Procédure de gestion des incidents et des violations de données

KYCJet — GREM S.R.L. À l'appui des obligations du client au titre de l'article 33 du RGPD (notification à l'autorité de contrôle dans un délai de 72 heures) et de l'article 19 du Règlement (UE) 2022/2554, lu conjointement avec le Règlement délégué (UE) 2025/301 de la Commission (notification initiale d'un incident majeur dans un délai de 4 heures à compter de sa classification et, en tout état de cause, dans un délai de 24 heures après en avoir pris connaissance). Version du 21 septembre 2026.

1. Pourquoi nos délais sont plus courts que les vôtres

Le client doit notifier ses autorités en quelques heures, et ne peut le faire qu'avec les informations que nous lui fournissons. C'est pourquoi nos délais envers le client courent à compter du moment où nous détectons l'incident, et non du moment où nous avons tout compris.

2. Ce qu'est un incident

- **Incident lié aux TIC** : un événement qui compromet la disponibilité, l'authenticité, l'intégrité ou la confidentialité du Service ou des données qu'il traite (par exemple une indisponibilité, des erreurs dans les vérifications, un accès non autorisé, un prestataire qui ne répond pas).
- **Violation de données à caractère personnel** : un incident entraînant, même potentiellement, de manière accidentelle ou illicite, la destruction, la perte, l'altération ou la divulgation non autorisée des données des personnes vérifiées, ou l'accès non autorisé à celles-ci (article 4, point 12), du RGPD).

3. Comment nous détectons les incidents

- Alertes automatiques en cas de défaillances critiques, envoyées au canal d'astreinte.
- Surveillance externe de la disponibilité [à activer].
- Journal des accès du personnel aux dossiers et journal des appels à l'interface.
- Signalements des clients, des personnes vérifiées ou des prestataires, à **security@gremcompany.com**. L'adresse est aussi publiée dans `/.well-known/security.txt` (RFC 9116), là où celui qui trouve une faille regarde en premier. Celui qui signale de bonne foi et n'aggrave pas le dommage n'est pas poursuivi.

4. Rôles

Rôle	Qui	Tâches
Responsable de l'incident	[Nom, fonction] — suppléant : [Nom]	Classe l'incident, décide, communique avec les clients
Ingénieur d'astreinte	[Roulement]	Confine, enquête, rétablit

Rôle	Qui	Tâches
Référent protection des données	[Nom]	Évalue s'il y a violation de données et les risques qui en découlent

5. Phases et délais envers le client

Phase	Délai, à compter du moment où nous le détectons	Ce que nous faisons
Détection et confinement	Immédiatement	Nous stoppons les dommages : révocation d'identifiants, blocage de fonctions, isolement
Première communication	Dans un délai de **[2 heures]** si l'incident affecte le Service ou les données	Ce qui s'est passé, pour autant que nous le sachions, quels clients et quelles données sont concernés, ce que nous avons déjà fait, qui est la personne de contact
Notification de violation de données	Dans les meilleurs délais et, en tout état de cause, dans un délai de **[24 heures]**	Les informations visées à l'article 33, paragraphe 3, du RGPD dont nous disposons : nature de la violation, catégories et nombre approximatif de personnes concernées et d'enregistrements, conséquences probables, mesures prises ou proposées
Mise à jour intermédiaire	Dans un délai de **[48 heures]**, puis chaque fois qu'un élément significatif change	Causes, impact actualisé, état du rétablissement. Contribue au rapport intermédiaire DORA (dans un délai de 72 heures à compter de la notification initiale)
Rapport final	Dans un délai de **[20 jours]** à compter de la résolution	Cause première, impact global, mesures permanentes. Contribue au rapport final DORA (dans un délai d'un mois)

Les communications sont adressées au contact sécurité que le client renseigne dans les paramètres de son organisation (e-mail et adresse certifiée) et, pour les incidents critiques, également par téléphone. Si aucun contact n'est renseigné, nous écrivons à la personne qui a ouvert l'organisation : le renseigner incombe au client, et le tableau de bord le rappelle.

6. Ce que nous ne faisons pas

- Nous ne notifions ni l'autorité de contrôle ni les autorités du client à sa place, et nous ne contactons pas les personnes vérifiées, sauf instruction écrite du client : c'est le client qui est le responsable du traitement et l'entité soumise à la surveillance.
- Nous n'attendons pas d'avoir toutes les informations pour effectuer la première communication.

7. Après l'incident

Chaque incident, même sans conséquences, est enregistré avec sa date, sa durée, ses causes, son impact et les mesures prises. Les enseignements tirés se traduisent par des modifications du Service ou de la présente procédure. Le registre est à la disposition des clients et de leurs autorités, pour la partie qui les concerne.

8. Tests

La procédure est testée [une fois par an] au moyen d'un exercice fondé sur un scénario réaliste, ainsi qu'après chaque incident majeur.