

Mentor Note

Bonjour ! On sait que le terme "Juridique" ou "RGPD" peut faire peur. Détendez-vous. Ce que vous allez apprendre aujourd'hui est avant tout une question de bon sens et de logique. Nous commençons là pour vous donner les clés de votre future réussite en entreprise.

Fuite de données : Pas de panique, vous avez le contrôle.

Guide pratique de gestion de crise
pour futurs professionnels.

- ✓ Une fuite de données peut arriver à n'importe qui (PME, Hôpital, Géant du web).
- ✓ Ce qui fera de vous un bon professionnel, ce n'est pas d'éviter l'inévitable, mais de savoir comment réagir.
- ✓ Objectif de ce module : Maîtriser la procédure 'Réflexe' immédiate.



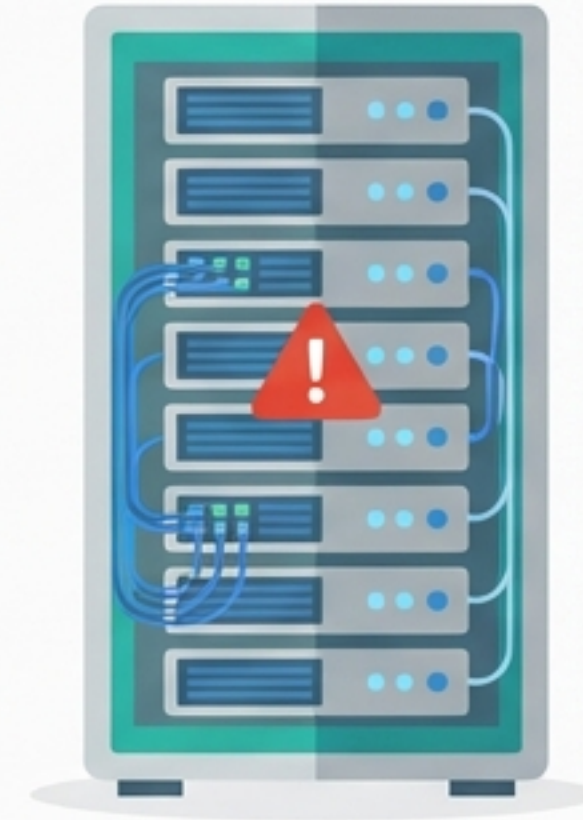
Imaginez votre système d'information comme une maison.

La Maison



Réflexe : Je constate l'effraction, je sécurise la porte, je regarde ce qui a disparu, j'appelle la police.

L'Entreprise



Réflexe : Je détecte la fuite, je coupe l'accès, j'évalue les données volées, je notifie la CNIL.

*Mentor Note: Vous voyez ? Si vous savez gérer un cambriolage, vous comprenez déjà la logique du RGPD.
C'est exactement le même processus.*

La Chronologie de Crise : Votre feuille de route.



En cas d'incident, la réactivité est votre meilleure arme.
Ne cherchez pas à tout résoudre d'un coup. Suivez les étapes une par une.

Étapes 1 & 2 : Arrêter l'hémorragie

Détecter et Contenir

L'Analogie

Comme on met une planche sur une fenêtre brisée, il faut isoler le problème informatique.



L'Action

Couper les accès compromis, isoler le serveur infecté, changer les mots de passe administrateurs.



Cas Concret : PME App Mobile



Une PME voit sa base client volée. Réflexe immédiat ? Isoler le serveur compromis pour empêcher le pirate de revenir ou de prendre plus de données.

*Ne perdez pas de temps à chercher "qui" a fait ça.
Votre priorité absolue est de fermer la porte.*

Étape 3 : L'enquête interne (Évaluer).

- Avant d'alerter, il faut comprendre l'impact.
- Quelles données ? (Noms, adresses, données bancaires, données de santé ?)
- Quel **volume** ? (10 clients ou 100 000 ?)
- Quel **risque** pour les gens ? (Usurpation d'identité, perte financière ?)

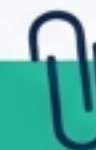


Exemple E-commerce : Si un site perd des adresses postales, c'est grave. S'il perd des données bancaires, c'est critique.

Étape 4 : La Règle d'Or des 72 Heures.

