Zpracování osobních dat v rámci pracovněprávního vztahu
  3. Nakládání s osobními údaji v rámci ukončení pracovního procesu
  4. Zpracování osobních údajů bývalých zaměstnanců – posouzení koherence rozsahu dat k identifikovaným účelům zpracování
  5. Kontrola a ev. revize pracovněprávní dokumentace

1. Kontrola souhlasů se zpracováním

*Požadavek na realizaci: dle odstavce č. 1. technické specifikace*

* 1. Kontrola relevance/absence souhlasů ve vztahu k jednotlivým agendám zpracování
  2. Posouzení souladu souhlasů s požadavky dle GDPR
  3. Kontrola, ev. revize dokumentů obsahujících souhlas

1. Posouzení zajištění ochrany osobních údajů při projednávání v orgánech města vč. přípravy podkladů pro rozhodování
   1. Posouzení způsobů předávání dokumentů obsahující osobní údaje orgánům města
   2. Kontrola zabezpečení ochrany osobních údajů při projednávání orgány města. (poučení, mlčenlivost – zastupitelé/nezastupitelné, úložiště apod.)
2. Kontrola metodiky postupů při uplatnění a výkonu práv subjektů údajů
   1. Kontrola způsobů přijetí žádostí pro uplatnění a výkonu práv subjektů údajů
   2. Posouzení oprávněnosti požadavků na výkon práv subjektů údajů
3. Kontrola metodiky postupů při porušení zabezpečení osobních údajů
   1. Kontrola detekce narušení osobních údajů
   2. Vyhodnocení porušení zabezpečení osobních údajů a ohlašování narušení bezpečnosti osobních dat dozorovému orgánu
   3. Testování procesu zvládání bezpečnostních incidentů
      * 1. Cílem je dodání služby spočívající v provedení cvičení zaměřeného na únik informací velkého rozsahu po napadení informačních technologií hackerem. Hlavním cílem cvičení bude ověření, zda stanovená prioritizace činností a komunikačních toků je efektivní a zajištuje informačně vitální funkce správy města a následně potřeby svých občanů a to zejména při úniku informací. Cvičení bude zaměřeno na procvičení vybraných procesů v rámci připravenosti zaměstnanců magistrátu a Městské policie Kladno. Cvičení bude provedeno štábní formou. Nedílnou součást přípravy budou představovat řízené pohovory s vedoucími odborů a oddělení, kteří popíší současnou praxi.
   4. Ověření procesu odstranění zjištěných příčin zabezpečení osobních údajů do prostředí úřadu
4. Kontrola zpracování osobních údajů ve vnitřním kamerovém systému objektu Magistrátu města Kladno
   1. Kontrola a zhodnocení stávajících pravidel pro užívání a manipulaci s kamerovým systémem
   2. Posouzení zavedeného řízení přístupu ke kamerovým záznamům včetně podmínek pro export záznamů
   3. Posouzení souladu provozu kamerového systému s platnými legislativními podmínkami a stanovisky dozorového orgánu
5. Kontrola listinné a elektronické evidence a způsobů archivace a uložení dokumentů
6. Posouzení zajištění likvidace nosičů osobních údajů
   1. Četnost reálně prováděných skartačních řízení
   2. Organizační a právní zabezpečení likvidovaných nosičů osobních údajů
7. Audit zpracování osobních údajů u městské police
   1. Posouzení rozsahu zpracovávaných osobních údajů
   2. Posouzení relevance právního základu zpracování osobních údajů dle GDPR v jednotlivých agendách
   3. Kontrola organizačních a technických opatření k zabezpečení osobních údajů
      1. Obecně při zajištění činnosti městské policie
      2. Při výkonu služby strážníků městské policie a dalších zaměstnanců zařazených do městské policie
8. Posouzení rozsahu zpracování a zabezpečení osobních údajů v projektech ochrany majetku obyvatel města využívající Městský kamerový dohledový systém
   1. Ověření povinnosti provedení posouzení vlivu na ochranu osobních údajů
   2. Kontrola a zhodnocení stávajících pravidel pro užívání a manipulaci s MKDS pro kontrolované projekty
   3. Posouzení zavedeného řízení přístupu ke kamerovým záznamům včetně podmínek pro export záznamů
9. Posouzení zajištění výkonu kontrolní činnosti správce osobních údajů
   1. Kontrola doložitelnosti kontrolní činnosti
   2. Prověření a posouzení vydaného plánu kontrol
   3. Ověření procesu implementace zjištěných nedostatků z kontrolní činnosti do prostředí úřadu
10. Posouzení systému vzdělávání pracovníků magistrátu v zabezpečení osobních údajů
    1. Kontrola systému pravidelného zvyšování bezpečnostního povědomí uživatelů k ochraně osobních údajů
    2. Kontrola zajištění informovanosti o aktuálních bezpečnostních hrozbách pro osobní údaje
    3. Namátková kontrola dodržování pravidel ochrany osobních údajů
11. Revize použité metodiky a výsledků analýzy rizik osobních údajů
    1. Posouzení katalogu zpracovávaných osobních údajů dle odst. 1)
    2. Posouzení použitého katalogu hrozeb a zranitelností
    3. Posouzení rozsahu a použití hodnotících škál analýzy rizik
    4. Posouzení celkového průběhu a jednotlivých závěrů analýzy rizik, včetně navržených opatření pro zajištění bezpečnosti osobních údajů
12. Kontrola systému řízení přístupů
    1. Přezkoumání vhodnosti systému řízení přístupů
    2. Posouzení prokazatelnosti přidělování, změny a odebírání přístupových oprávnění
    3. Posouzení rozsahu přidělených přístupových oprávnění k uživatelským stanicím
    4. Posouzení rozsahu přidělených přístupových oprávnění k jednotlivým aplikacím a informačním systémům
    5. Kontrola auditování přístupových oprávnění v aplikacích magistrátu
    6. Kontrola procesu přezkoumání přístupových oprávnění
13. Posouzení způsobů ochrany sítí magistrátů
    1. Ověření zavedení jednotných přístupových bodů do vnitřní sítě
    2. Posouzení způsobů ochrany vnitřní sítě magistrátu proti různým druhům základních útoků
    3. Ověření způsobů sledování nestandardních situací sítě magistrátu
    4. Posouzení způsobů ochrany zařízení magistrátu vynášených mimo prostory magistrátu
14. Posouzení ochrany uživatelských účtů
    1. Posouzení způsobů zabezpečení uživatelských účtů
    2. Posouzení nastavení, vhodnosti a vymáhání politiky hesel
    3. Ověření dodržování pravidel „neobsluhovaných zařízení“
15. Kontrola systému ukládání a ochrany dat
    1. Posouzení systému ukládání dat zaměstnanců magistrátu
    2. Posouzení metod pro sdílení dat a využití cloudových řešení a způsobů zabezpečení dat
    3. Prověření zabezpečení dat na externích discích či jiným přenosných zařízení
    4. Posouzení technických a organizačních opatření k zabezpečení dat při práci mimo perimetr magistrátu
    5. Zhodnocení míry zabezpečení mobilních zařízení
    6. Posouzení způsobů zálohování dat
16. Posouzení způsobů zajištění fyzické bezpečnosti serveroven a dalších klíčových míst pro chod IT
    1. Kontrola stavu fyzické bezpečnosti serveroven či dalších klíčových míst
    2. Zhodnocení systému přístupových oprávnění do serveroven apod.
    3. Posouzení vybavení serveroven apod. prostředky ochrany (kamery, detektory pohybu, hasící systémy, klíčový režim apod.) v porovnání s možnými riziky pro danou lokalitu
17. Kontrola způsobů zvyšování odolnosti prostředků zpracování osobních údajů
    1. Ověření realizace zvyšování odolnosti prostředků zpracování
    2. Kontrola provádění patch-managementu
    3. Ověřování postupů pro sledování a nápravu objevených zranitelností prostředků zpracování osobních údajů

