Juillet 2025

Les principales violations de données : obligations et conseils pour les prévenir

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

Selon l'article 32 de la loi n° 1.565 du 3 décembre 2024, une violation de données personnelles est un **incident de sécurité** (accidentel ou illicite) entraînant :

- la **destruction**, la **perte**, ou l'**altération** de données personnelles ;
- la **divulgation non autorisée** ou l'**accès non autorisé** à ces données.

Toute violation de données n'a pas à être notifiée à l'APDP.

L'article 32 de la Loi n° 1.565 du 3 décembre 2024 dispose en effet que le responsable du traitement doit notifier à l'APDP **toute violation dont il a connaissance et qui est susceptible** d'engendrer **un risque pour les droits et libertés des personnes concernées.**

Conformément aux trois principes de sécurité classiques, ces violations peuvent être classées en trois catégories :

- la « ***violation de la confidentialité*** » : survient en cas de divulgation ou d'accès non autorisé ou accidentel à des données personnelles ;
- la « ***violation de l'intégrité*** » : se produit en cas d'altération non autorisée ou accidentelle de données personnelles ;
- a « ***violation de la disponibilité*** » : correspond à la perte ou destruction accidentelle ou malveillante de données personnelles.

CONFIDENTALITE	INTEGRITE	DISPONIBILITE
Seules les personnes habilitées doivent avoir accès aux données	Les données ne doivent pas être altérées durant leur collecte, exploitation, transfert, etc.	L'accès aux données personnelles doit être garanti tant en termes de délai que de qualité

Par ailleurs, lorsque la violation est **susceptible** d'engendrer un **risque élevé pour les droits et libertés** d'une personne physique, le responsable du traitement doit également **communiquer** cette violation à la personne concernée **dans les meilleurs délais.**

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

L'appréciation du risque élevé se fait à la lumière d'un incident particulier et repose sur les conséquences qui en découlent. Elle doit se faire sur la base de critères objectifs en lien avec chacune des personnes dont les données ont été concernées par la violation, en fonction de leur situation spécifique. La détermination du niveau de risque n'est pas figée au jour de la violation, mais doit faire l'objet d'une réévaluation en cas d'évolution des informations dont dispose le responsable du traitement.

Cette fiche pratique vous propose ainsi plusieurs scénarios pour vous aider à mieux comprendre vos principales obligations en fonction des violations rencontrées et nos conseils pour éviter que celles-ci se produisent ou ne se reproduisent.

Quels sont les éléments à prendre en compte pour évaluer les risques d'une violation de données ?

- **le type de violation** (confidentialité, intégrité et/ou disponibilité des données)
- **la sensibilité des données** (données de santé, données financières infractions pénales, etc.)
- **le volume des données** et/ou des **personnes concernées**
- **la ou les catégorie(s) de personnes concernées** (enfants, salariés, personnes porteuses d'un handicap, personnes âgées, etc.)
- **la facilité d'identifier les personnes touchées par la violation** (données chiffrées ou non)
- **le domaine d'activité du responsable du traitement** (domaine médical, établissement bancaire, etc.)
- les **mesures de sécurité existantes**
- **les conséquences possibles pour les personnes** (usurpation d'identité, fraude, atteinte à la réputation, etc.)

[Pour plus d'information, voir **L'évaluation du risque d'une violation de données en 5 étapes**]

Erreur d'envoi de courrier ou d'e-mail

Une erreur d'envoi d'un courrier postal ou d'un e-mail peut être le résultat d'une inattention ou d'un bug informatique. Dans tous les cas, une telle erreur peut conduire à une violation de données personnelles, *a fortiori* lorsque le message contient des données confidentielles.

1er scénario : Courrier postal ou e-mail ne comprenant aucune donnée sensible ou confidentielle envoyé par erreur à un mauvais destinataire

Quel est l'impact de la violation ?

Violation de la confidentialité car une personne non habilitée à y avoir accès se retrouve en possession des données personnelles d'une ou d'autres personne(s) physique(s).

L'APDP doit-elle être notifiée ?

Oui si ce courrier/e-mail contient des données privées, non accessibles au public (adresse, date de naissance par exemple) dont la divulgation à des tiers non habilités peut entrainer un risque pour les droits et libertés des personnes concernées. Il ne peut en effet pas être exclu que la personne ayant reçu le courrier/l'e-mail par erreur en fasse usage (par exemple à des fins de démarchage commercial).

