DPIA / AIPD Support Pack (Technical Annex)

Document type: technical annex provided by the **processor** (Foil Envie SAS — **FluxeHRa** brand) to help the **controller** (customer employer organisation) draft or complete a Data Protection Impact Assessment (GDPR Art. 35 / French AIPD).

Version: 1.0 — July 2026 **Status:** generic platform-prefilled model — **must be adapted and validated** by the customer's DPO / counsel **This is not** a complete DPIA, legal advice, or a certification.

Related documents:

- Security white paper: `/livre-blanc-securite-fluxehra.html` (or PDF)
- ISO alignment pack: `/iso-alignment-fluxehra.html`
- DPA: `/legal/dpa.md`
- Sub-processors: `/legal/subprocessors.md`
- Trust Center: `/trust`

How to use this template

| Party | Role | |-------|------| | **FluxeHRa (processor)** | Supplies the technical elements below (controls, flows, hosting, backups). | | **Customer organisation (controller)** | Completes `[TO BE COMPLETED BY THE ORGANISATION]` fields, defines purposes, legal bases, formal DPIA, and any supervisory authority consultation. |

Search for `[TO BE COMPLETED BY THE ORGANISATION]` to personalise.

---

1. Processing identification

| Item | Pre-filled / to complete | |------|-------------------------| | **Processing name** | Implementation and operation of the **FluxeHRa** HRIS for the organisation's HR management | | **Controller** | `[TO BE COMPLETED BY THE ORGANISATION: legal name, address, DPO contact]` | | **Processor** | **Foil Envie SAS** — 8 rue Sylvestre, 69100 Lyon, France — RCS Lyon 949 663 124 — SIRET 94966312400012 — VAT FR56949663124 — contact@fluxehra.ai | | **Service** | FluxeHRa — https://fluxehra.ai | | **Processor privacy contact** | contact@fluxehra.ai | | **Annex date** | July 2026 | | **Customer DPIA adoption date** | `[TO BE COMPLETED BY THE ORGANISATION]` | | **Applicable DPA** | `[TO BE COMPLETED: DPA signature date]` |

---

2. Purposes

2.1 Typical purposes covered by the platform

Depending on **modules activated** by the organisation:

| ID | Purpose | FluxeHRa modules (indicative) | |----|---------|-------------------------------| | F1 | Employee master data / employment administration | Core HR | | F2 | Compensation data and payroll-oriented exports | Compensation, API/SFTP integrations | | F3 | Performance reviews, goals, feedback | Performance Management | | F4 | Learning / SCORM / compliance training | Learning | | F5 | HR documents and optional e-signature | DMS, DocuSign (if enabled) | | F6 | Employee / manager self-service; notifications | Self-service, Notifications | | F7 | HR analytics dashboards | Analytics | | F8 | Recruitment / talent pool / succession (if enabled) | Recruitment, Talent Pool | | F9 | Data-subject rights & retention tooling | DSAR, Retention |

Modules enabled for this organisation: `[TO BE COMPLETED BY THE ORGANISATION]`

2.2 Legal bases (controller responsibility)

| Purpose | Suggested basis (validate) | |---------|----------------------------| | F1–F2, F5–F6 | Employment contract / legal HR obligations | | F3–F4, F7–F8 | Legitimate interest and/or contract / works agreement | | Special categories (Art. 9) e.g. disability | `[TO BE COMPLETED: Art. 9 exception]` |

---

3. Data subjects and data categories

Subjects: employees, managers, org admins; optionally candidates if entered in the HRIS. **Headcount / geographies:** `[TO BE COMPLETED BY THE ORGANISATION]`

| Category | Examples | Special category? | |----------|----------|-------------------| | Identity & contact | Name, emails, phone | Usually no | | Employment | Employee ID, job, manager, effective dating | No | | Compensation | Salary, bonus, equity | Business-sensitive | | Performance / learning | Reviews, goals, courses | Usually no | | Documents | Contracts, attachments | Depends on content | | Disability / RQTH (if used) | `disability_*` fields | **Yes — Art. 9** if used | | Audit / technical logs | Admin actions, proxy | No |

The customer controls which fields exist (Schema Builder) and who can see them (Data Visibility).

