Bezpečnost a ochrana údajů v systému JMHZ

Zavedení Jednotného měsíčního hlášení zaměstnavatelů (JMHZ) vyvolává otázky týkající se bezpečnosti a ochrany osobních údajů. Tyto otázky jsou pochopitelné – JMHZ pracuje s mnoha informacemi a dotýká se velkého počtu zaměstnavatelů i zaměstnanců.
Cílem tohoto materiálu je **srozumitelně vysvětlit, jak jsou data v JMHZ chráněna, kdo k nim má přístup a jaká pravidla pro jejich využití platí**.

Informační systém JMHZ slouží jako centrální sběrné úložiště pro data zasílaná zaměstnavateli. JMHZ slučuje pravidelné informační povinnosti zaměstnavatelů vůči státním institucím z předchozího roztříštěného systému do současného jednoho elektronického měsíčního hlášení. Systém je spravován Ministerstvem práce a sociálních věcí (MPSV) v jeho vysoce zabezpečeném informačním prostředí. Spadá mezi regulované služby podle zákona č. 264/2025 Sb., o kybernetické bezpečnosti, a vztahují se na něj nejvyšší bezpečnostní požadavky stanovené tímto zákonem a jeho prováděcími vyhláškami.

---

1. Bezpečnost dat jako celek

Data v systému JMHZ jsou chráněna ve všech fázích svého životního cyklu – při přenosu, uložení i jejich zpracování.

Bezpečný přenos

Data jsou zasílána výhradně zabezpečenými kanály (např. prostřednictvím datové schránky, ePortálemČSSZ, napojením z mzdových systémů) a během přenosu jsou šifrována. Nelze je tedy zachytit ani přečíst neoprávněnou osobou.

Bezpečné uložení

Data jsou ukládána v zabezpečeném informačním a komunikačním prostředí MPSV splňujícím přísné požadavky kybernetické bezpečnosti. Opatření zahrnují zejména:

- fyzické zabezpečení,
- oddělení částí systému od jiných systémů,
- ochranu proti neoprávněnému přístupu,
- pravidelné zálohování dat.

Řízený a dohledatelný přístup

K datům mají přístup pouze zákonem oprávněné instituce a konkrétní pracovníci s přiděleným oprávněním, kteří jsou vázaní mlčenlivostí.

Přístupová práva jsou nastavena podle pracovních rolí a každý přístup je evidován a je možné ho auditovat.

Nepřetržitý dohled a kontroly

Systém je pod nepřetržitým bezpečnostním dohledem, který v režimu 24/7 monitoruje provoz. Pro mimořádné situace jsou připraveny postupy zahrnující okamžitou reakci, analýzu, nápravná opatření a případné informování dotčených subjektů.

Pravidelně probíhají:

- kontroly technických zranitelností,
- bezpečnostní testování,
- interní audity,
- kontroly NÚKIB.

JMHZ patří mezi nejpřísněji zabezpečené informační systémy, který spravuje státní instituce, a je provozován v souladu s požadavky zákona o kybernetické bezpečnosti.

Každý subjekt využívající data z JMHZ obdrží pouze ty data, na které má zákonný nárok, a výhradně pro zákonem stanovený účel.

V praxi to znamená, že:

- neexistuje centrální databáze přístupná všem,
- data jsou oddělena podle účelu a oprávnění,
- přístupy jsou řízené, evidované a kontrolované.

Právní a technický rámec

JMHZ funguje v souladu s právními předpisy o kybernetické bezpečnosti, ochraně osobních údajů a pravidly pro informační systémy veřejné správy.

Bezpečnostní standardy odpovídají postavení MPSV jako poskytovatele regulované služby ve vyšším režimu povinností.

---

2. Ochrana osobních údajů (GDPR)

Oprávněnost požadovaných údajů

Údaje, které jsou v rámci JMHZ požadovány, **nejsou nahodilé ani nadbytečné a jsou přísně účelově zpracovávány v souladu s platnou legislativou EU i ČR o ochraně osobních údajů.** Každý údaj má:

- **jasný zákonný důvod**,
- **konkrétní účel využití** (např. sociální zabezpečení, daně, dávky).

Nejde o „sběr dat pro sběr dat“, ale o **nahrazení více než 25 různých hlášení s různou četností vůči pěti státním institucím pouze jedním měsíčním hlášením**.

Ochrana proti neoprávněnému zobrazení údajů

Systém je navržen tak, aby:

- každý uživatel viděl **pouze údaje, ke kterým má oprávnění**,
- nedocházelo k náhodnému zpřístupnění údajů jiných osob,
- každý přístup byl **technicky dohledatelný a auditovatelný**.

Zkušenosti našich pracovníků z minulých digitalizačních projektů byly při návrhu JMHZ zohledněny a promítly se do bezpečnostních opatření.

---

3. Časté obavy z porušení zákona o digitálních službách

Na sociálních sítích se objevují dotazy, proč jsou vyžadovány údaje, které „už stát má“.
Je důležité rozlišovat mezi:

- **existencí informace v informačním systému**
- a **jejím konkrétním uplatněním pro daný účel**.

Typické příklady

- **Vzdělání**
  To, že stát informaci o vzdělání eviduje neznamená, že je automaticky použita pro ostatní agendy. Pro některé účely musí být údaj o vzdělání potvrzen v konkrétním kontextu zaměstnání.
- **Invalidita a její stupeň**
  Evidence invalidity se nerovná jejímu automatickému uplatnění ve vztahu k jiným možným nárokům (např. daňové slevy).
- **Údaje o dětech a partnerech**
  Rodiče se rozhodují, který z nich slevu na dítě uplatní, a toto rozhodnutí je nutno finanční správě sdělit – jinými slovy finanční správa touto dodatečnou informací nedisponuje.

---

4. Pohled zaměstnance: komu se moje údaje mohou dostat?

Jedna z častých obav zaměstnanců je, zda:

- se jejich údaje mohou dostat k jinému zaměstnavateli,

- může jiný zaměstnavatel „vidět“, co bylo nahlášeno jinde.

Jasná odpověď zní: NE

- Zaměstnavatel **nemá přístup k údajům, které zaměstnanec poskytl jinému zaměstnavateli**.
- Neexistuje mechanismus, který by jednomu zaměstnavateli umožnil získat údaje o pracovním vztahu u jiného zaměstnavatele.
- Protokoly o chybách podání ani systémové odpovědi **nesdělují žádné konkrétní údaje z jiných registrací**.

Každý vztah zaměstnanec–zaměstnavatel je v systému evidován a posuzován **odděleně a samostatně**.

Shrnutí

- JMHZ je navrženo tak, aby **zvýšilo efektivitu**.
- Ochrana dat a soukromí je **základním principem systému**, nikoli dodatečným opatřením.
- Zaměstnavatelé ani zaměstnanci **nejsou vystaveni vyššímu riziku, že by jejich údaje byly předány neoprávněnému uživateli,** než je tomu dnes – naopak, díky JMHZ dochází k větší standardizaci a kontrole.