Deklarace souladu EIS JASU® CS s nařízením GDPR

V souvislosti s nabytím účinnosti „Nařízení Evropského parlamentu a Rady (EU) č. 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů“ (tzv. GDPR) deklaruje společnost MÚZO Praha s.r.o., že systém EIS JASU® CS ve všech dostupných verzích umožňuje uživatelům jednoduše plnit podmínky uvedeného nařízení ke dni nabytí jeho účinnosti, a to nejméně v následujícím rozsahu:

- umožňuje realizovat podmínku dostupnosti údajů a informací o zpracování pro subjekt údajů (čl. 13 až čl. 15 GDPR),
- umožňuje realizovat právo subjektu na opravu a výmaz údajů (čl. 16 a čl. 17 GDPR),
- umožňuje realizovat právo na omezení zpracování (čl. 18 GDPR),
- umožňuje subjektu údajů poskytnout kopii zpracovávaných osobních údajů (čl. 15 odst. 3 GDPR),
- umožňuje realizovat právo na přenositelnost údajů (čl. 20 GDPR),
- umožňuje zabezpečení osobních údajů (čl. 32 GDPR):
    - identifikací uživatele a autentizací heslem s nastavitelnými požadovanými vlastnostmi,
    - definováním přístupových práv uživatelů podle rolí,
    - podporou logování v čitelné formě a s takovým rozsahem, že je možné jednoznačně prokázat denní činnosti informačního systému s vazbou na uživatele a jeho činnost.

MÚZO Praha s.r.o. se zároveň zavazuje spolupracovat v případě potřeby s pověřencem pro ochranu osobních údajů příslušného uživatele.

Základní informace

Ekonomický informační systém (EIS) JASU® CS je komplexní systém pro zpracování účetnictví a navazujících agend organizačních složek státu, územních samosprávných celků, státních fondů, příspěvkových a hospodářských organizací, veřejných vysokých škol, politických stran, hnutí, spolků a jiných nevýdělečných organizací.

Pokud je v systému EIS JASU® CS vyžadováno zadání osobních údajů, jde o takové údaje, které jsou nezbytné pro úkony související se zákonnými povinnostmi a běžnými obchodními vztahy.

Vymezení odpovědnosti

Systém EIS JASU® CS není primárně určen pro sběr, uchovávání a zpracování osobních údajů. Nicméně systém umožňuje zapsat a uchovávat další údaje (např. nestrukturované textové informace v otevřených textových polích, připojené dokumenty a podobně).

Systém je standardně dodáván jako komplexní řešení provozované v prostředí uživatele, standardně bez přímého nebo nepřímého přístupu dodavatele. Systém umožňuje různé stupně zabezpečení (základní přístup k datovému zdroji, detailní práva uživatelů).

Z výše uvedeného vyplývá:

- **odpovědnost za vkládané informace má provozovatel systému, který je v postavení správce nebo zpracovatele osobních údajů.**
- **odpovědnost za nastavení přístupových práv uživatelů a přístupu k datům má provozovatel systému.**

MÚZO Praha s.r.o. jako dodavatel systému zaručuje, že systém umožňuje realizovat úkony požadované uvedeným nařízením ve výše uvedeném rozsahu. V případě potřeby MÚZO Praha s.r.o. spolupracuje na nastavení systému tak, aby byla zjištěna ochrana veškerých dat systému, nejen s ohledem na GDPR.

