Zabezpečení a ochrana dat aplikace

1. Infrastruktura a fyzické zabezpečenie

1.1. Aplikace Homfi je provozována na cloudové infrastruktuře:

1.1.1. Aplikační servery a databáze běží v kontejnerizovaném prostředí (Docker, Kubernetes) v datovém centru společnosti Hetzner ve Finsku [Helsinky], které splňuje standardy fyzické bezpečnosti (mj. ISO 27001).

1.1.2. Autentizační služba a úložiště souborů jsou zajišťovány prostřednictvím Amazon Web Services v regionu eu-central-1 (Frankfurt nad Mohanem, EU). Datová centra AWS jsou certifikována dle mezinárodních standardů (mj. ISO 27001, SOC 1/2/3) a soubory jsou v nich šifrovány (encryption at rest).

1.1.3. Webová aplikace je distribuována prostřednictvím globální sítě Cloudflare, která zajišťuje ochranu proti DDoS útokům a šifrované doručování obsahu.

1.2. Databáze Aplikace a nahrané soubory jsou uloženy na území Evropské unie. Údaje, které pro nás zpracovávají další poskytovatelé (např. doručování push notifikací, platby nebo analytika se souhlasem), mohou být zpracovány i mimo EU za podmínek uvedených v Zásadách ochrany osobních údajů.

2. Zabezpečení na úrovni aplikace

2.1. Základem ochrany dat je zajištění, aby k jednotlivým informacím měly přístup pouze oprávněné osoby:

2.1.1. Vstup do Aplikace je chráněn přihlášením e-mailem a heslem, případně ověřením prostřednictvím poskytovatele identity (Google, Apple). E-mailová adresa je při registraci ověřována.

2.1.2. Správu přihlašovacích údajů zajišťuje specializovaná autentizační služba (AWS Cognito) — hesla Uživatelů nikdy neukládáme ve vlastních systémech a nemáme k nim přístup ani my. Obnova hesla probíhá prostřednictvím jednorázového odkazu nebo kódu s omezenou platností.

2.1.3. Přístupové tokeny mají omezenou platnost (1 hodina) a jsou průběžně obnovovány. Odhlášením jsou tokeny zneplatněny na všech zařízeních.

2.1.4. Aplikace uplatňuje řízení přístupu na základě rolí: Uživatel může měnit pouze své údaje a svůj obsah a číst konverzace, jichž je účastníkem. Administrátorský přístup je vyhrazen pověřeným osobám Provozovatele.

2.1.5. Obsah určený ke zveřejnění (profily, Firemní profily, portfolia, ceníky, Recenze a fotografie k nim) je dostupný i bez přihlášení. Nahrané fotografie jsou dostupné prostřednictvím jedinečného, obtížně odhadnutelného odkazu.

2.1.6. IP adresy používané pro měření kampaní ukládáme pouze v jednosměrně zašifrované (hashované) podobě a mažeme je nejpozději po 7 dnech.

2.1.7. Veškerá komunikace mezi vaším zařízením a Aplikací probíhá šifrovaně protokolem TLS (HTTPS).

2.1.8. Provoz Aplikace je monitorován (sledování dostupnosti, výkonu a chyb), což umožňuje včasnou detekci a řešení incidentů.

3. Zálohování

3.1. Data uložená v databázi Aplikace zálohujeme denně a zálohy uchováváme s historií 30 dnů. Zálohy jsou uloženy odděleně od produkčního prostředí a slouží k obnově provozu Aplikace v případě technické závady.

3.2. Postup obnovy ze zálohy pravidelně ověřujeme.

4. Bezpečnostní incidenty

4.1. Dojde-li k porušení zabezpečení osobních údajů, Provozovatel jej bez zbytečného odkladu vyhodnotí a přijme opatření k omezení jeho následků. Je-li to podle GDPR vyžadováno, ohlásí jej do 72 hodin Úřadu pro ochranu osobních údajů a v případě vysokého rizika informuje i dotčené Uživatele.

4.2. Zjistíte-li bezpečnostní chybu nebo zranitelnost Aplikace, oznamte nám ji prosím na e-mail [info@homfi.app]. Oznámení bez zbytečného odkladu prověříme.