Procédures opérationnelles — IG00 Core

13 procédures documentées au titre de l'ISO/IEC 42001 Annex A et des obligations AI Act

Document	PROCEDURES_V1
Version	1.0
Date	17 juin 2026
Auteur	Jean-Paul Koslowski, président 00Source SASU
Périmètre	IG00 Core — 9 actifs techniques + 3 actifs documentaires
Référentiels	ISO/IEC 42001:2023 Annex A — AI Act Articles 9, 10, 12, 13, 14, 15, 17, 50 — RGPD Articles 17 et 20

Sommaire

Chaque procédure suit la même trame : Objet, Périmètre, Responsable, Déclencheur, Étapes, Preuves, KPI, Revue.

P1 — Gouvernance des données

Objet : encadrer la collecte, le traitement et la conservation des données utilisateurs traitées par les systèmes embarquant IG00 Core. **Périmètre** : IG00 Core et tout déploiement applicatif sous gouvernance Constitution00. **Responsable** : référent données et RGPD (Jean-Paul Koslowski à la date V1). **Déclencheur** : tout traitement de données utilisateur passant par le pipeline IG00.

Étapes

1. Identifier la finalité du traitement (auto-déterminée par l'applicatif déployeur)
2. Vérifier la base légale RGPD applicable
3. Tracer le traitement dans `logs00.jsonl` avec horodatage
4. Appliquer le chiffrement BYOK AES-256-GCM (cf. P8) aux clés des fournisseurs LLM
5. Informer l'utilisateur de l'interaction avec un système IA (Art 50 AI Act, cf. P7)
6. Permettre l'exercice des droits RGPD (cf. P9)

Preuves : `logs00.jsonl`, table `security_events`, code source `server/lib/byok-secure.js`. **KPI** : 100 % des traitements tracés. Zéro fuite de clé. **Revue** : annuelle, alignée sur POLITIQUE_IA §9.

P2 — Supervision humaine

Objet : garantir l'effectivité du seuil de retrait 00− et de la validation humaine H00 en zone 00+. **Périmètre** : toute interaction passant par IG00 Core. **Responsable** : référent traçabilité (Jean-Paul Koslowski à la date V1). **Déclencheur** : chaque requête utilisateur entrante.

Étapes

1. Calcul du qualifieur 4D00 / 5D00 (signature sémantique locale)
2. Détermination de la zone (00− / 00± / 00+) selon `space_ig00.js`
3. Si zone 00+ : impossibilité algorithmique de poursuivre sans validation H00 effective de l'utilisateur ou d'un opérateur habilité
4. Si zone 00± : aide à la décision présentée comme telle, ne se substituant jamais à la décision finale
5. Possibilité de retrait inconditionnel à tout moment (Pacte du Seuil00)
6. Restitution de la réponse gouvernée avec mention de la zone et du niveau humain

Preuves : champ `niveau_humain` dans `logs00.jsonl`, tests Constitution00 39 cas (Soleau 6). **KPI** : 100 % des opérations Zone 00+ avec validation H00 effective. Zéro court-circuit détecté. **Revue** : annuelle + audit code mensuel des modules `space_ig00.js` et `resolveIG00Mode.js`.

P3 — Traçabilité et journalisation

Objet : assurer la traçabilité horodatée immuable de toutes les opérations IG00 Core. **Périmètre** : pipeline complet IG00 Core (recevabilité, qualification, routage, restitution). **Responsable** : référent traçabilité. **Déclencheur** : chaque appel passant par `routes00.js`.

Étapes

1. Génération d'un `trace_id` unique au point d'entrée
2. Capture du prompt utilisateur (anonymisé si configuré par le déployeur)
3. Capture de la signature 4D00 / 5D00 complète
4. Capture du mode IG00 retenu et du niveau humain
5. Capture de l'agent du Registry ou du fournisseur LLM sollicité
6. Capture de la réponse brute et de la réponse gouvernée
7. Calcul de l'indice de cohérence
8. Écriture en JSONL dans `server/trace/logs00.jsonl`

Preuves : fichier `logs00.jsonl` lisible en clair, table `security_events` PostgreSQL. **KPI** : 100 % des opérations tracées. Aucune trace tronquée détectée. **Revue** : annuelle. Politique d'archivage à formaliser dans le cadre d'une certification ultérieure portée par un partenaire.

