Support à l'AIPD (Analyse d'Impact relative à la Protection des Données)

Nature du document : annexe technique fournie par le **sous-traitant** (Foil Envie SAS — marque **FluxeHRa**) pour aider le **responsable du traitement** (organisation cliente / employeur) à rédiger ou compléter son AIPD / DPIA (art. 35 RGPD).

Version : 1.1 — septembre 2026 **Statut :** modèle générique prérempli côté plateforme — **à adapter et valider** par le DPO / conseil du client **Ce document n'est pas** une AIPD complète, ni un avis juridique, ni une certification.

Documents complémentaires :

- Livre blanc sécurité : `/livre-blanc-securite-fluxehra.html` (ou PDF)
- Pack d'alignement ISO : `/iso-alignment-fluxehra.html` (annexe A 2022 complète — 93 contrôles)
- DPA : `/legal/dpa.fr.md`
- Sous-traitants : `/legal/subprocessors.md`
- Trust Center : `/trust`
- Privacy by Design (Art. 25) : disponible via SU Admin → Documentation (interne / commercial)

Comment utiliser ce modèle

Qui	Rôle
FluxeHRa (sous-traitant)	Fournit les éléments techniques ci-dessous (mesures, flux, hébergement, sauvegardes).
Organisation cliente (responsable)	Complète les cases `[À COMPLÉTER PAR L'ORGANISATION]`, décide des finalités, bases légales, DPIA formelle, consultation éventuelle de la CNIL.

Cases à personnaliser : rechercher `[À COMPLÉTER PAR L'ORGANISATION]` dans ce fichier.

---

1. Identification du traitement (fiche signalétique)

Élément	Contenu prérempli / à compléter
Nom du traitement	Mise en œuvre et exploitation du SIRH **FluxeHRa** pour la gestion des ressources humaines de l'organisation

Élément	Contenu prérempli / à compléter
Responsable du traitement	`[À COMPLÉTER PAR L'ORGANISATION : raison sociale, adresse, contact DPO]`
Sous-traitant (éditeur / hébergeur applicatif)	**Foil Envie SAS** — 8 rue Sylvestre, 69100 Lyon, France — RCS Lyon 949 663 124 — SIRET 94966312400012 — TVA FR56949663124 — contact@fluxehra.ai
Marque / service	FluxeHRa — https://fluxehra.ai
Référent privacy sous-traitant	contact@fluxehra.ai
Date de rédaction de cette annexe	Juillet 2026 (rév. plateforme)
Date d'adoption AIPD client	`[À COMPLÉTER PAR L'ORGANISATION]`
Version DPA applicable	`[À COMPLÉTER : date de signature du DPA]`

---

2. Finalités du traitement

2.1 Finalités typiques couvertes par la plateforme (préremplies)

Selon les **modules activés** par l'organisation :

Code	Finalité	Modules FluxeHRa (indicatif)
F1	Gestion administrative du personnel (dossier, emploi, organisation, poste)	Core HR
F2	Gestion des éléments de rémunération et exports vers paie locale	Compensation, intégrations API/SFTP
F3	Évaluation, objectifs, feedback (entretiens / performance)	Performance Management
F4	Formation, conformité learning, contenus SCORM	Learning
F5	Documents RH (contrats, pièces) et signature électronique optionnelle	DMS, DocuSign (si activé)
F6	Self-service employé / manager ; notifications RH	Self-service, Notifications
F7	Analytique RH (tableaux de bord / agrégats)	Analytics
F8	Recrutement / vivier / succession (si activé)	Recruitment, Talent Pool
F9	Exercice des droits et conformité (export, anonymisation, rétention)	DSAR, Retention

Modules effectivement activés pour cette organisation : `[À COMPLÉTER PAR L'ORGANISATION : liste des modules ON]`

2.2 Bases légales (responsabilité du client)

Finalité	Base légale proposée (à valider)	Commentaire
F1–F2, F5–F6	Exécution du contrat de travail / obligations légales RH	À confirmer par le DPO client
F3–F4, F7–F8	Intérêt légitime et/ou contrat / accord d'entreprise	Documenter le bilan
Catégories particulières (Art. 9) — ex. handicap/RQTH	`[À COMPLÉTER : exception Art. 9 retenue]`	Champs éventuels `disability_*` marqués sensibles côté produit

---

3. Personnes concernées et données

3.1 Catégories de personnes concernées

- Salariés / collaborateurs
- Managers
- Administrateurs RH / IT de l'organisation
- Le cas échéant : candidats, prestataires (si saisis dans le SIRH)