Article 33 du RGPD

La CNIL doit être notifiée dans les 72 heures maximum si la violation présente un risque pour les droits des personnes.



*C'est souvent l'étape qui fait peur. On se dit : "Si je le dis à la CNIL, je vais me faire punir". C'est l'inverse !
Cacher la fuite est la vraie faute grave. La transparence est votre bouclier.*

L'erreur de débutant à éviter absolument.

Le Novice

J'attends d'avoir tous les détails de l'enquête pour appeler la CNIL. Je ne veux pas les déranger pour rien.

Résultat : Délai 72h dépassé = Sanctions.

Le Pro

Je signale l'incident dans les 72h, même si je n'ai que des informations partielles. Je compléterai mon dossier plus tard.

Résultat : Conformité et bonne foi.

N'attendez pas la perfection. La réactivité prime sur l'exhaustivité immédiate.

Étape 5 : Faut-il prévenir les clients ?

Pas systématique, mais obligatoire si le risque est **ÉLEVÉ** pour leur vie privée. Pourquoi ? Pour qu'ils puissent se protéger (changer de mot de passe, surveiller leurs comptes bancaires).



Scénario : Un piratage vole les mots de passe de 10 000 clients.



L'entreprise **DOIT les prévenir immédiatement** pour qu'ils changent leurs codes.



Scénario PME : Des emails ont fuité.



Prévenez vos clients d'être vigilants face au Phishing.

Étape 6 : Réparer et Documenter.

Corriger



Appliquer le correctif de sécurité pour que ça ne recommence plus demain.

Documenter



Tenir un registre des violations.

Mentor Note : Un bon manager note tout. Même les incidents mineurs qui n'ont pas été notifiés à la CNIL doivent être inscrits dans votre registre interne. C'est la preuve de votre sérieux en cas de contrôle.

Étude de Cas : Quand les géants trébuchent.



Sujet : British Airways (Juin 2018)

Histoire : Fuite massive de données de cartes de crédit (centaines de milliers de clients).

Conséquence : Sanction lourde par l'ICO (équivalent britannique de la CNIL).

Mentor Note : Même les plus grandes entreprises peuvent échouer si les mesures de sécurité ne sont pas adéquates. Votre rigueur protège votre entreprise, quelle que soit sa taille.

Au-delà de l'amende : L'impact humain.



Sujet : Hôpital français (2022)

Histoire : Cyberattaque majeure. Dossiers patients inaccessibles, plannings du personnel bloqués.

Impact : Transfert de patients, notification urgente à la CNIL pour impact significatif sur la santé.

Mentor Note : Ici, on ne parle pas juste de données, mais de vies humaines. C'est pour cela que votre rôle dans la protection des données est si noble et important.

À vous de jouer : Que feriez-vous ?

Scénario :

Vous gérez un site e-commerce. Une intrusion dévoile les noms et adresses de vos clients. Aucune donnée bancaire n'est touchée.



C'est moins grave, donc on ne fait rien ?

Faux ! Même sans données sensibles, il y a un risque (usurpation d'identité). Vous devez évaluer ce risque. Si le risque existe pour les droits et libertés, vous devez notifier la CNIL.

Ne sous-estimez jamais une fuite, même 'petite'.

Votre Allié : Le DPO.

- Dans ce processus, vous n'êtes pas seul.
- Le Délégué à la Protection des Données (DPO) est votre pilote. C'est lui qui orchestre la notification à la CNIL et la communication.
- Votre rôle : Lui remonter l'information immédiatement.



L'essentiel à retenir pour l'examen (et la vie pro)

Check-list de Révision



1. **Réflexe** : Fuite = Cambriolage (Sécuriser d'abord).



2. **Délai** : 72h max pour la CNIL (Même avec infos partielles).



3. **Transparence** : Prévenir les victimes si risque élevé.



4. **Attitude** : Ne jamais cacher l'incident.

*Note du Mentor :
Pensez
"Transparence +
Action Rapide".
C'est la clé !*

"En cas de violation, la CNIL doit être notifiée dans les 72 heures."

Vous êtes prêts.



Bravo ! Vous maîtrisez maintenant l'un des aspects les plus délicats du droit numérique. Cette compétence est très recherchée en entreprise. Gardez cette logique en tête, restez calmes, et vous saurez gérer n'importe quelle crise.

Bonne chance pour votre examen !