Zabezpečení dat v modulech SOFT-PC Mzdy a Personalistika, verze Access v souvislosti s nařízením GDPR

Tento dokument slouží jako doporučení, jaká provést opatření z hlediska zabezpečení dat v souvislosti s nařízením GDPR v modulech Mzdy a Personalistika (případně dalších souvisejících modulech ISP, rozúčtování mezd), verze Access. Podle předpisu GDPR je třeba zavést přiměřená a vývoji techniky odpovídající opatření, doporučení v tomto dokumentu nejsou tedy závazná, a každý musí zvážit potřebnou míru zabezpečení.

Vzhledem k tomu, že data v těchto modulech jsou ukládána do souboru mdb, který není sám o sobě nijak šifrován či zabezpečen, doporučujeme provést opatření, která zamezí případný únik citlivých dat. V této souvislosti nutno zmínit, že přihlášení do programu/modulu plní pouze funkci přístupu do příslušného modulu, rozhodně nelze zaměňovat se zabezpečením dat, k nimž se z modulu přistupuje.

Zabezpečení přístupu k PC

V prvé řadě je třeba zabezpečit přístup k PC, na kterých se s moduly Mzdy a Personalistika Access pracuje. Zabezpečením přístupu je myšleno jak zabezpečení fyzického přístupu k PC pouze oprávněné osobě/osobám, tak i zabezpečení přihlášení do systému dostatečně silným heslem apod. Při práci s PC je třeba dbát zřetel i na základní zásady jako např. že oprávněné osoby nesmí opouštět počítač bez odhlášení se apod.

Zabezpečení dat

Další doporučení směřují na samotné zabezpečení dat, tedy souboru/ů mdb, ve kterých jsou uložena data. Zde je potřeba zdůraznit, že zabezpečit je třeba:

- aktuální datové soubory - pro každé účetní období(rok) samostatný datový soubor
- vytvářené zálohy uživatelem

- automaticky vytvářené zálohy – zálohy, které se vytvářejí v podadresáři aktuálního datového souboru. Vytvářejí se automaticky před převodem/uzávěrce dat výplatního období do archivu

V případě, že data nejsou uložena lokálně na PC (kde se pracuje s moduly Mzdy a Personalistika), ale jsou umístěna na serveru či ve sdílené složce, je třeba prověřit a případně upravit oprávnění přístupu k této sdílené složce s datovými soubory. V případě že data jsou uložena lokálně, platí i zde opatření zmíněná v předchozím odstavci o zabezpečení přístupu k PC.

Další vhodné zabezpečení dat jsou opatření pro zvýšení ochrany dat na pevném disku. Taková opatření pomohou zabránit získání přístupu k datům na disku např. odebráním disku z vašeho PC a instalací do jiného počítače. Jedná se zejména o použití šifrování, ať už hardwarového či softwarového šifrování pevných disků, případně jiné zabezpečení přístupu k pevnému disku s uloženými daty (např. Heslo pro přístup k disku – HHD on password), či šifrování souborů (BitLocker Drive Encryption apod.)

Přístup do aplikace

Veškeré informace o uživatelích, přiřazení do skupin uživatelů a přístupová hesla jsou uloženy v souboru SoftPC.mdw. Tento soubor je implicitně umístěn v adresáři C:\WINDOWS\SYSTEM\. Přístup k tomuto souboru je tedy důležité zabezpečit, stejně tak jako zabránění spouštění aplikace s jiným mdw souborem(mdw soubor se předává jako parametr příkazové řádky či v zástupci programu) .Pro adekvátní zabezpečení přístupu do aplikace je třeba nastavit dostatečně silná hesla, aby bylo znemožněno přístupu neoprávněným osobám. V této souvislosti je nutno zdůraznit, že je třeba změnit a nastavit mj. silná hesla všem implicitním uživatelům, tj. uživatelům „mzdy“, „personal“ a „spravce“, jejichž implicitní hesla jsou všeobecně známá.

