Civix

Bezpečnost a ochrana dat

Verze 1.1

Aktualizováno 8. 10. 2026

Jak Civix chrání data obce a jejích občanů. Nejdřív srozumitelně pro starostu a úřad, pak technicky pro správce IT a pověřence pro ochranu osobních údajů.

Srozumitelně

1. Kde jsou data obce

Web, administrace, databáze i nahrané soubory běží u poskytovatele hostingu v **Nizozemsku** (Amsterdam), tedy v EU. Všechny obce sdílejí jednu aplikaci, ale data každé obce jsou od ostatních oddělená a jiná obec je nevidí.

Kdo další se na provozu podílí (hosting, e-maily, mapy), je vyjmenováno níže v technické části a v podmínkách zpracování osobních údajů.

2. Kdo k datům má přístup

- **Lidé z vašeho úřadu**, kterým přístup dáte vy. Každý má roli a vidí jen ty části, ke kterým ho role pustí. Nikdo nemůže jinému dát víc práv, než má sám.
- **Občané** vidí jen to, co obec zveřejní. Soubory, které poslali občané (například přílohy žádostí), se veřejně nezobrazují ani nedostanou do vyhledávačů.
- **My jako provozovatel** do administrace obce vstupujeme jen na vaši žádost nebo při opravě poruchy. Takový vstup platí nejvýše 2 hodiny a zapíše se do záznamu změn.

Do administrace se nepřihlašuje heslem, ale jednorázovým odkazem poslaným na e-mail. Heslo tak nejde uhodnout ani ukrást z jiné služby.

Kdo chce víc, zapne si v „Můj účet" dvoufázové ověření: k odkazu z e-mailu přidá kód z aplikace v telefonu. Obec ho může vyžadovat po všech svých uživatelích; my ho při vstupu do správy platformy máme povinné.

3. Co když se něco pokazí

Databáze se zálohuje každý den. Každou noc navíc odchází šifrovaná kopie databáze i všech souborů do nezávislého úložiště v EU, které by přežilo i výpadek celého hostingu. Kopie se drží 30 dnů a obnova ze zálohy se zkouší nejméně jednou za čtvrtletí.

Změny v administraci se zapisují (kdo, kdy, co). Když se na úřední desce nebo webu něco ztratí, dá se dohledat, co se stalo.

Bezpečnostní problém nám můžete kdykoli nahlásit na info@civix.cz. Pokud by došlo k úniku osobních údajů, oznámíme ho obci podle smlouvy o zpracování osobních údajů.

4. Co se stane s daty po skončení smlouvy

Data zůstanou dostupná ještě **30 dnů**. Na požádání dostanete kompletní export: obsah webu, úřední desku včetně archivu, všechny agendy ve formátu JSON a nahrané soubory v původní podobě.

Potom data smažeme z databáze, úložiště souborů i záznamů o odeslané poště. Ze záloh zmizí nejpozději do 30 dnů a o smazání vám pošleme potvrzení.

5. Kdo za co odpovídá (GDPR)

- **Obec je správce** osobních údajů svých občanů. Rozhoduje, co na webu zveřejní, komu dá přístup a které agendy používá.
- **UTORU, s.r.o. je zpracovatel.** Data zpracováváme jen pro provoz služby a podle smlouvy o zpracování osobních údajů, kterou s obcí uzavíráme.

Stránku „Ochrana soukromí" na webu obce skládáme automaticky podle modulů, které obec používá, včetně lhůt, po kterých se údaje mažou.

6. Co dělá obec a co my

- **Obec:** hlídá, komu dává přístup, a odebere ho lidem, kteří na úřadě skončili; nezveřejňuje na webu víc osobních údajů, než musí; drží v pořádku e-mailové schránky, na které chodí přihlašovací odkazy.
- **My:** provozujeme a aktualizujeme aplikaci, oddělujeme data obcí, zálohujeme, mažeme údaje po uplynutí lhůt a hlásíme obci incidenty.

Technicky

1. Hosting a subzpracovatelé

Aplikace, PostgreSQL a objektové úložiště běží na Railway v regionu europe-west4 (Amsterdam). DNS, TLS a ochranu před útoky zajišťuje Cloudflare. Úplný seznam subzpracovatelů (příloha 3 smlouvy o zpracování osobních údajů):

- **Railway Corporation** (USA) — hosting aplikace, databáze PostgreSQL, úložiště souborů, plánované úlohy, provozní logy. Umístění: Nizozemsko (region europe-west4, Amsterdam) pro aplikaci, databázi a soubory; umístění provozních logů a záloh poskytovatel ověřuje. Předání: standardní smluvní doložky (SCC); DPF ověřit.
- **Cloudflare, Inc.** (USA) — DNS, šifrované spojení (TLS), proxy a ochrana před útoky; úložiště nočních záloh (R2). Umístění: globální síť; návštěvníky z EU obsluhují zpravidla uzly v EU; zálohy v úložišti s jurisdikcí EU. Předání: standardní smluvní doložky (SCC); DPF ověřit.
- **Resend (Plus Five Five, Inc.)** (USA) — odesílání e-mailů. Umístění: odesílání přes Amazon Web Services v Irsku (eu-west-1); kde Resend ukládá záznamy a obsah zpráv, poskytovatel ověřuje. Předání: standardní smluvní doložky (SCC); DPF ověřit.
- **Amazon Web Services** (USA) — infrastruktura pro odesílání e-mailů (subzpracovatel společnosti Resend). Umístění: Irsko. Předání: prostřednictvím smlouvy se společností Resend.
- **Seznam.cz, a.s.** (Česká republika) — mapové podklady a zpětné vyhledání adresy (Mapy.com). Umístění: Česká republika. Předání: bez předání mimo EU; předává se jen souřadnice bodu na mapě, nikdy IP adresa návštěvníka.
- **Better Stack, Inc.** (USA) — dohled nad během služby (pravidelné kontrolní dotazy) a nad doběhnutím plánovaných úloh; zpracovává jen výsledky kontrol a signály úloh, žádná data obcí ani občanů, a technicky nutně IP adresu serveru, který signál posílá. Umístění: datová centra v EU (výchozí region poskytovatele), infrastruktura Amazon Web Services; poskytovatel si ve smlouvě vyhrazuje i zpracování v USA. Předání: standardní smluvní doložky (SCC); DPF ověřit.