V případě, kdy společnost MÚZO Praha s.r.o., resp. její zaměstnanci nebo jí pověřené osoby přistupují k datům provozovatele systému (nahlížení, práce s daty, administrace systému), je takový stav dle povahy věci ošetřen smluvním vztahem (dohodou o mlčenlivosti nebo smlouvou o zpracování osobních údajů), který vymezuje práva a povinnosti obou stran v souvislosti s ochranou osobních údajů.

květen 2018

Realizované změny v EIS JASU® CS s ohledem na GDPR

EIS JASU® CS již v předchozích verzích splňoval vybrané požadavky související s GDPR. Nyní byly do systému dopracovány nové vlastnosti a funkce, které práci s daty v požadovaném rozsahu doplňují. Konkrétně se jedná o:

- rozšíření auditu o logování spuštění každého formuláře,
- vyhledání výskytu osobních údajů konkrétní osoby (případně obchodního partnera) včetně výpisu odpovídajícího protokolu; prohledání se netýká přiložených dokumentů, protože tyto jsou uloženy v různých, často strojově nezpracovatelných formátech,
- všechny doklady je možné uložit v běžně používaném a strojově čitelném formátu (csv, xls, …),
- možnost nastavení, zda se na dokladech mají tisknout údaje „Vystavil“,
- možnost nastavení požadovaných vlastností přístupového hesla.

Revize nastavení systému

Vzhledem k tomu, že řada vlastností a funkcí systému je parametrická (záleží na rozhodnutí provozovatele, jak je chce používat), uvádíme dále přehled těch částí, jejichž nastavení nebo způsob používání je vhodné prověřit.

Ochrana přístupu k datům

- Přihlášení do systému pomocí integrovaného ověřování identity
  Je-li v organizaci využíváno integrované ověřování identity (Active Directory, také označované v systému jako trusted connection), není při spuštění systému vyžadováno zadání přístupových údajů. Pro přihlášení do EIS i pro přístup k datům na serveru je použit výhradně účet uživatele, kterým se přihlásil do počítače (operačního systému).
  Doporučení: V tomto případě je třeba provést revizi uživatelů, kteří mají přístup na SQL server k databázi EIS JASU® CS, event. stanovit pravidla pro zavádění nových uživatelů na úrovni SQL serveru (vyjmenovaný uživatel domény, vyjmenovaná skupina a podobně).
- Přihlašování jménem a heslem
  Pokud není využíváno integrované ověřování identity uživatele, EIS při spuštění vyžaduje zadání uživatelského jména a hesla. EIS umožňuje nastavit požadované vlastnosti hesla (minimální délka hesla, povinnost použít malá písmena, velká písmena, číslice a ostatní znaky). Pro přístup k datům je použit definovaný účet na databázovém serveru.
  Doporučení: Nastavení účtu je v kompetenci správce systému a předmětem revize by mělo být zajištění ochrany přihlašovacích údajů tohoto účtu (informace by měl mít jen omezený počet pracovníků provozovatele, např. administrátor systému). Správce EIS by vždy měl uživatelům nastavit výchozí hesla s omezenou platností a případně nastavit vyšší požadavky na vlastnosti hesla a jeho pravidelnou obměnu.
- Podrobně nastavitelná přístupová práva k funkcím systému (funkční role).
  Doporučení: Revize nastavení rolí a jejich přiřazení konkrétním uživatelům.
- Práva omezující přístup k uloženým dokladům (dokladová role).
  Doporučení: Revize nastavení rolí a jejich přiřazení konkrétním uživatelům.
- Obecná doporučení
  - *Revize zabezpečení přístupu k PC uživatelů (např. automatické uzamykání PC při nečinnosti).*
  - *Zabezpečení fyzického přístupu k počítačům, na kterých je nainstalován databázový server, případně kam jsou ukládány zálohy dat.*
  - *Logování přístupů k databázovému serveru z jiných aplikací než EIS (přístup z EIS je logován v auditu systému).*
  - *Omezení přístupu k databázovému serveru z pracovních stanic z jiného prostředí než z vyjmenovaných aplikací (EIS). Toto lze realizovat např. vhodným nastavením firewallu.*
  - *Zvážit využití možnosti aktivace logování na úrovni politik - Group Policy, služeb Active Directory, operačního systému, případně jeho rozšíření.*

Práce se systémem

Doporučení: Prověřit, jaké osobní údaje jsou v systému zadány, a zvážit, zda jsou skutečně nezbytné pro stanovený účel zpracování.

květen 2018