Non si le courrier/e-mail envoyé par erreur ne contient aucune donnée dont l'utilisation pourrait avoir des effets négatifs pour les personnes concernées (par exemple des données personnelles connues du grand public telles que les informations relatives à des politiciens ou figurant sur des annuaires officiels).

Les personnes concernées doivent-elles être informées ?

Cela dépendra de la **gravité des conséquences** pour les personnes concernées, en particulier de **la nature** et/ou du **volume** des données divulguées par erreur.

2ème scénario : Courrier postal ou e-mail comprenant des données sensibles et/ou confidentielles envoyé par erreur à un mauvais destinataire

Quel est l'impact de la violation ?

Violation de la confidentialité car une personne non autorisée à y avoir accès se retrouve en possession des données personnelles d'une ou d'autres personne(s) physique(s).

L'APDP doit-elle être notifiée ?

Oui. La nature même des données (**sensibles et/ou confidentielles**) est susceptible d'entraîner un risque pour les personnes concernées.

Les personnes concernées doivent-elles être informées ?

Oui en principe. Le risque pour les personnes concernées peut être considéré comme **élevé** car même si le responsable du traitement, après s'être rendu compte de l'erreur, demande aux destinataires du courrier/de l'e-mail de ne pas en tenir en compte et de le supprimer immédiatement, il peut dans certains cas ne pas être certain que cela ait effectivement été fait, et que le fichier n'ait pas été intercepté par une tierce personne.

Mesures organisationnelles et techniques pour éviter qu'une telle violation ne se (re)produise

- Etablir des règles précises en interne pour l'envoi de courriers/e-mails
- Former le personnel sur la manière d'envoyer des lettres/e-mails
- Vérifier les destinataires des courriers/e-mails avant d'envoyer des données personnelles
- Limiter le nombre des destinataires d'e-mails contenant des données personnelles
- Lorsqu'un e-mail est envoyé à un grand nombre de personnes, opter pour **«** *Cci* **»** (copie carbone invisible) afin de masquer à chacun des destinataires la liste des autres destinataires de cet e-mail
- Ne pas envoyer de données sensibles (données médicales par exemple) ou confidentielles (données bancaires par exemple) mais utiliser des moyens de communication sécurisés et chiffrés (e-mails sécurisés ou coffres numériques par exemple)
- Appliquer le principe des 4 yeux pour l'envoi de données sensibles ou confidentielles en attribuant chacune des étapes de vérification à une personne différente
- Privilégier l'adressage automatique plutôt que manuel, avec des données extraites d'une base de données disponible et actualisée
- Appliquer le délai de temporisation qui permet par exemple de supprimer/éditer un message dans un certain délai après l'avoir envoyé
- Désactiver la saisie semi-automatique lors de la saisie d'adresses électroniques
- (…)

Exfiltration par un employé de données d'une entreprise

Toutes les attaques ne proviennent pas de menaces externes. Les menaces internes sont en effet fréquentes parmi lesquelles le vol de données par des employés représente un risque particulièrement compliqué à prévenir.

Quel est l'impact de la violation ?

Le plus souvent il s'agit d'une **violation de la confidentialité** car le salarié souhaite uniquement copier des données appartenant à son entreprise en vue de les utiliser ultérieurement pour son propre profit.

L'APDP doit-elle être notifiée ?

Oui. Même si les intentions du salarié dont s'agit sont inconnues et que les données concernées ne sont pas sensibles ou confidentielles, le responsable du traitement ne peut considérer que le risque pour les personnes concernées est négligeable.

Les personnes concernées doivent-elles être informées ?

Dans certains cas, oui. En effet, en fonction de la nature des données copiées, les conséquences de la violation peuvent dans le meilleur des cas se limiter à de la sollicitation commerciale non désirée mais dans d'autres cas, ladite violation peut conduire à des risques élevés pour les personnes concernées (utilisation frauduleuse des données par exemple).

Mesures organisationnelles et techniques pour éviter qu'une telle violation ne se (re)produise

- Définir différents profils d'habilitation (basés sur le principe du « *moindre privilège* ») en fonction des rôles et responsabilités des personnes ayant accès aux informations
- Contraindre l'utilisateur à s'authentifier lorsqu'il accède à des données personnelles sensibles
- Désactiver puis supprimer le compte d'un utilisateur dès que celui-ci quitte l'entreprise
- Revoir régulièrement le système des habilitations (gestion des accès obsolètes)
- Régler le verrouillage automatique de tous les ordinateurs après un certain temps d'inactivité
- Rédiger une charte informatique à destination de tous les utilisateurs du Système d'Information (employés, stagiaires, prestataires, etc.), détaillant les bonnes pratiques et les obligations en matière de sécurité des données
- Organiser des formations/présentations régulières pour sensibiliser les employés à la sécurité des données et à l'utilisation des systèmes d'information
- Effectuer des audits périodiques des privilèges d'accès pour garantir leur conformité avec la ou les politique(s) de sécurité de l'organisme
- (…)