---

4. Data-flow schematic

```
[ Org users: HR / Manager / Employee / Admin ]
        │  HTTPS (TLS) + JWT session (Supabase Auth)
        ▼
[ FluxeHRa app — Vercel dub1 (Dublin, EEA) ]
        │  server authz + rate limiting
        ▼
[ Supabase — eu-west-1 (Ireland, EEA) ]
   ├─ PostgreSQL + Row Level Security (tenant isolation)
   ├─ Auth
   ├─ Private Storage (documents)
   └─ Realtime (in-app notifications)
        │
```

```
        ├──► [ Customer SMTP ] transactional email (optional)
        ├──► [ Customer OIDC IdP ] SSO (optional)
        ├──► [ Payroll / SFTP / webhooks ] exports (optional)
        └──► [ DocuSign — customer account ] e-sign (optional)
```

Isolation: shared schema with `organization_id` + PostgreSQL RLS; private document paths under `org/{orgId}/…`.

Production hosting: primary data and app execution in the **EEA** (Ireland / Dublin). Optional customer-chosen tools (SMTP, DocuSign, SFTP, IdP) are the customer's responsibility for transfer assessments.

---

5. Security measures matrix (for DPIA)

| Domain | FluxeHRa control | Where to verify | |--------|------------------|-----------------| | Access control | RBAC, module permissions, HR scope, field visibility | Org Setup → Manage Roles / Data Visibility | | Encryption in transit | HTTPS, HSTS | Security white paper | | Encryption at rest | Supabase disk encryption + app-level `sensitive` field crypto (`ENC2::`, AES-256-GCM) | White paper § encryption | | Integrity | Effective-dated Core HR history, audit trail | Audit Trail | | Availability | Managed Supabase / Vercel; platform backups | Backup/restore ops docs; Supabase plan | | Traceability | `audit_logs` (real vs proxied actor) | Audit Trail | | Minimisation / PbD | Typed schemas, restrictive defaults, private storage, privileged MFA | White paper / Privacy by Design note | | Sub-processing | DPA + sub-processor list | `/legal/dpa.md`, subprocessors | | Data-subject rights tooling | DSAR export, anonymisation, retention purge | HR compliance features |

---

6. Backups & continuity

| Layer | Mechanism | DPIA note | |-------|-----------|-----------| | Postgres & Storage | Supabase backups / PITR (plan-dependent) | Record contracted RPO/RTO | | Application | Immutable Vercel deployments | App rollback ≠ data restore | | Contract end | Delete / return per DPA | Document exit scenario |

`[TO BE COMPLETED BY THE ORGANISATION: target RPO/RTO if required internally]`

---

7. Retention

Field-level `retentionMonths`, real analyse/purge APIs, document retention triggers, optional legal hold.
Customer retention policy: `[TO BE COMPLETED BY THE ORGANISATION]`

---

8. Recipients

Authorised org users; Foil Envie SAS (need-to-know support); Supabase; Vercel; plus any customer-configured SMTP / IdP / payroll / DocuSign endpoints.

---

9. Shared residual risks (summary)

| Risk | Reduced by FluxeHRa | Remains with customer | |------|---------------------|-----------------------| | Cross-tenant access | RLS + API scope checks | Account hygiene / MFA | | Sensitive data leakage | Field encryption, private storage, TLS | Avoid unnecessary Art. 9 data | | Over-retention | Retention/purge tools | Configure lawful periods | | Health-data hosting (HDS) | **FluxeHRa is not HDS / SecNumCloud certified** | Do not store occupational health dossiers unless a dedicated compliant offer exists |

Risk acceptance decision: `[TO BE COMPLETED BY THE ORGANISATION]`

---

10. Customer DPIA checklist

- [ ] Involve DPO
- [ ] Confirm DPIA necessity (Art. 35 / local guidance)
- [ ] List enabled FluxeHRa modules
- [ ] Complete all `[TO BE COMPLETED BY THE ORGANISATION]` fields
- [ ] Document legal bases / Art. 9 if any
- [ ] Configure Data Visibility & Retention
- [ ] Sign DPA; archive sub-processor list
- [ ] Define data-subject request procedure
- [ ] Schedule periodic DPIA review
- [ ] Attach security white paper + this annex to the DPIA file

---

11. Revision history

| Version | Date | Reason | |---------|------|--------| | 1.0 | 2026-07-23 | Initial generic DPIA/AIPD technical support annex |

Provided by Foil Envie SAS (FluxeHRa) — contact@fluxehra.ai