



Fuite de données

Les premiers réflexes à adopter

Une fuite de données peut concerner un fichier patient envoyé au mauvais destinataire, un compte piraté, un vol d'ordinateur, un logiciel compromis ou une divulgation non autorisée. L'objectif est simple : protéger les personnes, limiter l'impact, conserver les preuves et décider rapidement s'il faut notifier la CNIL.

Urgence : les 4 réflexes qui comptent

Isoler l'accès ou le support concerné, ne pas supprimer les traces, alerter le responsable/DPO, noter précisément les faits et l'heure de découverte.

Dans les 30 premières minutes

1 Identifier ce qui a fuité

Type de données, personnes concernées, volume approximatif, origine probable : erreur humaine, piratage, perte, vol, prestataire, mauvais paramétrage.

2 Stopper sans effacer

Bloquez le compte, retirez le lien partagé, isolez le poste ou le dossier exposé. Ne supprimez pas les journaux, e-mails ou preuves utiles.

3 Alerter immédiatement

Prévenez la direction, le support informatique, le prestataire concerné et le DPO ou référent RGPD. Une fuite ne doit jamais rester isolée.

4 Documenter simplement

Notez l'heure de découverte, la personne qui constate, les systèmes touchés, les actions déjà réalisées, les captures d'écran et les messages reçus.

5 Sécuriser les accès

Changez les mots de passe depuis un appareil sain, révoquez les sessions actives, activez la MFA et vérifiez les accès à distance.

6 Préparer la décision RGPD

Évaluez vite le risque pour les patients, salariés ou partenaires : santé, identité, coordonnées, mots de passe, données financières, secret médical.

Réflexe RGPD : la question des 72 heures

Une violation de données correspond à une perte de confidentialité, d'intégrité ou de disponibilité. Si elle présente un risque pour les droits et libertés des personnes, le responsable de traitement doit notifier la CNIL dans les meilleurs délais et, si possible, sous 72 heures. Si le risque est élevé, les personnes concernées doivent aussi être informées clairement.

Contacts à compléter avant diffusion

Support informatique / prestataire : _____ Téléphone / e-mail : _____

DPO / référent RGPD : _____ Téléphone / e-mail : _____

Responsable de la structure : _____ Téléphone / e-mail : _____



La sécurité comme fondation.

Fiche gratuite fournie par Cerberis Conseil - rubrique Guides & outils

© 2026 Cerberis Conseil · Licence CC BY-NC-ND 4.0

Libre diffusion gratuite avec mention de Cerberis Conseil. Modification et reprise sur un support payant interdites.

cerberis-conseil.fr



Dans les heures qui suivent

À faire

1. Centraliser la crise

Désignez une personne pilote : technique, RGPD, communication et continuité d'activité.

2. Qualifier la violation

Confidentialité, intégrité ou disponibilité ? Erreur ponctuelle ou attaque ? Données de santé ou secret professionnel ?

3. Mesurer le risque

Type de personnes, sensibilité, volume, facilité d'identification, conséquences possibles : usurpation, discrimination, anxiété, perte de chance.

4. Tenir le registre interne

Inscrivez l'incident dans le registre des violations, même si la CNIL n'est finalement pas notifiée.

À faire aussi

1. Décider de la notification

Si un risque existe pour les personnes, préparez la notification CNIL sans attendre la fin complète de l'analyse.

2. Informer si risque élevé

Message simple : ce qui s'est passé, données concernées, conséquences possibles, mesures prises, contact DPO.

3. Corriger la cause

Mots de passe, MFA, droits d'accès, faille logiciel, mauvais partage, erreur de procédure, contrat prestataire.

4. Rassurer sans minimiser

Communiquez de façon factuelle. Ne promettez pas que tout est réglé tant que l'analyse n'est pas terminée.

Pourquoi un DPO aide grandement

Le DPO apporte une méthode : qualification de la violation, analyse du risque, décision de notification, relation avec la CNIL, rédaction des messages aux personnes et traçabilité. Pour un cabinet de santé, il sécurise les décisions et évite les oublis dans un moment de stress.

Points de vigilance 2026

RGPD : notification CNIL sous 72 h si risque, information des personnes si risque élevé, documentation de toutes les violations. Santé : vigilance renforcée sur les données de santé, HDS, MSSanté et secret professionnel. Cyber : MFA, sauvegardes testées, gestion des accès et préparation de crise sont des attendus de base. NIS2 peut concerner certaines structures ou prestataires de santé : vérifiez votre périmètre.

Les erreurs à éviter

Attendre pour prévenir le DPO, effacer les preuves, sous-estimer une fuite, informer les patients sans message validé, oublier le sous-traitant ou ne pas conserver la décision de ne pas notifier.

Préparer la structure avant une fuite

Cartographie	Savoir où sont les données : logiciel métier, cloud, messagerie, sauvegardes, prestataires.
Accès et traces	Limiter les droits, activer la MFA, supprimer les anciens comptes et conserver les journaux utiles.
Sous-traitants	Identifier les contacts incident et vérifier les clauses de notification rapide.
Procédure	Tester au moins une fois par an : qui décide, qui notifie, qui communique, quoi conserver.

Pour aller plus loin

Sources utiles : CNIL - violations de données personnelles et téléservice de notification ; Cybermalveillance.gouv.fr - assistance aux victimes ; ANSSI - NIS2 et bonnes pratiques de gestion des risques cyber.