Data Processing Agreement (DPA) — FluxeHRa

Status: Template for customer legal review (not legal advice). Customize with counsel before signature.

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

This Data Processing Agreement ("DPA") supplements the agreement between the customer ("Controller") and **Foil Envie SAS** ("Processor"), which operates the SaaS application marketed under the **FluxeHRa** brand (the "Service").

By subscribing to or using the Service, the Controller agrees that this DPA governs the processing of personal data performed by the Processor on behalf of the Controller under Regulation (EU) 2016/679 (GDPR).

---

1. Definitions

For the purposes of this DPA:

1. "Personal Data", "Controller", "Processor", "Data Subject", "processing", "Personal Data breach", and "personal data transfer" have the meanings given in GDPR.
2. "Controller Instructions" means the Controller's documented instructions for processing, including the Service configuration, the types of data the Controller uploads/enters, and retention/deletion requests made using the Service's features or otherwise in writing.
3. "Sub-processor" means another processor engaged by the Processor to process Personal Data for the Service.

---

2. Scope and subject matter

1. **Subject matter:** The Processor processes Personal Data in the Service's multi-tenant HRIS functionality (Core HR and related modules that are enabled by the Controller/its Super Admin).
2. **Nature and purpose:** Hosting, storage, retrieval, transmission, and support related to employee lifecycle workflows configured by the Controller (including onboarding, employee data updates, learning records, performance documents, notifications, and integration export, where activated).
3. **Roles:** The Controller determines the purposes and means of processing employee personal data. The Processor processes such Personal Data on the Controller's behalf.
4. **Data subject categories:** employees, managers, HR users, authorized administrators, and (where the Controller uses onboarding features) candidates requesting employee data.
5. **Duration:** for the term of the subscription(s), and thereafter for any period strictly necessary to comply with legal obligations and to complete orderly deletion/return as described in Section

10.

---

3. Processing on documented Controller Instructions

1. The Processor processes Personal Data only on documented Controller Instructions, including:

- Service configuration and activated modules; - which personal data fields are configured/used by the Controller; - the Controller's organization-level actions (e.g., employee records, learning enrollments, documents, exports, and deletion/DSAR requests).

1. If the Processor considers an instruction to be unlawful under applicable data protection law, it will inform the Controller promptly.

---

4. Processor obligations (Article 28 GDPR)

4.1 Confidentiality

The Processor ensures that persons authorized to process Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

4.2 Security of processing (Article 32 GDPR)

The Processor implements appropriate technical and organizational measures, taking into account the state of the art, implementation costs, and the nature of the processing and risks. Measures include (as implemented in the Service):

1. **Tenant isolation:** PostgreSQL Row Level Security (RLS) keyed by organization/tenant, designed to prevent cross-organization access.
2. **Application-level authorization checks** for privileged operations.
3. **Application-layer encryption** for sensitive schema fields marked as sensitive (server-side encryption applied before insertion into PostgreSQL; current format uses an `ENC2::` prefix with authenticated encryption).
4. **Private document storage** in Supabase Storage (private bucket commonly referenced as `documents`), including HR documents and learning assets (e.g., SCORM packages) stored under tenant-structured paths (e.g., `{orgId}/{employeeId}/...`). Access to documents is controlled by authenticated application logic and secure upload/download flows (including signed URLs where applicable).
5. **Authentication and assurance:** Supabase Auth with PKCE and optional MFA/step-up for privileged roles.
6. **Logging and auditability:** operational/audit logs to support traceability of processing actions.
7. **Hardened network controls** for upload/download paths and secure handling of integration/export flows.

The Processor will maintain and improve these measures over time, consistent with applicable security practice and risk evolution.

4.3 Personnel

The Processor ensures that authorized personnel are trained and subject to appropriate controls.

4.4 Assistance to the Controller

The Processor will reasonably assist the Controller in responding to:

1. Data Subject rights requests (access/rectification/erasure/objection/restriction/portability), to the extent the Service features and processor tooling support such assistance.
2. Controller obligations concerning DPIAs and consultations with supervisory authorities, to the extent reasonably required.
3. Data security and breach investigations, as described in Section 7.

---

5. Sub-processing

1. The Processor may engage Sub-processors to provide parts of the Service. A current list is provided in **Annex B** (and updated from time to time).
2. Where required by GDPR, the Processor will ensure Sub-processors are bound by contractual obligations providing at least the same level of protection as this DPA.
3. The Controller may request reasonable information about Sub-processor changes and the Processor will provide updates as needed for transparency obligations.

---

6. International data transfers

1. The Service is deployed using hosting and database infrastructure located primarily in the **EU/EEA** (including: Supabase project region and Vercel application hosting region configured for production).
2. If and to the extent any component of the Service involves access by Sub-processors outside the EU/EEA, the Processor will put in place appropriate safeguards required by GDPR (e.g., SCCs and related transfer measures) where applicable.