P4 — Gestion des incidents

Objet : encadrer la détection, l'analyse, le traitement et la remédiation des anomalies et incidents. **Périmètre** : IG00 Core et son infrastructure. **Responsable** : référent sécurité applicative + référent traçabilité. **Déclencheur** : signal automatique de la table `security_events`, ou signalement par un tiers via `jpk@ig00.org`.

Étapes

1. Réception du signal d'incident (auto ou manuel)
2. Qualification — gravité (mineur / majeur / critique), périmètre, durée
3. Analyse — recherche de cause racine, examen des traces, examen du code source si nécessaire
4. Traitement immédiat — correction de la cause si possible, ou contournement temporaire
5. Documentation dans un journal d'incidents (à formaliser dans `docs/conformite/v1/incidents.md`)
6. Si incident critique sur un applicatif régulé : notification à l'autorité compétente selon AI Act Article 73 (porté par le déployeur)
7. Revue post-incident pour amélioration

Preuves : table `security_events`, journal d'incidents, commits git de remédiation. **KPI** : délai de prise en charge initial < 24 h pour incident majeur ou critique. Temps moyen de remédiation à mesurer post-V1. **Revue** : annuelle. Premier rapport d'incidents publié dans la revue annuelle 2027.

P5 — Revue annuelle de la conformité

Objet : produire une revue documentée annuelle du système de management IG00 Core et publier les scores d'auto-évaluation actualisés. **Périmètre** : ensemble du dossier conformité IG00 Core. **Responsable** : signataire de la politique IA (Jean-Paul Koslowski à la date V1, ou successeur). **Déclencheur** : échéance annuelle (17 juin de chaque année), ou événement structurant (transfert, désignation successeur, évolution majeure).

Étapes

1. Compilation des KPI de l'année écoulée (P1 à P12)
2. Compilation des incidents et de leur traitement (P4)
3. Revue article par article des scores AI Act et ISO 42001
4. Décision de mise à jour ou de maintien
5. Compte-rendu écrit signé
6. Publication sur `ig00.org/conformite` et information du comité éthique externe si activé

Preuves : compte-rendu annuel signé, mises à jour publiées sur `ig00.org/conformite`. **KPI** : revue effective au plus tard le 30 juin de chaque année. **Revue** : auto-référente, mécanisme d'amélioration continue.

P6 — Formation et sensibilisation

Objet : assurer la sensibilisation des personnes intervenant sur IG00 Core, et des déployeurs applicatifs. **Périmètre** : titulaire actuel des rôles + partenaires repreneurs + déployeurs. **Responsable** : signataire de la politique IA. **Déclencheur** : entrée d'un nouveau partenaire ou licencié, ou évolution majeure du framework.

Étapes

1. **Titulaire actuel** : auto-formation continue documentée par les dépôts Soleau, le présent dossier de conformité, et la base mémoire `CLAUDE.md`
2. **Partenaire repreneur / licencié** : transmission du dossier de conformité publié + session de transfert de connaissances par le conseil de transition (cf. MATRICE_ROLES §6.1)

3. **Déployeur applicatif** : référence à `ig00.org/conformite` pour la documentation publique, possibilité d'accompagnement contractuel
4. **Utilisateur final** : information de l'interaction avec un système IA (Art 50 AI Act) intégrée à l'applicatif

Preuves : trace des dépôts Soleau, mémoire projet `CLAUDE.md`, accords de transfert de connaissances dans les actes de cession ou licence. **KPI** : 100 % des nouveaux partenaires bénéficient d'une session de transfert documentée. **Revue** : annuelle.

P7 — Classification AI Act des applicatifs

Objet : guider les déployeurs dans la classification de leurs applicatifs embarquant IG00 Core selon les catégories AI Act. **Périmètre** : tout applicatif final embarquant IG00 Core. **Responsable** : déployeur, avec recommandation du référent conformité 00Source. **Déclencheur** : déploiement d'un nouvel applicatif ou modification structurante d'un applicatif existant.

Étapes

1. Identifier la finalité de l'applicatif
2. Vérifier l'inscription éventuelle dans l'**Annex III** AI Act (haut risque)
3. Sinon, vérifier l'interaction avec une personne physique (risque limité Art 50)
4. Classifier l'applicatif et documenter la classification
5. Si haut risque : engager les obligations Annex IV complètes, conformity assessment notifié, marquage CE (à la charge du déployeur, **pas à la charge d'IG00 Core seul**)
6. Si risque limité : assurer la mention d'interaction IA (Art 50) et l'option de retrait
7. Informer 00Source ou son successeur du résultat de la classification pour mise à jour du registre des déploiements

Preuves : registre des déploiements (à mettre en place post-V1), classification documentée pour chaque applicatif. **KPI** : 100 % des déploiements connus classifiés. Zéro non-conformité Art 50 détectée. **Revue** : annuelle.

