

Procédure de notification en cas de violation de données

Ce qui compte comme violation

Tout incident de sécurité, accidentel ou malveillant, qui entraîne la destruction, la perte, l'altération ou la divulgation non autorisée de données personnelles, ou l'accès non autorisé à ces données. Exemples dans notre contexte :

- une clé API ou un secret exposé (dépôt public, poste compromis) donnant accès au bucket des résultats ;
- un bucket ou un export rendu public par erreur ;
- un compte référent compromis (mot de passe volé) ayant consulté des fiches ;
- un email d'invitation parti au mauvais destinataire avec des données d'apprenant ;
- la perte d'un export JSON téléchargé et non supprimé.

Un doute se traite comme un incident jusqu'à preuve du contraire.

Étape 1 - Détection et premières mesures (immédiat)

Points d'entrée : signalement à contact@onboardy.fr, anomalie dans les journaux des fonctions Scaleway, alerte d'un référent ou d'un apprenant.

Dès la prise de connaissance, Learnly Bloom :

1. **Coupe la voie d'accès** : révocation de la clé ou du secret compromis, remise en privé du stockage, désactivation du compte compromis, verrouillage de la fonction concernée s'il le faut. Contenir d'abord, comprendre ensuite.
2. **Figé les éléments** : horodatage de la découverte, journaux concernés, périmètre apparent (quelles clés de stockage, quelles cohortes, quelles données).
3. **Ouvre une entrée dans le registre interne des incidents** (voir plus bas), même si l'incident paraît mineur.

Étape 2 - Qualification (dans les heures qui suivent)

Trois questions, notées par écrit dans l'entrée de registre :

- **Quelles données ?** Identité seule, événements pédagogiques, empreintes de mots de passe (rappel : jamais de mot de passe en clair nulle part).
- **Quelles personnes ?** Combien d'apprenants, quelles écoles, des mineurs ?
- **Quel risque ?** Divulcation réelle ou simple exposition potentielle, durée de la fenêtre, exploitabilité.

Étape 3 · Notification aux écoles concernées (sans délai injustifié)

Pour chaque établissement dont des apprenants sont concernés :

- **Destinataire** : le DPO ou contact données désigné à l'article 12 du contrat de sous-traitance, avec copie au référent de la cohorte. Par email, doublé d'un appel téléphonique si le risque est élevé.
- **Contenu** (article 33.3 du RGPD) : nature de la violation, catégories et nombre approximatif de personnes et d'enregistrements concernés, conséquences probables, mesures prises et proposées, point de contact chez Learnly Bloom (contact@onboardy.fr).
- **Ce qu'on ne fait pas** : attendre d'avoir tout compris pour prévenir. Une première notification incomplète, complétée ensuite, vaut mieux qu'une notification parfaite hors délai. Le RGPD prévoit explicitement la fourniture d'informations par étapes.

Étape 4 · Appui à l'école (les 72 heures)

C'est l'école, responsable de traitement, qui décide de notifier la CNIL (sous 72 heures si le risque le justifie) et d'informer les personnes (si le risque est élevé, article 34). Learnly Bloom fournit sans se faire prier :

- la chronologie technique établie à l'étape 1 ;
- la liste des apprenants concernés par cohorte (extraite du stockage) ;
- la description des mesures de sécurité en place et des mesures correctives ;
- toute pièce utile au formulaire de notification CNIL.

Cas des mineurs : si l'information des personnes est requise et que des mineurs sont concernés, elle passe par l'école, qui informe aussi les représentants légaux (cohérent avec l'article 8 du DPA).

Étape 5 · Registre interne et retour d'expérience

- **Registre des incidents** (article 33.5) : chaque violation, notifiée ou non à la CNIL, y est consignée : faits, effets, mesures. C'est lui qui prouve, en cas de contrôle, que même les incidents mineurs sont suivis. Tenu dans le coffre de l'équipe, jamais dans un dépôt de code.
- **Sous quinze jours** : retour d'expérience écrit : cause racine, ce qui aurait détecté ou empêché l'incident plus tôt, actions correctives avec responsable et échéance (issue GitHub si c'est du code).

Contacts et délais, en résumé

Qui	Quoi	Quand
Learny Bloom	Contenir, figer, qualifier	Immédiat
Learny Bloom → DPO de l'école	Notification article 33.3	Sans délai injustifié après prise de connaissance
École → CNIL	Notification si risque	72 h après SA prise de connaissance
École → personnes (et représentants légaux)	Information si risque élevé	Sans délai injustifié
Learny Bloom	Registre interne + retour d'expérience	Toujours, sous 15 jours pour le REX

Learny Bloom, SASU au capital de 9 000 €, 17 rue Isaac Newton, 17000 La Rochelle, SIREN 899 835 078 · contact@onboardy.fr · onboardy.fr