Technická a organizační opatření

Verze 1.4, účinná od 21. 10. 2026.

1. Oddělení dat obcí

- Všechny obce sdílejí jednu instanci aplikace. Data každé obce jsou v databázi oddělena na úrovni řádků (row-level security).
- Aplikace se k databázi připojuje rolí, která bez nastavené obce nevidí žádná data modulů. Každý dotaz nad daty obce běží v transakci s nastavenou obcí.
- Oddělení obchází jen serverové úlohy provozovatele, které pracují napříč obcemi: správa obcí, rozesílání pošty, automatické mazání a zálohy. Veřejný web ani administrace obce touto cestou nejdou.
- Tabulky provozovatele (seznam obcí, ceník, poptávky, provozní záznamy o poště, fakturace) aplikační role nečte vůbec.
- Soubory každé obce jsou v úložišti pod vlastní předponou a vydávají se jen v rámci téže obce.

2. Šifrování

- Veškerý provoz mezi prohlížečem a službou je šifrován protokolem TLS.
- Spojení mezi sítí Cloudflare a hostingem je šifrované v režimu „Full“. Certifikát hostingu se v tomto režimu neověřuje.
- Tajemství obcí (například přístupový token k bankovnímu výpisu) jsou v databázi uložena šifrovaně algoritmem AES-256-GCM. Klíč je uložen mimo databázi.

3. Přihlášení a oprávnění

- Do administrace se přihlašuje bez hesla, jednorázovým odkazem zaslaným na e-mail uživatele.
- Uživatel si může zapnout dvoufázové ověření (kód z aplikace v telefonu podle RFC 6238, k tomu jednorázové záložní kódy) a obec ho může vyžadovat po všech svých uživatelích. Pro správce platformy na straně poskytovatele je povinné.
- Přihlášení vyprší po 30 dnech nečinnosti; každé použití administrace ho prodlouží. Drží ho cookie, ke které nemá přístup skript stránky (HttpOnly).
- Oprávnění se přidělují rolemi po jednotlivých modulech. Obec sama určuje, kdo co smí.
- Změny v administraci se zapisují do auditního záznamu (kdo, kdy, co).
- Poskytovatel se do administrace obce přihlašuje jen na žádost obce nebo k odstranění poruchy. Takové přihlášení platí nejvýše 2 hodiny a zapisuje se do auditního záznamu.

4. Ochrana formulářů a vstupů

- Počet odeslání formulářů je omezen. IP adresa se pro tento účel ukládá jen jako otisk a otisky se mažou po 2 dnech.
- Fotografie od občanů se na serveru ověří podle skutečného obsahu souboru, odstraní se z nich všechna metadata EXIF (zachová se jen poloha, pokud ji hlášení potřebuje) a zmenší se.
- Text z editoru (HTML) i obrázky SVG nahrané obcí procházejí sanitizací, která odstraní skripty a nepovolené prvky.

5. Automatické mazání

Osobní údaje, u kterých to služba umožňuje, se po uplynutí lhůty mažou nebo anonymizují automaticky. Lhůty po modulech uvádí Popis služby (příloha 1).

- Záznam o odeslaných e-mailech: obsah zprávy se maže po 90 dnech, záznam o doručení po 12 měsících. Se smazáním obce se mažou i všechny její e-maily.
- Auditní záznam se nemaže; je dokladem o zveřejnění na úřední desce (kdy byla položka vyvěšena a sejmuta). Maže se až se smazáním obce.

6. Zálohy

- Databáze se zálohuje denně u poskytovatele hostingu; denní zálohy se uchovávají 6 dnů, týdenní 27 dnů.
- Každou noc se šifrovaná kopie databáze (AES-256) a kopie nahraných souborů ukládají do nezávislého úložiště v EU (Cloudflare R2, jurisdikce EU) a uchovávají se 30 dnů. Heslo k šifrování není uloženo u tohoto úložiště.
- Postup obnovy ze zálohy je popsaný. Obnova ze zálohy se zkouší nejméně jednou za čtvrtletí a výsledek se zaznamenává.

7. Přístup k produkčním datům a incidenty

- K produkčním datům a k účtům u poskytovatelů hostingu, DNS a e-mailu má přístup jen provozovatel služby.
- Bezpečnostní incident lze hlásit na info@civix.cz. Porušení zabezpečení osobních údajů oznámí poskytovatel obci podle smlouvy o zpracování osobních údajů (příloha 3).