ČASTO KLADENÉ DOTAZY K GDPR

Je za soulad informačního systému s GDPR odpovědný zákazník či dodavatel IS?

- Za informační systém (IS) **primárně odpovídá tzv. Správce**. Dle GDPR čl. 4 určuje účel i prostředky pro zpracování osobních údajů (OÚ). Odpovídá tedy i za to, aby IS nebo Zpracovatel vyhovoval požadavkům GDPR. Roli Správce zde vykonává zákazník.
- **Zpracovatel** provádí dle čl. 4 GDPR zpracování OÚ (vyhledávání, zápis, …). Zodpovídá za OÚ **v rozsahu podmínek smlouvy** nebo jiného právního aktu uzavřeného mezi Správcem a Zpracovatelem dle GDPR čl. 28. Dodavatel IS je v roli Zpracovatele, jen pokud přímo zajišťuje provoz IS (např. formou cloudu).
- **Dodavatel IS**, který nemá přístup k OÚ uloženým v IS, respektive nezajišťuje samotný provoz IS, není v postavení Zpracovatele, tudíž **nemá zodpovědnost dle GDPR**.

Je TESCO SW připraveno na GDPR?

- Již nyní plníme požadavky zákona č. 181/2014 o kybernetické bezpečnosti a požadavky normy ČSN ISO/IEC 27001 – řízení bezpečnosti informací.
- Jako firma **budeme v květnu plně v souladu s GDPR**. Provedli jsme rozsáhlou interní analýzu.

Jak jsou aplikace TESCO SW připravené na GDPR?

- Každá aplikace TESCO SW postavená na jednotném aplikačním frameworku TEAF **disponuje základními vlastnostmi pro ochranu OÚ**.

  Jedná se o:

  - **Minimalizace údajů** – možnost přizpůsobení formulářů a tiskových sestav skrytím či odstraněním nepotřebných OÚ

  - **Auditování** – možnost parametrického nastavení auditu
    - Čtení, zápisu, změny, výmazu OÚ.
    - Změn oprávnění přístupu k OÚ.

  - **Řízení přístupů** – uživatelé, aplikační role, kompetence

  - **Šifrování**
    - **Komunikace**
      - Mezi klientem a webovým serverem – protokol TLS.
      - Mezi aplikačním serverem a databází – protokol SSL/TLS.
      - Mezi externími aplikacemi – v závislosti na konkrétním případě.
    - **Dat uložených v DB**
      - Transparent Data Encryption (pro Oracle i MS SQL).

- **Zpracování OÚ** – řízení životního cyklu OÚ prostřednictvím parametrizovatelného workflow.

- **Ruční oprava a výmaz OÚ**

- Pro zajištění souladu s nařízením GDPR je třeba aplikovat výše uvedené vlastnosti na individuální potřeby konkrétního zákazníka v souladu s opatřenými identifikovanými v rámci analýzy GDPR.
- Volitelně lze rozšířit aplikace o:
  - Specializovaný modul na „Správu osobních údajů“
  - Automatická validace a oprava OÚ ze základních registrů
  - Automatická likvidace OÚ po pominutí účelu zpracování
  - Integrace
    - na koncentrátory logů či bezpečnostní dohledový systém
    - na IDM

Jaké další produkty a služby TESCO SW v souvislosti s GDPR nabízí?

- **Specializovaný modul „Správa osobních dat, která umožňuje:**
  - Možnost definic vlastních exportů a importů OÚ.
  - Automatizovaný výmaz dat po ukončení zpracování.
  - Přehledové reporty a statistiky zpracování OÚ dle požadavků.

- **IDM s nadstavbovým modulem GDPR**
  - Centrální správa identit, zákonných titulů, účelů zpracování, souhlasů se zpracováním, žádostí a námitek subjektů OÚ v souvislosti s GDPR.
  - Synchronizace OÚ napříč podnikovou architekturou.

- **Komplexní službu „GDPR na klíč“, která zahrnuje**
  - Zmapování životního cyklu zpracování OÚ ve společnosti.
  - Identifikace nesouladů s požadavky GDPR.
  - Návrh a realizace vhodných organizačních, technických a právních opatření.
  - Zákazník poskytuje jen potřebné informace formou rozhovorů a dokumentů.
- Outsourcing odborných kapacit pověřence pro ochranu osobních údajů.
- Konzultace a semináře.

Mají / budou mít aplikace či firma TESCO SW certifikát/osvědčení GDPR?

- Zatím není ustanovena národní certifikační autorita ani certifikační politiky. **Oficiální certifikát ani osvědčení zatím nelze získat.**
- „Prozatím“ jsme držiteli certifikátů mj. norem ČSN ISO 9001 – management kvality, ČSN ISO/IEC 27001 – bezpečnost informací, aj.
- Máme zkušenosti s provozem 2 kritických a 2 významných informačních systémů dle zákona č. 181/2014 o kybernetické bezpečnosti.
- **Situaci ohledně osvědčení a certifikací rozhodně sledujeme.**

Kam se mohu při řešení souladu s GDPR obrátit?

- Jednoduše **na vaše smluvní konzultanty TESCO SW**, kteří váš požadavek dále přesměrují.

Co musí zajistit Zákazník aplikací TESCO SW na své straně?

- V první řadě musí mít přehled o životním cyklu zpracování OÚ. Tj. co, proč, kdo, jak dlouho, kde a čím zpracovává.
- Dále musí provést **analýzu shody s GDPR** s cílem
    - Potvrdit zákonnost zpracování.
    - Potvrdit účel zpracování.
    - Potvrdit rozsah zpracovávaných OÚ.
    - Potvrdit zajištění důvěrnosti a integrity dat.
    - Zajistit doložitelnost souladu s GDPR.
- Na základě identifikovaných neshod s GDPR a z toho plynoucích rizik **zajistit s konzultanty TESCO SW návrh a implementaci opatření** jako jsou (nikoli výlučně):
    - Úpravy rozsahu zpracovávaných OÚ
    - Změnu definic aplikačních rolí
    - Úpravy v nastavení logování
    - Atd.
- V případě, že správce OÚ nemá vlastní odborné kapacity k posouzení stavu souladu s GDPR, **může využít služby „GDPR na klíč“** (viz „Jaké produkty a služby TESCO SW nabízí“)

Bude vše připravené do 25. 5. 2018?

- Nezbytná technická **funkcionalita je připravena již nyní**.
- **Termín poskytnutí podpory** pro správné nastavení aplikace, další rozvojové požadavky a dodávky rozšiřujících modulů **dle konkrétní objednávky**.

Mohu předat TESCO SW kopii produkční databáze pro účely vývoje či testování?

- Ano, ale před tím je nutné OÚ vymazat či anonymizovat. OÚ se v databázi mohu vyskytovat v jakékoli formě, tedy ve formě textů, čísel, dat nebo souborů.