PAY-FAIR

FORMÁLNÍ TBS

Technická a bezpečnostní specifikace

Popis technického řešení a zabezpečení služby Pay-Fair

Dokument v 1.2 | 10. 11. 2026

Obsah

Jaké řešení využíváme 2
Technické požadavky na provoz systému 2
Architektura a zabezpečení 2
Backend – databázové rozhraní 2
Frontend – webová aplikace 3
Volitelný AI modul 4

Aktuální verze dokumentu je vždy dostupná na www.pay-fair.cz/technicka-specifikace

Jaké řešení využíváme

Naše řešení realizujeme v rámci datové platformy, na jejímž vývoji se podílí naše mateřská organizace Vissto s.r.o. (backend) a partnerská organizace Cleevio s.r.o. (webové rozhraní a provoz infrastruktury). Na této stránce naleznete popis této platformy, technickou a bezpečnostní specifikaci celého řešení.

Naše řešení kombinuje webovou aplikaci (frontend) s cloudovým databázovým úložištěm, které dokáže data ihned synchronizovat mezi libovolný počet uživatelů na straně klienta a zabezpečit je pomocí uživatelských přístupů a rolí. Všechna data se nahrávají do zabezpečeného uživatelského účtu klienta, tak aby se nemusely žádné citlivé informace posílat mailem.

Technické požadavky na provoz systému

Pro úspěšný a bezproblémový chod tohoto systému je potřeba zajistit na straně klienta:

- **Aktuální webový prohlížeč** (Google Chrome, Microsoft Edge nebo Safari) a připojení k internetu
- **Nic se neinstaluje**, aplikace běží v prohlížeči
- **Data v šabloně Pay-Fair** ve formátu XLSX, XLS nebo CSV (import firemních dat do uživatelského účtu)

Více podrobností je rozepsáno v odstavcích níže.

Architektura a zabezpečení

Z pohledu softwarové architektury se naše řešení dělí na frontend (webová aplikace v prohlížeči klienta) a backend (kolekce propojených cloudových služeb v rámci jednoho poskytovatele).

Backend – databázové rozhraní

- Infrastruktura je kompletně hostována v **certifikovaném cloudovém prostředí společnosti Microsoft Azure.**
    - Toto prostředí je vybaveno robustní ochranou proti různým typům kybernetických útoků a útočných vzorů chování.
    - Veškeré naše infrastrukturní a aplikační komponenty jsou situovány v rámci EU v nizozemském datacentru (West Europe), abychom zajistili **soulad s GDPR** směrnicí. Z bezpečnostních důvodů společnost Azure nezveřejňuje přesné geografické lokace svých datových center.
- Klientská data jsou ukládána v **zabezpečené a spravované databázi** („managed database“).
    - Toto řešení nabízí automatizované zálohování a funkci **Point-in-Time Restore** (PITR), která umožňuje obnovu dat v časovém horizontu minimálně 14 dní.

- Veškerá manipulace s daty formou čtení, zápisu, aktualizace či mazání (CRUD) probíhá nad databází, do které se data vždy trvale ukládají. Aplikační server uchovává pouze cache a dočasná data v paměti, která se při restartu ztrácejí. Volání externích služeb třetích stran se týká pouze volitelného AI modulu uvedeného níže.

- Komunikace mezi frontendem a backendem probíhá přes **šifrované HTTPS spojení**.
  - Přímý přístup k datům v DB není nikdy pro klienty možný, pouze pomocí frontend aplikace, která data stahuje na bázi přístupových práv skrze API.
- Komunikace mezi API endpointem a DB probíhá pouze přes **privátní virtuální síť (VPC).**
  - V rámci autentizace využíváme validační přístupové tokeny (JWT), které aplikace získá při každém přihlášení.
  - Z důvodu bezpečnosti mají vydané tokeny nastavenou časovou expiraci.
- Hesla uživatelů ukládáme pouze v **šifrované podobě** – uložení v nešifrované podobě není možné.
- O řízení přístupů uživatelů se starají ověřené interní **RBAC mechanismy**.
  - Přístupy řídíme na bázi přístupových práv a skupin na úrovni jednotlivých business objektů/tabulek i konkrétních řádků pomocí RLS.
- Z důvodu bezpečnosti jsou klientská data vždy ukládána do **striktně separovaných schémat** v rámci databázového systému.
- Cloudová databázová infrastruktura poskytuje možnost škálování výpočetních zdrojů při výpočetní či datové zátěži.
- V rámci průzkumu Pay-Fair může klient do systému nahrát i **pseudonymizovaná data**.
  - Nahrávání osobních informací (jméno, příjmení) je čistě volitelné a slouží pouze pro snazší orientaci v připravených reportech.