P8 — Architecture BYOK et gestion des clés

Objet : garantir l'intégrité et la confidentialité des clés d'accès aux fournisseurs LLM. **Périmètre** : tout fournisseur LLM utilisé sous gouvernance IG00 Core. **Responsable** : référent sécurité applicative. **Déclencheur** : ajout, rotation ou retrait d'une clé fournisseur.

Étapes

1. Génération ou réception de la clé fournisseur (OpenAI, Anthropic, Groq, Mistral, HF, etc.)
2. Chiffrement immédiat avec algorithme **AES-256-GCM** (Sprint P3 sécurité, mai 2026)
3. Stockage en base PostgreSQL ou variable d'environnement Render selon le palier
4. Aucune écriture en clair dans les logs ou la sortie utilisateur
5. Rotation périodique recommandée (au moins annuelle)
6. Révocation immédiate en cas de soupçon de compromission, avec entrée dans `security_events`

Preuves : code `server/lib/byok-secure.js`, configuration Render, audit code mensuel. **KPI** : zéro clé en clair détectée. Zéro incident de fuite. **Revue** : annuelle + audit code mensuel.

P9 — Exercice des droits RGPD (Articles 17 et 20)

Objet : permettre l'exercice effectif des droits d'effacement et de portabilité des données utilisateurs. **Périmètre** : données utilisateurs collectées par les applicatifs embarquant IG00 Core. **Responsable** : référent données et RGPD. **Déclencheur** : demande de l'utilisateur via les canaux prévus par l'applicatif ou directement à 00Source.

Étapes

1. Réception de la demande (Art 17 effacement ou Art 20 portabilité)
2. Vérification de l'identité du demandeur
3. Localisation des données concernées (base PostgreSQL, logs, traces)
4. **Art 17** : effacement effectif sous 30 jours maximum, confirmation au demandeur
5. **Art 20** : restitution des données en format machine-lisible (JSON ou CSV) sous 30 jours maximum
6. Documentation de la demande et de son traitement

Preuves : implémentation V10.19 vérifiable dans le code source, journal des demandes. **KPI** : 100 % des demandes traitées dans les 30 jours réglementaires. **Revue** : annuelle.

P10 — Sécurité applicative

Objet : maintenir et faire évoluer le Sprint sécurité P1-P8 mis en production en mai 2026. **Périmètre** : infrastructure et code applicatif 00Source. **Responsable** : référent sécurité applicative. **Déclencheur** : déploiement, signalement de vulnérabilité, revue annuelle.

Étapes

1. Maintien des huit volets P1-P8 : Helmet headers, rate-limit, BYOK AES-256-GCM, validation Joi, sanitizer post-LLM, RGPD Art 17/20, Kids00 guard, `security_events`
2. Mise à jour des dépendances `npm` à la prise de connaissance d'une vulnérabilité CVE
3. Surveillance hebdomadaire des journaux `security_events`
4. Audit code mensuel des modules sensibles (qualifieur sémantique, BYOK, RGPD)
5. Suggestion : pen test externe annuel à porter par un partenaire repreneur (cf. ROADMAP_V1)

Preuves : présent code source, table `security_events`, commits de mise à jour. **KPI** : zéro CVE critique non patchée au-delà de 7 jours. **Revue** : annuelle + audit mensuel.

P11 — Évaluation des fournisseurs LLM

Objet : encadrer l'ajout, le retrait ou la mise à jour des fournisseurs LLM utilisés sous gouvernance IG00 Core. **Périmètre** : tous les fournisseurs LLM listés en INVENTAIRE §2. **Responsable** : signataire de la politique IA. **Déclencheur** : proposition d'ajout d'un nouveau fournisseur, retrait d'un fournisseur existant, changement substantiel des conditions de service d'un fournisseur.