Effectif approximatif : `[À COMPLÉTER PAR L'ORGANISATION]` **Zones géographiques :** `[À COMPLÉTER : pays des personnes concernées]`

3.2 Catégories de données (générique plateforme)

Catégorie	Exemples	Sensible / Art. 9 ?
Identité & contact	Nom, prénom, e-mail pro/perso, téléphone	Non (sauf contexte)
Vie professionnelle	Matricule, poste, manager, dates d'effet, organisation	Non
Rémunération	Salaire, bonus, equity (si module)	Peut être sensible métier
Performance / formation	Évaluations, objectifs, parcours, attestations	Non (sauf contenu spécifique)
Documents	Contrats, pièces jointes	Selon contenu
Données locales / statutaires	Champs pays configurés par le client	Selon pays
Handicap / RQTH (si utilisés)	`disability_status`, `disability_disclosure`	**Oui — Art. 9** si activés
Logs techniques / audit	Connexions, actions admin, proxy	Non

Le client contrôle quels champs existent (Schema Builder) et qui les voit (Data Visibility).

4. Schéma de flux de données (architecture)

4.1 Vue d'ensemble

```
[ Utilisateurs org : RH / Manager / Employé / Admin ]
        │  HTTPS (TLS) + session JWT (Supabase Auth)
        ▼
[ Application FluxeHRa — Vercel, région dub1 (Dublin, EEE) ]
        │  contrôles d'autorisation applicatifs + rate limiting
        ▼
[ Supabase — eu-west-1 (Irlande, EEE) ]
   ├─ PostgreSQL + Row Level Security (isolation multi-tenant)
   ├─ Auth (GoTrue)
   ├─ Storage privé (documents)
   └─ Realtime (notifications in-app)
        │
        ├──► [ SMTP configuré par l'org ] e-mails transactionnels (optionnel)
        ├──► [ IdP OIDC de l'org ] SSO (optionnel)
        ├──► [ Paie / SFTP / webhooks client ] exports (optionnel)
        └──► [ DocuSign — compte client ] signature (optionnel)
```

4.2 Principes d'isolation

Mécanisme	Description
Multi-tenant	Chaque enregistrement métier porte un `organization_id`
RLS	Politiques PostgreSQL : un utilisateur d'une org ne lit pas les données d'une autre
API	Périmètre org vérifié côté serveur pour les opérations admin
Documents	Chemins `org/{orgId}/…` ; bucket privé ; lecture via API authentifiée

4.3 Transferts hors EEE

Production FluxeHRa : stockage principal et exécution applicative en **Irlande / Dublin (EEE)**.

Flux optionnel	Qui choisit	Garanties
Turnstile (Cloudflare)	Activation SU / org	Anti-bot ; pas de dossier RH métier
DocuSign	Organisation	Compte et facturation **client**
SMTP / SFTP / OIDC / webhooks	Organisation	Responsabilité du client sur le destinataire

Tout transfert hors EEE imposé par un outil **client** doit être documenté dans l'AIPD du client.

---

5. Matrice des mesures de sécurité (éléments techniques pour l'AIPD)

Alignement indicatif art. 32 RGPD — détail dans le livre blanc sécurité.

Domaine	Mesure FluxeHRa	Preuve / où vérifier
Confidentialité — accès	RBAC, permissions modules, périmètre HR, matrice Data Visibility	Org Setup → Manage Roles ; Data Visibility
Confidentialité — chiffrement transit	HTTPS, HSTS	En-têtes HTTP / livre blanc
Confidentialité — chiffrement repos	Chiffrement infra Supabase + chiffrement applicatif des champs `sensitive` (`ENC2::`, AES-256-GCM)	Livre blanc §10
Intégrité	Historisation à date d'effet (Core HR), audit trail, validations schéma	Audit Trail ; Core HR
Disponibilité	Hébergement managé Supabase / Vercel ; sauvegardes plateforme	`docs/backup-restore.md` (ops) ; contrat Supabase
Résilience / incident	Procédure incident ; notification client sans retard injustifié	DPA ; incident-response
Traçabilité	`audit_logs` (acteur réel / proxy)	Org Setup → Audit Trail
Minimisation	Schémas typés, listes fermées, pas de free-text imposé	Schema Builder
Privacy by default	Visibilité restrictive champs sensibles ; MFA privilégiée (défaut prod) ; storage privé	Livre blanc ; Setup
Sous-traitance	DPA + liste sous-traitants ultérieurs	`/legal/dpa.fr.md`, subprocessors
Droits des personnes	Export DSAR, anonymisation, rétention/purge configurables	APIs / écrans RH conformité