**Výstupy:**

1. Písemná zpráva o provedení auditu obsahující:
   1. zjištění nesouladu zpracování a ochrany osobních údajů s aktuální legislativou,
   2. klasifikaci závažnosti konkrétních nedostatků,
   3. návrhy opatření k odstranění identifikovaných neshod, včetně provedení potřebných změnových řízení v příslušných vnitřních předpisech zadavatele.
2. Školení zaměstnanců města v oblastech ochrany osobních údajů zaměřené na závěry auditu.
   1. Uchazeč bude realizovat vzdělávání pro cca 440 uživatelů magistrátu a Městské policie Kladno. Cílem je zvýšit jejich povědomí v oblasti ochrany osobních údajů a představení nálezů z auditu.

**Způsob realizace:**

1. Audit bude proveden formou:
   1. osobního pohovoru s odpovědnými pracovníky určenými zadavatelem,
   2. formou namátkových kontrol během auditu určených pracovišť.
2. Auditní zpráva bude vyhotovena v sídle dodavatele.
3. Prezentace závěrů z auditu zadavateli.
4. Validace auditní zprávy ze strany zadavatele.
5. Školení zaměstnanců města ve čtyřech kurzech o délce 2 hodin v prostorách zadavatele.

**Další požadavky:**

1. **Zadavatel požaduje výkon činnosti v rozsahu minimálně 250 člověkohodin v prostorách zadavatele za účelem provedení pohovorů, obhlídek a zjištění současného stavu v auditovaných oblastech.**
2. **Vítězný uchazeč obdrží po podpisu smlouvy veškeré relevantní vnitřní předpisy, podklady a záznamy související s oblastí osobních údajů a bezpečnosti informací.**