Étapes

1. Évaluation de la **juridiction du traitement** (juridiction du fournisseur, transferts internationaux, adéquation RGPD)
2. Évaluation de la **disponibilité d'un endpoint stable** et documenté
3. Évaluation du **mécanisme BYOK** ou équivalent
4. Évaluation des **conditions de service** au regard de la Constitution00 (absence de revendication décisionnelle, droit de retrait utilisateur)
5. Évaluation des **conditions tarifaires** soutenables sans dépendance unique
6. Décision documentée d'ajout, de maintien ou de retrait
7. Mise à jour de l'inventaire INVENTAIRE §2

Preuves : tableau des fournisseurs dans INVENTAIRE §2, journal des décisions d'évaluation. **KPI** : 100 % des fournisseurs inscrits ont fait l'objet d'une évaluation documentée. **Revue** : annuelle.

P12 — Signature SHA-256 du Registry

Objet : assurer l'intégrité cryptographique des entités du 00Registry par signature SHA-256. **Périmètre** : 119 agents + 35 intentions = 154 entités à la date V1. **Responsable** : owner technique du Registry. **Déclencheur** : création, modification ou retrait d'une entité du Registry.

Étapes

1. À la création d'une entité, calcul de la signature SHA-256 sur les champs canoniques (nom, type, intentions compatibles, zone autorisée, audience, risque, version)
2. Stockage de la signature dans le champ `signature_sha256` de la table `agents_registry` ou `intentions00`
3. Publication via les routes `/00registry/public` (agents) et `/api/intentions/list` (intentions)
4. À toute modification : recalcul de la signature, mise à jour du champ, versioning git
5. Vérification automatique mensuelle de la cohérence entre les signatures stockées et le contenu canonique

Preuves : tables `agents_registry` et `intentions00`, scripts de vérification dans `server/scripts/`. **KPI** : 100 % de signatures valides. Détection immédiate de toute altération. **Revue** : annuelle + vérification automatique mensuelle.

P13 — Vérification d'intégrité par tiers (triple ancrage)

Objet : permettre à tout tiers (utilisateur, partenaire, régulateur, contradicteur) de vérifier indépendamment l'authenticité d'une entité revendiquant l'appartenance à IG00. **Périmètre** : ensemble du 00Registry et des actifs IG00 Core ancrés. **Responsable** : tiers vérificateur, avec support documentaire de 00Source. **Déclencheur** : suspicion d'altération ou de contrefaçon, demande d'authentification, due diligence d'un partenaire repreneur.

Étapes

1. **Récupérer la signature SHA-256 publiée** pour l'entité concernée via `GET /api/intentions/list` (intentions) ou `/00registry/public` (agents)
2. **Recalculer la signature SHA-256** sur les champs canoniques de l'entité reçue par ailleurs (l'outil de calcul est publié dans le dépôt source 00Source)
3. **Comparer les deux signatures** : égalité = intégrité préservée ; divergence = altération
4. **Vérifier le DNS du `domain00` associé** : un `nslookup` doit pointer vers l'infrastructure Render contrôlée par 00Source. Pointage ailleurs = signal d'usurpation
5. **Croiser avec les références Soleau INPI** listées dans INVENTAIRE §3.1 : consulter l'enveloppe Soleau correspondante en cas de doute juridique sur l'antériorité
6. **En cas de divergence avérée** : transmettre les éléments à 00Source via `jpk@ig00.org` pour qualification et action éventuelle (opposition INPI, action en contrefaçon, etc.)

Preuves : routes publiques `/api/intentions/list` et `/00registry/public`, INVENTAIRE §3, dépôts Soleau INPI 1 à 16. **KPI** : aucun (procédure ouverte à tout tiers, métriques non centralisées). **Revue** : annuelle, en synthèse des éventuels signalements reçus.

Schéma de convergence des trois ancres

Cas	Soleau INPI	Signature SHA-256	Domaine DNS	Verdict
Entité légitime IG00	✓ daté	✓ valide	✓ JPK/00Source	**Canonique**
Fork légitime communiqué	✓ Soleau d'origine	✗ signature divergente	possible	**Fork tracé**
Contrefaçon	✗ aucun dépôt	✗ signature absente	✗ tiers non agréé	**Parasitique, opposable**
Doublon malveillant sous même nom	✗	✗	✗	**Détectable et opposable**

Revue des procédures

L'ensemble des 13 procédures est revu **au moins une fois par an** en cohérence avec la revue de politique IA (POLITIQUE_IA §9). Toute évolution structurante du framework IG00 Core ou des référentiels de conformité (mise à jour AI Act, nouvelle version ISO 42001) déclenche une revue anticipée.

Jean-Paul Koslowski Président, 00Source SASU 17 juin 2026 *Signé électroniquement*