Nastavení hesla se provádí v nabídce „Nastavení->Účty uživatelů a skupin“ na záložce „Změnit heslo“. V tomto formuláři ´“Účty uživatelů a skupin“ lze provádět i další administraci uživatelů(platí pro uživatele „správce“ či vlastní vytvořené uživatele patřící do skupiny administrátoři) tj. vytváření a mazání uživatelů, přiřazení uživatelů do skupin oprávnění či výmaz hesla.

Práva subjektu údajů:

1. Přístup k osobním údajům - výpis údajů

Jak v modulu Mzdy Access, tak v modulu Personalistika Access bude možno pořídit výpis osobních údajů evidovaných o zaměstnanci. Výpis bude řešen formou sestavy, kde bude název položky a aktuální evidovaný osobní údaj.

Sestavy s výpisem evidovaných údajů lze vytisknout z nabídky „Tisky->GDPR->Výpis evidovaných údajů“. V modulu mzdy se po spuštění této nabídky a výběru zaměstnance zobrazí tyto sestavy:

- *Evidované údaje zaměstnance* – výpis údajů evidovaných v hlavním kmeni pracovníků
- *Evidované údaje zaměstnance - další prac.poměry* – výpis údajů evidovaných v dalších prac.poměrech zaměstnance
- *Evidované údaje zaměstnance - srážky*- výpis dalších údajů jako jsou srážky prováděné zaměstnanci, údaje o dětech apod.

V modulu personalistika se po spuštění této nabídky a výběru zaměstnance zobrazí tyto sestavy:

- *Evidované údaje zaměstnance-personální údaje* – výpis personálních údajů evidovaných pro zvoleného zaměstnance
- *Evidované údaje zaměstnance-další personální údaje* – výpis dalších personálních údajů jako např. Kurzy, školení, praxe apod.

2. Výmaz osobních údajů

Výmaz osobních údajů lze provést „vyřazením zaměstnance“ z evidence. Vyřadit lze zaměstnance, kteří mají ukončen pracovní poměr v minulém roce nebo dříve (vztaženo k roku datového souboru). Vyřazení zaměstnance se provádí v nabídce „**Nastavení->Vyřazení pracovníků**“. V zobrazeném formuláři se zobrazí seznam zaměstnanců, po výběru záznamu/zaměstnance se vyřazení provede kliknutím na tlačítko „Vymazat záznam“. Tímto krokem se tedy odstraní veškeré údaje o zaměstnanci v aktuálním datovém souboru.

3. Přenositelnost osobních údajů

Přenositelnost údajů je zajištěna standartní funkcí implementovanou v prostředí MS Access „Analyzovat v prostředí MS Excel“ případně „Publikovat v dokumentu Microsoft Office Word“. Tyto funkce zajistí export dat příslušného formuláře či sestavy v náhledu do formátu xls či textového rtf. Postup exportu je podobný jako při výpisu evidovaných údajů, tzn. v nabídce „Tisky->GDPR->Výpis evidovaných údajů“ se zobrazí jednotlivé sestavy s údaji, místo tisku však zvolíme z nabídky „Soubor-> Analyzovat v prostředí MS Excel“ či „Soubor-> Publikovat v dokumentu Microsoft Office

Word“. Následně se data zobrazí v asociovaném programu pro příslušný typ souboru, tzn. např.v programu MS Excel či MS Word.

Mzdy a Personalistika SQL – lepší možnosti zabezpečení i další

Jelikož možnosti zabezpečení dat u modulů verze Access jsou omezená zejména v použití souborové databáze mdb, posledním doporučením je přechod na verzi SQL, kde je zaručeno mnohem lepší zabezpečení dat vzhledem k ukládání dat na MS SQL server, správa hesel – možnost ověřování uživatelů pomocí Active directory, logování apod. Pokud je to možné, přejděte na verzi SQL co nejdříve, přináší i další podstatné výhody např. v evidenci pracovních poměrů, v evidenci a výpočtu exekucí apod.