Red Smart

RedSmart HR - Security & Privacy

How we protect your people's information, at all times.

Your people's data is among the most sensitive there is

Names, CURP, RFC, SSN, payroll data, incidents and even health data. In RedSmart HR that information is **protected at all times** and its safekeeping is designed **into the foundation of the system**, not bolted on afterward. Here is how:

How we protect your information

Encryption at every layer

Everything travels encrypted (HTTPS/TLS) and is stored encrypted. The most sensitive data —payroll, bank account, SSN, health— gets **additional field-level encryption**, with keys guarded in **Azure Key Vault**.

Least-privilege, role-based access

Formal roles (brand admin, HR, employee): each person sees **only what pertains to them**. Sensitive data is shown masked except to authorized users.

Strong identity, passwordless

Sign in with a **passkey** and the device lock, over a modern single sign-on (SSO).

Sessions under control

If you deactivate or block someone, they **lose access immediately**. No sessions left open forever.

Traceability

We log **who views or modifies** sensitive information: for your audit and to detect any misuse.

Trusted cloud + backups

On **Microsoft Azure** (Go4IT is a Microsoft Partner), with high availability and **encrypted backups**.

We comply with the law (Mexico's LFPDPPP)

RedSmart HR is designed in accordance with Mexico's **Federal Law on Protection of Personal Data Held by Private Parties (LFPDPPP)**:

- **Privacy notice and consent** — with explicit consent for sensitive data (health, biometric).
- **ARCO rights** — your employees can Access, Rectify, Cancel or Object to the use of their data.
- **Retention and secure deletion** — we keep what labor law requires and securely delete it when the relationship ends.

Isolation between clients: two levels, no fine print

- **All plans:** your information lives **isolated per brand inside the database engine itself** (Row-Level Security): no other client can see or touch it. Field encryption uses **platform keys** guarded in Azure Key Vault.
- **Enterprise plan:** for corporate or regulatory policies that require it, we offer a **dedicated database with your own per-client encryption keys** ("your data, with your key").

Privacy by design

- **Your fingerprint never leaves the device.** The device lock is resolved by the device itself; RedSmart **never receives or stores your fingerprint**. The clock-in selfie is kept for a configurable period (90 days by default) and then deleted; facial verification (optional) uses an **encrypted template**, with express consent.
- **Minimization.** We collect and keep **only what is necessary** to comply with the law and operate.
- **Your data is yours.** Exportable whenever you want. RedSmart is white-label; we **do not sell or share** your people's information.

Microsoft Partner · Microsoft Azure · Encryption in transit and at rest · Per-brand isolation (RLS) · Backups · Role-based access · Privacy by design

Some controls are enabled depending on the implementation and the contracted plan. This document describes our security and privacy approach and does not constitute a certification. We recommend validating data handling with your legal advisor.