Privacy Policy — FluxeHRa

Status: Public transparency notice. Review with counsel before treating as final.

Effective date: 26 July 2026 **Last updated:** 26 July 2026

FluxeHRa is a registered brand of **Foil Envie SAS**, a société par actions simplifiée (SAS) registered in France ("we", "us", "Provider").

This Privacy Policy explains how we process personal data when you visit our public website (including `/`, `/trust`, `/privacy`, and related pages) and when you use the FluxeHRa SaaS application (the "Service").

For a contractual Data Processing Agreement (DPA) between FluxeHRa and a customer organization, see `/legal/dpa.md` and our Trust Center.

Contact for privacy questions: contact@fluxehra.ai

---

1. Who we are

Item	Detail
Controller / Provider	Foil Envie SAS (brand: FluxeHRa)
Contact	contact@fluxehra.ai
Product	FluxeHRa — multi-tenant HRIS / people platform

If we appoint a Data Protection Officer (DPO), contact details will be published here and on the Trust Center.

---

2. Scope

This Policy covers:

1. **Website visitors** — marketing site, Trust Center, contact form, public legal downloads.
2. **Service users** — employees, managers, HR, organization admins, and Super Admins who authenticate to FluxeHRa (including via SSO / OIDC / SAML when configured by their organization).

It applies regardless of language UI (English, French, Spanish, German, etc.).

---

3. Roles: controller vs processor

3.1 When we act as **controller**

We typically act as controller for:

- Website contact-form submissions sent to us
- Account authentication data we need to operate login (e.g. email used for Sign-In)
- Security, anti-abuse, and operational logs related to accessing our platform
- Aggregated product/performance analytics that do not include customer HR payloads by design (e.g. Vercel Analytics / Speed Insights when enabled)
- Bug reports you voluntarily send to us from the product

3.2 When we act as **processor**

For **HR and employee personal data** stored in a customer organization's FluxeHRa tenant (employee records, documents, performance content, etc.), the **customer organization is the controller**. FluxeHRa processes that data on the customer's documented instructions under a **DPA**.

If you are an employee using FluxeHRa for your employer:

- Your employer's privacy notice and policies apply to your HR data.
- Requests to access, correct, or delete HR data should normally be addressed **first to your employer**.
- We assist the customer under the DPA (including technical measures such as export / retention tools where configured).

---

4. Categories of personal data we process

4.1 Website visitors

Depending on how you use the site, we may process:

Data	Examples	Source
Contact form	First name, last name, email, message title and body	You
Technical	IP address, browser type, request metadata (standard hosting/security logs)	Your device / our hosts
Preferences	Selected marketing language (`localStorage`)	Your browser
Security challenge	Cloudflare Turnstile token/outcome when Turnstile is enabled	Cloudflare / your browser
Performance analytics	Aggregated page performance / vitals (Vercel Analytics / Speed Insights)	Runtime (aggregated)

4.2 Service users (authenticated)

Data	Examples	Source
Account identity	Email, role, organization membership	You / your organization / IdP

Data	Examples	Source
Session	Supabase Auth session cookies (`sb-*` / auth-token cookies)	Auth service
Browser session aids	`sessionStorage` keys (e.g. browser-session lock; proxy overlay state)	Your browser
Audit / security	Access and action audit events as configured	System
Support	Bug reports (page URL, description, optional stack, org context)	You
Documents	Files uploaded to Storage under your organization's tenant	You / your organization
HR domain data	Employee master data, events, performance, learning, etc.	Customer (we process as processor)

SSO (OIDC/SAML) users: your identity provider shares identity claims (typically email and related identifiers) with FluxeHRa to create or match your session. We do not receive your IdP password.

---

5. Purposes and legal bases

We process personal data to:

Purpose	Typical legal basis (GDPR)
Operate and secure the website and Service	Legitimate interests / contract
Respond to contact-form messages	Legitimate interests / pre-contract
Authenticate users and maintain sessions	Contract / legitimate interests
Provide the HRIS to customers (processor activities)	Contract (DPA) with customer; customer's legal bases apply to data subjects
Prevent abuse (e.g. Turnstile when enabled)	Legitimate interests / security
Improve reliability (aggregated analytics/vitals)	Legitimate interests
Comply with law and defend legal claims	Legal obligation / legitimate interests

---

6. Cookies and similar technologies

6.1 Essential authentication cookies

When you sign in, FluxeHRa uses **Supabase Auth** cookies (names typically starting with `sb-` or containing `auth-token`) to keep your session across requests. These are **essential** for signed-in use of the Service.