Frontend – webová aplikace

- Uživatelské rozhraní pro práci s daty je **webová aplikace** dostupná v prohlížeči.
  - Kompatibilita je optimalizována pro aktuální verze **Google Chrome, Microsoft Edge a Safari, na Windows i macOS.**
  - Nic se neinstaluje, nevyžaduje se MS Excel s povolenými makry.
- V aplikaci je připraveno kompletní „klikatelné“ uživatelské rozhraní.
  - Uživatel nepotřebuje žádné dovednosti s prací v Excelu či jiných analytických nástrojích. Nahrání dat, kontrola, zařazení pozic, grading i reporty probíhají v jednom rozhraní, vedené krok za krokem.
  - Rozhraní je dostupné v češtině a angličtině.
- Webová aplikace běží na **aplikačním serveru ve stejném prostředí Microsoft Azure (EU)** jako databáze.
  - Aplikační server **neukládá žádná klientská data na disk**. Data firmy jsou uložena výhradně v databázi, server drží v paměti jen přihlášení a rozpracovaný import.

    - Každé čtení a zápis probíhá **pod účtem přihlášeného uživatele** a s jeho oprávněními. Server nemá žádný společný servisní účet.
- Data jsou kompletně uložená v cloudu a stahují se na bázi **přístupových práv** (systém ověřovacích tokenů).
    - Webová aplikace neumožňuje uživatelům přímý přístup do databáze.
    - Přístupové tokeny k API **nikdy neopouštějí aplikační server** a do prohlížeče se nedostanou.
    - Přihlašovací relace je vedena zabezpečenou cookie, kterou nelze číst skriptem (HttpOnly). Relace končí po 30 minutách nečinnosti, nejpozději 12 hodin po přihlášení. Platnost přístupového tokenu určuje API Pay-Fair, aplikační server jej před vypršením sám obnovuje.
    - Po opakovaném chybném hesle aplikace další pokusy dočasně pozastaví.
- Komunikace s backendem probíhá pomocí API requestů. Aplikační server volá API přímo v rámci téhož serveru, jinak výhradně přes HTTPS.
    - Komunikace mezi prohlížečem a aplikačním serverem probíhá skrze **zabezpečené šifrované spojení na bázi HTTPS protokolu**.
    - Webová aplikace nevolá z prohlížeče žádné externí služby třetích stran, písma a ikony jsou součástí aplikace.
- Excelové soubory (XLSX, XLS) se zpracovávají na serveru v odděleném procesu s limitem času a paměti, soubory CSV v hlavním procesu aplikace s omezením velikosti. Chybný soubor aplikace odmítne s popisem, co opravit.
- Technické chyby aplikace se zaznamenávají do monitorovacího nástroje provozovaného v EU (Německo). Zaznamenává se jen technický popis chyby (typ, stránka, verze aplikace, typ prohlížeče). Obsah formulářů, soubory, cookies ani IP adresa uživatele se nezaznamenávají; osobní a mzdová data aplikace ze záznamu odstraňuje.

Volitelný AI modul

V rámci snahy o maximální automatizaci a úsporu času na straně klienta nabízíme k využití náš volitelný, automatizační AI modul integrovaný přímo ve webové aplikaci. **Tento modul pomáhá zejména se zařazením pozic klienta do připraveného katalogu.**

V rámci tohoto modulu využíváme zabezpečené služby třetích stran, které uvádíme níže. Do těchto služeb **nikdy neposíláme žádná citlivá data**, pracujeme pouze se základními informacemi, které nemají povahu osobních informací.

- Využíváme jazykové modely (ChatGPT z rodiny GPT4 a vyšší) od OpenAI ve firemní API verzi (**nevyužívá se pro trénování a analýzu dat**: https://trust.openai.com/).
    - Do tohoto modelu nikdy neposíláme žádná citlivá data – pracujeme pouze se základními informacemi viz níže a dále již jen s výstupy, které tímto způsobem vytváříme.
    - Volání AI probíhá výhradně z aplikačního serveru, nikdy z prohlížeče.
    - Všechna data, která používáme pro potřeby AI dokážeme jednoznačně identifikovat – abyste měli přehled, jaké informace odchází.
        - Název pozice
        - Název organizačních jednotek

- Odvětví organizace (hodnota z katalogu)
- Funkce pozice zadaná uživatelem (volitelné) a volitelný text popisu pozice (pokud tyto informace klient nahraje)
- Struktura organizace: název nadřízené pozice, názvy pozic na stejné úrovni a podřízených pozic a jejich počty