

Comment réagir face à une violation de données ?



*Découvrez les bons
réflexes à adopter
pour renforcer
votre stratégie
de cybersécurité*

Lire la suite

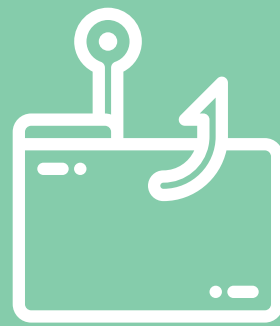


Qu'est-ce qu'une violation de données ?

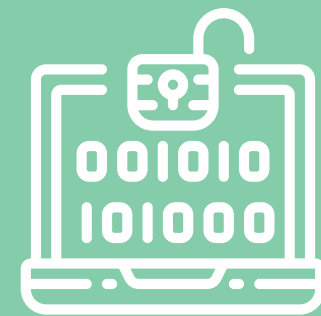
Une violation de données se manifeste par **des incidents** tels que :



L'accès non autorisé



Le vol de données



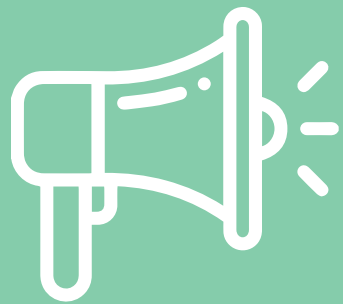
La fuite de données involontaires

Ces attaques proviennent de sources variées comme **le piratage, les ransomwares** ou **le phishing**.

Elles ciblent **une diversité de données**, de l'information personnelle aux secrets industriels.

Quels sont les impacts juridiques ?

Les entreprises sont tenues de respecter certaines **obligations légales strictes**, prévues dans le RGPD :



- Notifier à la CNIL toute violation de données **à caractère personnel** dans les 72h
- **Communiquer la violation à la personne concernée** dans les meilleurs délais (en cas de risque élevé pour les droits et libertés de la personne)

! À noter

La CNIL préconise aux entreprises de tenir un registre des violations de données (nature de la violation, personnes concernées, mesures prises, etc.)

Quels sont les impacts économiques?

