Vážení uživatelé IS Compekon !

V souvislosti s Obecným nařízením EU o ochraně osobních údajů 2016/689 (General Data Protection Regulation-dále jen GDPR), které vstoupí v platnost 25.5.2018 Vás chci informovat, že IS Compekon ve verzi 1801_97 (tedy pouze NOVÝ IS COMPEKON) bude připraven tak, abyste Vy, naši zákazníci, plně dostáli výše uvedené legislativě.

*Podstatou nařízení je ochrana osobních údajů a zavádí po celé EU jednotná pravidla jejich ochrany. V zásadě se snaží dát maximální práva fyzickým osobám a v maximální možné míře omezit hromadné zpracování osobních údajů a tím i riziko jejich úniku a zneužití. Prakticky veškerou odpovědnost za ochranu osobních údajů přenáší na ty, kdo s nimi nakládají. Definuje základní zásady odpovědnosti a přístupu založeném na riziku. Tj. ten, kdo zpracovává osobní údaje, musí vyhodnotit, jaké osobní údaje zpracovává nebo se chystá zpracovávat, jaké hrozí riziko jejich úniku a zneužití a podle toho přijímat opatření pro jejich ochranu. Nařízení přináší i poměrně vysoké sankce.*

*Více informací na webu GDPR.cz a. UOOU.cz*

Přestože odpovědnost je primárně na uživatelích IS COMPEKON, je pochopitelné, že tito očekávají od IS COMPEKON podporu, která jim umožní nařízení dodržovat. A i když se momentálně jedná o velké téma a "všichni to řeší", tak je fakt, že jak stávající česká i slovenská legislativa ochranu osobních údajů řeší a většinu toho, co nařízení obsahuje, už je v ČR i SK de facto uzákoněno.

V následujících odstavcích se dozvíte, kde lze v IS Compekon uchovávat osobní popř. citlivé údaje fyzických osob, jak lze přístup k těmto datům chránit a jaká opatření připravujeme do uvedené verze 1801.

1) Úložiště

| Tabulka | Popis | Modul | Pole |
|---|---|---|---|
| ECPRAC | Číselník pracovníků | Spol. číselníky | PRIJM, JMENO, ULICE, MESTO, EMAIL, RODCIS, COP, CRP, TELM, TELD |
| ECOD | Obchodní partneři | Spol. číselníky | KNAZ, NAZEV, ULICE, MESTO, TELEFON |
| ECODK | Kontakty partnerů | Spol. číselníky | PRIJM, JMENO, DATUMNAR, TELD, TELM, EMAIL |
| ECODD | Dodatky k partnerům | Spol. číselníky | JMENO, HODNOTA |
| UDZH | Hlavičky protokolů | Dispečink | JMENO, PRIJMENI, RODNECISLO, DNAROZENI, ULICE, CPOPISNE, MESTO, TELEFON, EMAIL, SOURADNICEX, SOURADNICEY, CISLOKARTY |
| UEC | Evidence členů | Dispečink | JMENO, PRIJMENI, RODNECISLO, DNAROZENI, POHLAVI, ULICE, MESTO, TELEFOND, TELEFONM, EMAIL |

Nedá se vyloučit, že někteří uživatelé uchovávají osobní data nestandardně ještě i v dalších částech IS Compekon (např. poznámky). Analýza zpracovávání a uchovávání těchto dat musí být součástí Vašeho řešení GDPR.

2) Přístup k datům

   a) Přístup vnitřní – uživatelský přes IS Compekon
      Ke všem výše uvedeným tabulkám je v rámci IS Compekon možné zakázat či povolit přístup (aktivní i pasivní) dle nastavení účtu každého uživatele IS Compekon. Struktura privilegií je dostatečně bohatá, abyste mohli k dané evidenci povolit přístup jen skutečně v nutných případech. Hesla k daným účtům jsou šifrována na SQL serveru Uživatelé s přístupem musí být proškolení, jak s daty pracovat.

   b) Přístup vnější – přes SQL server, Excel, Olap atp.
      Celá databáze je uložena na SQL serveru, který je chráněn standardními prostředky proti zneužití (přístup administrátora, zabezpečení na úrovni operačního systému, šifrování atp.)

3) Připravované funkce

   c) Smazání osobních dat na přání včetně vytvoření e-mailu o smazání údajů pro žadatele
   d) Doplnění souhlasů s uchováváním osobních údajů do potřebných evidencí
   e) Rozšíření funkcionality Žurnál změn o všechny evidence uchovávající osobní či citlivé údaje
   f) Šifrování dat na úrovni databáze či jednotlivých polí – placená funkce na přání

Poznámka:
Obecně se jako „jednoduché“ řešení uvádí šifrování databáze a dat. Opravdu se tak vyhoví řadě požadavků. Prakticky však realizace může narazit na množství otázek. Uvedu nejdůležitější:

- Šifrování dat v tabulkách sql serveru je možné nastavit od verze SQL2005, nicméně operační systém musí být novější než Windows2008 („historické“ instalace jsou tedy z aplikace šifrování vyloučeny)
- Šifrování zatěžuje procesor, šifrovaná data nelze komprimovat (v zálohách)
- Zálohování šifrovaných databází je třeba zásadně překonfigurovat s ohledem na zálohy nejen databází (jako dosud), ale i doprovodných bezpečnostních dat (klíče, certifikáty), bez nichž nelze provést obnovu. Je třeba prověřit, zda zálohovací sw umí pracovat s šifrovanými technologiemi sql serveru.
- Obnova dat je podstatně složitější, časově náročnější a vyžaduje specialistu (je mnoho variant šifrování podle verze sql serveru, nelze jen „kliknout a počkat“)
- Při napadení databáze kryptovirem bývá možno podstatnou část databáze obnovit. Pokud bude databáze šifrovaná, nebude už toto možné.
- Je proto třeba zvážení rizik a nevýhod u zašifrovaných databází, zda nestačí ochrana standardními prostředky.
- Všeobecně ale můžeme šifrování databází doporučit jen v těch firmách, kde mají vlastního administrátora sql serveru. Jinak nelze garantovat sledování např. expirací certifikátů.