

## Příloha č. 1 – Specifikace činností

### 1. V rámci vstupního auditu ochrany osobních údajů budou provedeny

- ▶ Studium stávající dokumentace
- ▶ Řízené strukturované rozhovory s určenými zaměstnanci, na jejichž základě bude provedena analýza rizik souvisejících s osobními údaji:
- ▶ Zhodnocení stavu ochrany osobních údajů v oblastech definovaných Přílohou A normy ISO 27001:
  - ▶ Politika bezpečnosti informací
  - ▶ Organizace bezpečnosti informací
  - ▶ Bezpečnost lidských zdrojů
  - ▶ Řízení osobních údajů
  - ▶ Řízení přístupu
  - ▶ Kryptografie
  - ▶ Fyzická bezpečnost a bezpečnost prostředí
  - ▶ Bezpečnost provozu
  - ▶ Bezpečnost komunikací
  - ▶ Akvizice, vývoj a údržba systémů
  - ▶ Dodavatelské vztahy
  - ▶ Řízení incidentů bezpečnosti informací
  - ▶ Aspekty řízení kontinuity činností organizace z hlediska bezpečnosti informací
  - ▶ Soulad s požadavky
- ▶ Příprava závěrečné zprávy shrnující nejzávažnější slabé stránky při shromažďování a zpracovávání osobních údajů včetně možných dopadů
- ▶ Zpracování návrhu pro minimalizaci zjištěných slabých míst prostřednictvím nápravných opatření

### 2. Zajištění souladu s GDPR a následná údržba v rozsahu 5 hodin/měsíc zahrnuje:

- ▶ Realizaci nebo dohled nad realizací nápravných opatření
- ▶ Provedení školení odpovědných zaměstnanců
- ▶ Provedení kontrolního auditu po zavedení opatření
- ▶ Koordinace ochrany osobních údajů, řešení bezpečnostních incidentů, komunikace s Úřadem pro ochranu osobních údajů