Closing all browser tabs may require you to sign in again due to an additional **browser-session lock** stored in `sessionStorage` (not an HTTP cookie).

6.2 Preferences (not cookies)

Marketing language preference may be stored in **`localStorage`** (`marketing-locale` / related keys). This is not an HTTP cookie.

6.3 Cloudflare Turnstile (optional)

When enabled by platform or organization configuration, a challenge may load from Cloudflare. That may involve **third-party** cookies or similar storage on Cloudflare's domain for the challenge. It is used to reduce bots and account enumeration—not for advertising.

6.4 Vercel Analytics / Speed Insights

The application may load Vercel Analytics and Speed Insights for aggregated performance and usage insights. These are intended to be privacy-oriented and **not** classic advertising trackers; they still constitute third-party telemetry. See also our sub-processors list.

6.5 Cookie notice on the marketing site

The homepage cookie notice explains essential session cookies. Accepting dismisses the notice for that visit; refusing clears cookies visible to JavaScript on our host and signs you out of Supabase if signed in. The notice does not itself set a long-lived "consent" cookie.

For full transparency, see this Policy and the Trust Center.

---

7. Sub-processors and hosting

Production hosting and core sub-processors (as of the date of this Policy):

- **Supabase** — database, Auth, Storage, Realtime (production region `eu-west-1`, Ireland)
- **Vercel** — web application hosting and serverless APIs (production `dub1`, Dublin)

Optional / configuration-dependent: Cloudflare Turnstile, Vercel Analytics / Speed Insights, Sentry (if configured), DocuSign (customer-configured), customer SMTP, customer IdP, customer export endpoints.

Full list: `/legal/subprocessors.md` · Trust Center

---

8. Retention

Context	Retention approach
Contact messages	Retained as needed to handle your request and related follow-up, then deleted or archived according to our internal retention practices
Auth sessions	Until logout, cookie expiry, or browser-session controls revoke local session

Context	Retention approach
Customer HR data	Controlled by the customer's configuration and instructions (retention matrix / purge tools where enabled); we do not independently decide HR retention
Audit / security logs	Retained as needed for security, accountability, and legal obligations
Bug reports	Retained as needed to investigate and improve the Service

9. International transfers

Primary production processing for the core platform is designed in the **European Union** (Supabase Ireland; Vercel Dublin).

If optional tools or customer-configured integrations process data outside the EEA/UK, appropriate transfer safeguards (e.g. SCCs) are addressed in the DPA / customer configuration and the sub-processors note.

10. Your rights

Under applicable law (including the GDPR where it applies), you may have rights to:

- access, rectification, erasure
- restriction of processing
- data portability
- objection to certain processing
- lodge a complaint with a supervisory authority (in France: CNIL)

HR data in a customer tenant: please contact **your employer (controller)** first. We support customers under the DPA.

Website contact data / our controller processing: contact contact@fluxehra.ai.

We may need to verify your identity before fulfilling a request.

11. Security

We apply technical and organizational measures appropriate to the risk (access control, encryption in transit, tenant isolation via RLS, audit capabilities, EU hosting for core services). Details for due diligence are published in the Trust Center (security white paper, ISO alignment pack, AIPD/DPIA support materials).

No method of transmission or storage is 100% secure; we continuously improve controls.

12. Children

FluxeHRa is a business/HR platform and is **not directed at children**. We do not knowingly collect personal data from children through the marketing site or Service.

---

13. Changes

We may update this Privacy Policy from time to time. The “Last updated” date at the top will change when we do. Material changes may also be highlighted on the Trust Center or by notice to customers.

---

14. Contact

Privacy and data-protection inquiries: contact@fluxehra.ai

Trust Center: /trust DPA templates: /legal/dpa.md Sub-processors: /legal/subprocessors.md Terms of Use: /legal/terms-of-use.md

---

This document is a transparency notice. It does not replace the DPA between FluxeHRa and a customer, nor an employer’s own employee privacy notice.