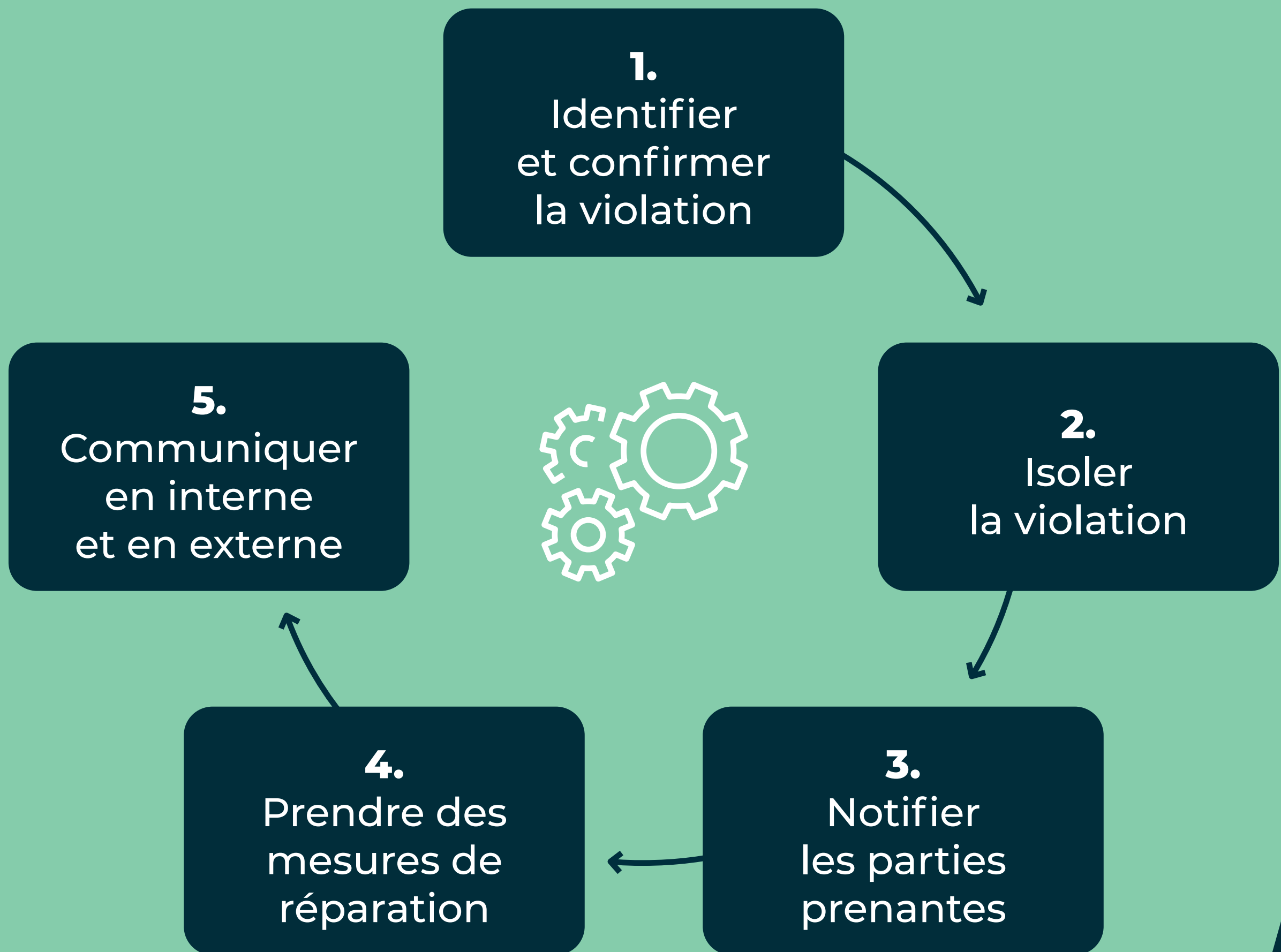


Le non-respect des obligations en cybersécurité peut entraîner **des sanctions administratives sévères** (amende pouvant atteindre **20M€** et **4% du CA mondial annuel**).



Les entreprises doivent aussi faire face à **des coûts directs et indirects** : remédiation technique, indemnisations aux parties lésées, perte de clientèle, etc.

Les 5 étapes à suivre en cas de violation de données



Comment prévenir les violations de données ?

- **Mettre en place une stratégie de cybersécurité**

Pour établir **des directives claires et cohérentes** pour la gestion, la protection et l'accès aux données au sein de votre organisation

- **Sensibiliser vos collaborateurs**

Pour prévenir les risques cyber > le maillon le plus faible de la cybersécurité est généralement **l'humain**

- **Evaluer les risques cyber**

Pour adapter **les mesures de cybersécurité** à mettre en place dans votre entreprise (analyse de vulnérabilité, identification et classification des données...)

- **Héberger et sauvegarder les données**

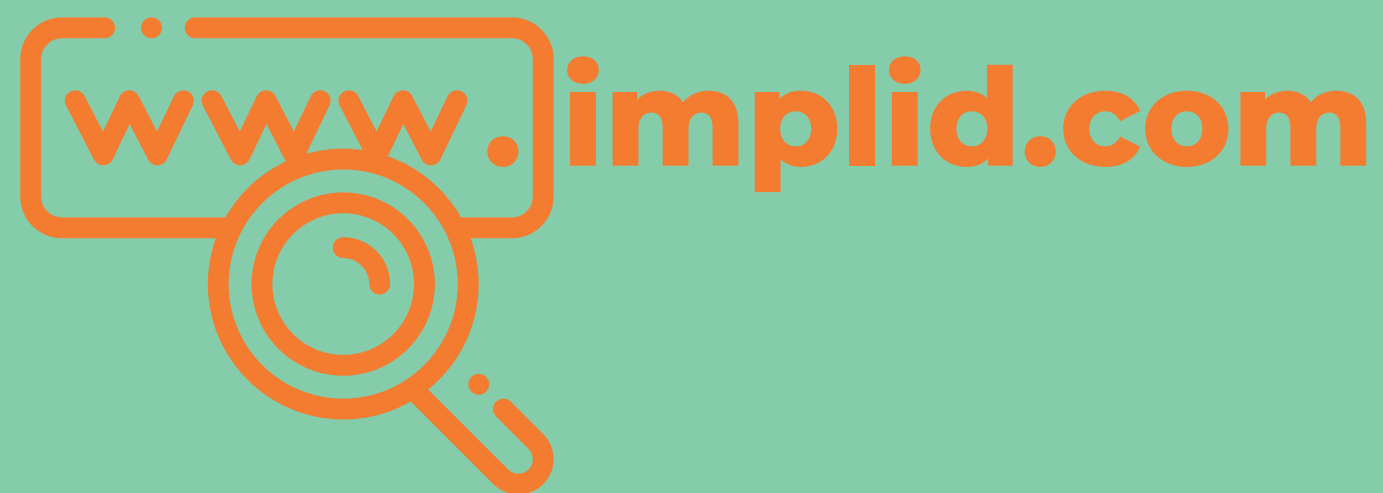
Pour limiter **les conséquences de la violation** et permettre **la récupération des données**



/ Pour en savoir plus...

Vous souhaitez en savoir plus
sur ***les violations de données ?***

Découvrez notre article sur :



implid