---

6. Sauvegardes et continuité

Couche	Mécanisme	Notes pour l'AIPD client
Base PostgreSQL & Storage	Sauvegardes / PITR selon **offre Supabase** du projet FluxeHRa	RPO/RTO à reporter depuis le plan contractualisé FluxeHRa / hébergeur
Application	Déploiements immutables Vercel	Rollback applicatif ≠ restauration des données
Fin de contrat	Suppression / restitution selon DPA	Prévoir scénario de sortie dans l'AIPD

À compléter par l'organisation (si exigé en interne) : `[RPO cible]`, `[RTO cible]`, `[fréquence de revue PRA]`

---

7. Durées de conservation

Mécanisme produit	Description
Rétention par champ	`retentionMonths` après départ — configurable
Purge	Analyse et purge réelles via fonctionnalités RH
Documents	Rétention / expiration par type documentaire
Legal hold	Peut bloquer anonymisation / certaines opérations
Logs d'audit	Conservation selon politique ops FluxeHRa + besoin client

Politique de conservation adoptée par l'organisation : `[À COMPLÉTER PAR L'ORGANISATION — ex. : bulletins 5 ans, dossiers …]`

8. Destinataires

Destinataire	Rôle
Utilisateurs autorisés de l'organisation	Selon rôles et visibilité
Foil Envie SAS	Support / exploitation strictement nécessaire
Supabase	Hébergement BDD, Auth, Storage (EEE)
Vercel	Hébergement app / API (EEE)
Autres (SMTP, IdP, paie, DocuSign…)	Uniquement si configurés par le client

9. Droits des personnes et assistance

Le sous-traitant met à disposition des **outils** (export, anonymisation, rétention) ; le **responsable** reste garant de l'exercice des droits (délais, réponse aux personnes, registre des demandes).

Droit	Support technique FluxeHRa
Accès / portabilité	Export DSAR (JSON)
Effacement / limitation	Anonymisation / purge selon config et legal hold
Rectification	Workflows Core HR / self-service selon habilitations
Opposition	Processus organisationnel client (+ config champs)

Procédure interne client : `[À COMPLÉTER PAR L'ORGANISATION]`

10. Risques résiduels et responsabilités partagées

10.1 Risques typiques (aide à la cotation client)

Risque	Facteurs de réduction côté FluxeHRa	Reste à charge client
Accès non autorisé inter-organisations	RLS, contrôles API	Gestion des comptes et MFA utilisateurs
Fuite de données sensibles	Chiffrement champ, storage privé, TLS	Ne pas stocker de données de santé hors besoin ; DPIA Art. 9
Mauvaise conservation	Outils de rétention/purge	Paramétrer les délais légaux
Sous-traitant non conforme	DPA, UE hosting	Valider DocuSign/SMTP/SFTP choisis
Données de santé / HDS	**FluxeHRa n'est pas certifié HDS ni SecNumCloud**	Ne pas exiger HDS sans offre dédiée ; minimiser Art. 9

10.2 Décision d'acceptabilité du risque

`[À COMPLÉTER PAR L'ORGANISATION : risque accepté / mesures complémentaires / avis DPO]`

---

11. Checklist AIPD — ce que le client doit encore faire

- [ ] Désigner / consulter le DPO
- [ ] Confirmer la nécessité d'une AIPD (critères CNIL / art. 35)
- [ ] Lister les modules FluxeHRa réellement activés
- [ ] Remplir toutes les cases `[À COMPLÉTER PAR L'ORGANISATION]`
- [ ] Documenter bases légales et éventuel Art. 9
- [ ] Paramétrer Data Visibility & Retention
- [ ] Signer le DPA et archiver la liste des sous-traitants
- [ ] Définir la procédure d'exercice des droits
- [ ] Planifier revue périodique de l'AIPD (ex. annuelle ou à tout changement majeur)
- [ ] Joindre le livre blanc sécurité + cette annexe au dossier AIPD

---

12. Historique

Version	Date	Auteur	Motif
1.0	2026-07-23	Foil Envie SAS / FluxeHRa	Première annexe technique générique de support à l'AIPD

13. Accusé de réception (optionnel)

Organisation : _____ Nom / fonction : _____ Date : _____ Signature : _____

Document fourni par Foil Envie SAS (FluxeHRa) — contact@fluxehra.ai