Změnu subzpracovatele oznamujeme obci nejméně 30 dnů předem.

2. Šifrování

- Provoz mezi prohlížečem a službou je šifrován TLS. Šifrované je i spojení mezi Cloudflare a hostingem.
- Tajemství obcí (například token k bankovnímu výpisu) jsou v databázi šifrována AES-256-GCM s klíčem uloženým mimo databázi.
- Noční záloha databáze je šifrována AES-256 (PBKDF2) dřív, než opustí kontejner; heslo není uloženo u úložiště záloh.

3. Oddělení obcí

- Každá tabulka modulu nese tenant_id a má zapnutou a vynucenou row-level security (PostgreSQL RLS) s politikou na aktuální obec.
- Aplikace se připojuje rolí bez práva obejít RLS. Dotaz nad daty obce běží v transakci, ve které je nastavená obec; bez ní role nevidí žádné řádky modulů. Aplikační vrstva navíc do dotazů doplňuje podmínku na obec.
- Tabulky provozovatele (seznam obcí, ceník, poptávky, fakturace, záznamy o poště) aplikační role nečte vůbec; pracují s nimi jen serverové úlohy provozovatele.
- Soubory obce leží pod vlastní předponou a vydávají se jen v rámci téže obce.

4. Přihlášení, role a audit

- Přihlášení bez hesla jednorázovým odkazem z e-mailu, platným 1 hodinu. V databázi se ukládá jen otisk tokenu.
- Relace drží cookie HttpOnly; vyprší po 30 dnech nečinnosti.
- Dvoufázové ověření: TOTP podle RFC 6238 (SHA-1, 6 číslic, 30 s, tolerance ±1 krok, ochrana proti opakovanému použití kódu) a 10 jednorázových záložních kódů, v databázi jen jako otisk. Tajemství TOTP je uložené šifrovaně (AES-256-GCM). Na kód je po odkazu 10 minut a nejvýš 5 pokusů; po ověření dostane relace nový token. Povinné pro správce platformy, volitelně vyžadované obcí.
- Role se skládají z oprávnění po modulech. Server odmítne udělit roli nebo oprávnění širší, než má ten, kdo je uděluje.
- Přístup k jednotlivým záznamům (například spolek a jeho zástupce) se ověřuje na serveru u každého požadavku, ne jen schováním tlačítka.
- Změny v administraci se zapisují do auditního záznamu. Ten se nemaže, protože je dokladem o vyvěšení na úřední desce; zaniká se smazáním obce.

5. Formuláře, nahrávání a soubory

- Přihlášení a veřejné formuláře mají limity počtu požadavků. IP adresa se ukládá jen jako otisk HMAC-SHA256 s tajným klíčem (ne holý hash, který by šel zpětně dohledat) a otisky se mažou po 2 dnech.
- Fotografie od občanů: typ souboru se ověřuje podle obsahu, ne podle přípony; z metadat EXIF se zachová jen poloha, vše ostatní (model fotoaparátu, sériové číslo, čas) se zahodí; obrázek se zmenší.
- Soubory od občanů a další soukromé přílohy se vydávají s Cache-Control: private, no-store a X-Robots-Tag: noindex.
- Text z editoru (HTML) a SVG nahrané obcí procházejí sanitizací, která odstraní skripty a nepovolené prvky.
- Nahrávání souborů ověřuje typ a velikost na serveru.

6. Mapy

Mapové dlaždice a hledání adresy jdou přes náš server. Mapy.com tak dostanou jen souřadnice bodu, nikdy IP adresu návštěvníka, a přístupový klíč ke službě se do prohlížeče nedostane.

7. Zálohy a automatické mazání

- Zálohy PostgreSQL u poskytovatele hostingu: denní uchovávané 6 dnů, týdenní 27 dnů.
- Každou noc šifrovaný výpis databáze a kopie souborů do Cloudflare R2 s jurisdikcí EU, uchování 30 dnů. Staré zálohy se mažou podle data v názvu, ne podle stáří souboru, takže nic nevydrží déle, než je slíbeno. Exporty ukončených obcí se do záloh nekopírují.
- Záznamy o odeslané poště: obsah zprávy se maže po 90 dnech, záznam po 12 měsících; se smazáním obce se maže i její pošta.
- Poptávky z webu se mažou 24 měsíců po poslední změně, nepotvrzené přihlášky k odběru 48 hodin po vypršení odkazu.
- Lhůty mazání v jednotlivých modulech uvádí Popis služby a stránka „Ochrana soukromí" na webu obce.

8. Ukázková obec a ukončení

- Ukázková obec (demo) je oddělená stejně jako každá jiná, každou noc se smaže a postaví znovu, neodesílá žádné e-maily a nedá se do ní pozvat další uživatel. Její soubory se do záloh nekopírují.
- Po ukončení smlouvy vznikne export obce (JSON a soubory). Drží se 30 dnů, odkaz pro obec platí nejvýše 7 dní; pak se export automaticky smaže.

9. Související dokumenty

Závazné znění opatření je v příloze smlouvy Technická a organizační opatření; dále Smlouva o zpracování osobních údajů a Obchodní podmínky. Tento přehled je vysvětlení, ne smluvní text.