---

7. Personal Data breach notification (Article 33–34 GDPR)

1. The Processor will notify the Controller of a Personal Data breach without undue delay after the Processor becomes aware of it.
2. Taking into account the circumstances of the breach, the Processor will provide:

- description of the breach (including categories and approximate number of impacted Data Subjects and records); - likely consequences; and - measures taken or proposed to address the breach and mitigate adverse effects.

1. Where feasible, the Processor will provide additional information in phases as investigations continue.

---

8. Audit and compliance

1. The Processor will make available upon reasonable Controller request documentation sufficient to demonstrate compliance with its GDPR processor obligations (subject to confidentiality).
2. The Processor may require the Controller to execute an NDA for audit/compliance materials not already public or non-confidential.

---

9. Confidentiality of the DPA

The parties agree to maintain confidentiality of the terms of this DPA except to the extent required by law or to enable compliance verification.

---

10. Return or deletion of Personal Data (Article 28(3)(g) GDPR)

1. At the end of the Controller's use of the Service and/or subscription, the Processor will, upon Controller Instructions:

- delete Personal Data within the product's operational capabilities and after lawful retention periods, and/or - return Personal Data as reasonably required for the Controller's compliance obligations.

1. Deletion and DSAR-driven anonymization/export actions are supported through Processor tooling and product features, including organization deletion cascade and employee DSAR export/anonymization operations, subject to any legal hold or legal retention requirements configured by the Controller.

---

11. Term and termination

1. This DPA begins on the effective date of the master agreement between Controller and Processor and continues for the duration of the Service.
2. The Processor may suspend processing operations if the Controller materially breaches its obligations under the master agreement or this DPA and such breach remains unresolved after reasonable notice.

---

12. Liability

This section is intended to reflect processor obligations and does not replace the liability terms in the master agreement. Where the master agreement contains conflicting provisions with this DPA, the parties will resolve the conflict in good faith so that GDPR processor requirements are satisfied.

---

13. Governing law and dispute resolution

This DPA is governed by the laws of **France**, without regard to conflict-of-law rules.

Any dispute arising out of or in connection with this DPA shall be subject to the exclusive jurisdiction of the **courts of Lyon, France**, unless mandatory law provides otherwise.

Annex A — Processing details (for the Service)

1. **Data types:** Identification and contact information, employment data, compensation/performance/learning records, HR documents, and other local statutory fields configured by the Controller via schema/data builder features.
2. **Processing operations:** collection, storage, retrieval, organization, consultation, transmission to and from authorized systems as configured by integrations, and deletion/anonymization actions through product tooling.
3. **Access controls:** tenant-scoped access using RLS and application RBAC; document access through authenticated routes and storage controls.
4. **Primary storage locations:** employee and configuration data in Supabase PostgreSQL (RLS tenant isolation) and document/learning assets in Supabase Storage (private `documents` bucket).
5. **Security measures:** as described in Section 4.2.
6. **DSAR support:** processor tooling for employee export and anonymization, subject to product configuration and legal hold status.

Annex B — Sub-processors (transparency list)

As of July 2026 (production configuration):

| Sub-processor | Purpose | Region / notes | |---|---|---| | Supabase | Database, Auth, Storage, Realtime | `eu-west-1` (Ireland) | | Vercel | Hosting of the Next.js application & serverless APIs | `dub1` (Dublin) | | Cloudflare Turnstile (optional) | Bot/abuse protection for select auth flows when enabled | Cloudflare infrastructure (region depends on request routing) | | Vercel Analytics / Speed Insights (optional) | Aggregated performance analytics (no HR payloads by design) | `dub1` / Vercel services | | Sentry (optional) | Technical error monitoring if a Sentry DSN is configured | Region depends on Sentry configuration | | DocuSign Connect (optional integration) | E-signature workflows where enabled per organization | Region

depends on DocuSign account | | Customer-configured SMTP provider (not FluxeHRa default) | Delivery of invitation/reset emails where configured | Customer provider region | | Customer OIDC IdP (not FluxeHRa default) | SSO authentication for the organization where enabled | Customer IdP region | | Customer SFTP / webhook endpoints (not FluxeHRa default) | Integration export destinations chosen by the Controller | Customer endpoint region |

Update mechanism: The Processor may update this list to reflect changes in the Service. The Controller should treat this annex as a transparency baseline and review updates in the Service's trust/legal materials (including the sub-processor notice).

Contact

For DPA-related questions and Sub-processor list updates, contact: `contact@fluxehra.ai`

Company details

- **Processor legal entity:** Foil Envie SAS
- **Registered brand:** FluxeHRa
- **Registered office:** 8 rue Sylvestre, 69100 Lyon, France
- **R.C.S. Lyon:** 949 663 124
- **VAT number:** FR56949663124
- **SIRET:** 94966312400012
- **DPO contact:** contact@fluxehra.ai

Signatures (optional)

Controller: _____ Date: _____

Processor: Foil Envie SAS (FluxeHRa) _____ Date: _____