L’évaluation du risque d’une violation de données en 5 étapes

L’appréciation du niveau de risque engendré par une violation de données personnelles doit être réalisée au cas par cas.

Elle dépendra notamment des critères suivants :

- la nature des données (sensibles, biométriques, financières, etc…);
- le nombre et les catégories de personnes concernées, notamment si celles-ci sont des personnes vulnérables (personnes porteuses de handicap, mineurs, salariés, etc.) ;
- la facilité d’identifier ces personnes concernées suite à la violation ;
- les mesures de sécurité existantes (chiffrement, pseudonymisation, accès restreint, etc.) ;
- la capacité à détecter et réagir rapidement à l’incident.

Aussi, pour évaluer le niveau de risque d’une violation de données, l’APDP vous propose de suivre les 5 étapes suivantes :

1. Vérification de la nécessité d’évaluer le risque

- L’incident concerne-t-il des **données à caractère personnel** ?
- Existe-t-il un **impact potentiel sur les droits et libertés** des personnes concernées ?

Si la réponse est **oui** à ces deux questions, **l’évaluation du risque est obligatoire.**

2. Évaluation de la gravité des conséquences pour les personnes concernées

Cette étape mesure l’impact **possible** sur les personnes concernées :

NIVEAU	CONSEQUENCES POSSIBLES
Faible	Gêne légère, peu d’impact sur la vie privée.
Moyen	Risque réel mais limité : perte financière mineure, discrimination.
Elevé	Dommages sérieux ou irréversibles : réputation, santé, usurpation d’identité.

3. Évaluation de la vraisemblance de réalisation d'un dommage

Cette étape estime la **probabilité de réalisation** d'un dommage :

NIVEAU	INDICATEURS
Faible	Données protégées, accès limité, incident isolé. Mesures correctives efficaces.
Moyen	Défenses partielles, imparfaites. Risque plausible que l'incident se reproduise si aucune action préventive n'est prise.
Elevé	Données exposées, faille avérée. L'incident est susceptible de se reproduire presque immédiatement si aucune mesure corrective/technique n'est prise dans les plus brefs délais.

4. Identification du niveau de risque via une matrice croisée (gravité × vraisemblance)

Une fois l'évaluation de la vraisemblance et celle de la gravité réalisées, ces éléments peuvent être reportés dans la matrice suivante (l'axe vertical représentant la gravité et l'axe horizontal la vraisemblance) :

		VRAISEMBLANCE		
		Faible	Moyen	Elevé
GRAVITE	Faible	Risque faible	Risque moyen*	Risque moyen
	Moyen	Risque moyen*	Risque moyen	Risque élevé
	Elevé	Risque moyen	Risque élevé	Risque élevé

***Risque moyen pouvant être réduit en risque faible si les mesures préventives adéquates ont été prises

5. Conséquences de l'évaluation

Maintenant que le risque est identifié, le responsable du traitement peut désormais prendre les mesures techniques et organisationnelles pour limiter l'impact de la violation mais également pour éviter que celle-ci ne se reproduise.

[Pour plus d'information, voir **Les principales violations de données : obligations et conseils pour les prévenir]**

Par ailleurs, en vertu de l'article 32 de la Loi n° 1.565 du 3 décembre 2024, le responsable du traitement doit notifier à l'APDP toute violation des données **susceptible** d'engendrer un **risque pour les droits et libertés des personnes concernées.**

Une **communication aux personnes concernées** peut également être exigée en fonction du niveau de gravité

Niveau de risque	Action(s) obligatoire(s)
Aucun risque	- Consignation dans le registre des violations de données
Risque faible	- Consignation dans le registre des violations de données - Notification à l'APDP dans les 72 heures
Risque moyen	- Consignation dans le registre des violations de données - Notification à l'APDP dans les 72 heures
Risque élevé	- Consignation dans le registre des violations de données - Notification à l'APDP dans les 72 heures - Communication aux personnes concernées

[Pour plus d'information, voir **Les notifications de violations de données personnelles**]