# Procédure de Gestion des Incidents de Données / Violations (PR-03 + REG-03)

Entreprise : OptiValue.ai  
Version : 1.0  
Date : 03/09/2025  
Auteur : Délégué à la Protection des Données (DPO)

## Introduction

Cette procédure définit le cadre opérationnel de gestion des incidents de données et des violations de données personnelles chez OptiValue.ai. Elle s’appuie sur les exigences du RGPD (articles 33 et 34), de l’ISO 27001 et des bonnes pratiques de gestion d’incidents, en intégrant les standards PR-03 (gestion des incidents) et REG-03 (registre des incidents).

## 1. Objectifs

• Détecter rapidement toute violation de données.  
• Assurer une réponse coordonnée et efficace.  
• Notifier les autorités et les personnes concernées dans les délais légaux.  
• Documenter toutes les étapes pour assurer la traçabilité et la conformité.

## 2. Gouvernance et RACI

• \*\*DPO\*\* : Supervise le processus, valide les notifications et gère les relations avec les autorités.  
• \*\*RSSI\*\* : Analyse technique des incidents et actions de remédiation.  
• \*\*Comité de Gestion de Crise\*\* : Supervision des incidents critiques et coordination inter-départements.  
• \*\*IT SecOps\*\* : Identification, containment, analyse technique détaillée.  
• \*\*Juristes\*\* : Conseil juridique et support en cas de contentieux.

## 3. Processus de Gestion des Incidents

Le processus comprend les étapes suivantes :  
1. \*\*Détection\*\* : Identification via outils SIEM, alertes SOC, ou signalement interne.  
2. \*\*Triage\*\* : Qualification de l’incident (faible, moyen, critique).  
3. \*\*Containment\*\* : Isolation des systèmes et données affectées pour limiter l'impact.  
4. \*\*Eradication\*\* : Correction des vulnérabilités identifiées.  
5. \*\*Notification\*\* : Transmission des informations pertinentes au DPO pour validation.  
6. \*\*Communication\*\* : Information des parties prenantes et, si nécessaire, des autorités sous 72h.  
7. \*\*Post-mortem\*\* : Analyse des causes racines (RCA), rapport d’incident et mise à jour des contrôles.

## 4. Notification des Violations

• \*\*Notification CNIL\*\* : Obligatoire sous 72h après détection de la violation.  
• \*\*Notification des personnes concernées\*\* : Dès lors que le risque est jugé élevé pour leurs droits et libertés.  
• \*\*Contenu de la notification\*\* : Nature de l’incident, données impactées, mesures correctives, contacts pour assistance.

## 5. REG-03 : Registre des Incidents

Tous les incidents sont enregistrés dans le registre des incidents de données (REG-03) avec les informations suivantes :

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ID | Date | Type | Système | Gravité | Notification Autorité/Clients | MTTA | MTTR | Actions |
| INC-001 | 2025-07-15 | Fuite de données client | CRM SaaS | Critique | CNIL / Clients | 2h | 12h | Patch appliqué, audits terminés |
| INC-002 | 2025-08-02 | Tentative d’accès non autorisé | Serveur Prod | Moyenne | Non | 1h | 6h | Renforcement MFA, surveillance accrue |
| INC-003 | 2025-08-18 | Suppression accidentelle de données | DB interne | Faible | Non | 30min | 3h | Restauration depuis backups |

## 6. Outils et Automatisation

• Intégration SOC / SIEM pour détection et analyse temps réel.  
• Outils EDR pour investigation et containment rapides.  
• Plateforme ComplianceHub.ai pour automatiser les notifications et mises à jour du registre.  
• IA prédictive pour identifier les signaux faibles avant incident critique.

## 7. Formation et Exercices

• Formation annuelle obligatoire sur la gestion des incidents.  
• Exercices de simulation table-top tous les trimestres.  
• Tests de restauration et reprise après sinistre (BCP/DRP).

## 8. Amélioration Continue

• Analyse post-incident systématique.  
• Mise à jour trimestrielle des procédures.  
• Intégration des retours d’audit interne et externe.  
• Benchmarks sectoriels intégrés pour aligner le dispositif sur les meilleures pratiques.

## Annexes

• Modèle de rapport d’incident.  
• Schéma de workflow de gestion des incidents.  
• RACI complet des rôles et responsabilités.  
• Exemples de scénarios de tests table-top.  
• Historique des incidents critiques et actions menées.