Perte ou vol d'un appareil

En raison d'une mobilité accrue, les appareils professionnels nomades – et les données qui y sont stockées – sont davantage susceptibles d'être volés ou perdus, ce qui peut avoir de multiples conséquences, dont certaines particulièrement lourdes, si des mesures techniques et organisationnelles n'ont pas été mises en place au préalable pour prévenir ces risques.

1er scénario : Données chiffrées et sauvegardées

Quel est l'impact de la violation ? (Aucun, sauf si la clé est compromise)

Grâce aux sauvegardes effectuées, les données restent disponibles. Il n'y a donc **pas de violation de la disponibilité.**

Par ailleurs, dès lors que la clé de déchiffrement n'a pas été divulguée ou volée, il n'y a **ni violation de la confidentialité des données, ni violation de leur intégrité** car les données étant chiffrées, elles ne sont pas accessibles par un tiers et ne peuvent être altérées.

En revanche, si la clé est également compromise, il y aura violation de la confidentialité des données, et potentiellement violation de leur intégrité si la personne en leur possession les altère de quelque manière que ce soit.

L'APDP doit-elle être notifiée ?

Non. Dès lors que les données étaient protégées par un algorithme de chiffrement à l'état de l'art (attention toutefois à ce que la clé de chiffrement ne soit pas compromise) et que les données sont rapidement restaurées grâce aux sauvegardes effectuées, il est peu probable que cette violation entraîne un risque pour les droits et libertés des personnes concernées.

Les personnes concernées doivent-elles être informées ?

Non. En l'**absence de risque élevé** pour les droits et libertés des personnes concernées, celles-ci n'ont pas à être informées de cette violation. Là encore, la réponse sera différente si la clé a été compromise. En effet, en fonction de la **nature** , de la **catégorie** ou du **volume** des données concernées par la violation ainsi que de la **gravité des conséquences** pour les personnes concernées, une information de ces dernières pourrait être nécessaire.

2ème scénario : Données chiffrées mais non sauvegardées

Quel est l'impact de la violation ?

En l'absence de toute sauvegarde, les données ne sont plus disponibles. Il y a donc **violation de la disponibilité.**

En revanche, il n'y a **ni violation de la confidentialité des données, ni violation de leur intégrité** car les données étant chiffrées, elles ne sont pas accessibles par un tiers et ne peuvent être altérées. Toutefois, si la clé est également compromise, il y aura violation de la confidentialité des données, et potentiellement violation de leur intégrité si la personne en leur possession les altère de quelque manière que ce soit.

L'APDP doit-elle être notifiée ?

Oui, très probablement car en fonction des données et des personnes concernées, leur absence de disponibilité pourrait entrainer un risque pour les droits et libertés des personnes concernées (disparition d'un dossier médical par exemple)

Les personnes concernées doivent-elles être informées ?

Cela dépendra de **l'évaluation de la nature** ou du **volume** des données rendues indisponibles ainsi que de la **gravité des conséquences** pour les personnes concernées.

3ème scénario : Données non chiffrées

Quel est l'impact de la violation ?

Violation de la confidentialité car les données n'étant pas protégées elles sont accessibles par toute personne non autorisée à y avoir accès se retrouvant en possession de l'appareil.

Par ailleurs, cette personne pourrait volontairement ou non modifier ces données, ce qui constituerait une **violation de leur intégrité**.

Enfin, **s'il n'existe aucune sauvegarde des données**, la violation peut également constituer une **violation de la disponibilité** de ces données.

L'APDP doit-elle être notifiée ?

Oui. L'absence de mesures élémentaires de protection (absence de chiffrement des données stockées sur l'appareil) entraîne un risque pour les personnes concernées affectées par la violation. Ce risque peut être d'autant plus important si les personnes concernées peuvent être facilement identifiées, si elles sont vulnérables, que leur nombre est important et/ou que les données concernées sont sensibles

Les personnes concernées doivent-elles être informées ?

Oui, le risque élevé est très probable. Là encore, le responsable du traitement devra prendre en compte la **nature**, **les catégories** ou le **volume** des données concernées par la violation ainsi que la **gravité des conséquences** pour les personnes concernées.

Mesures organisationnelles et techniques pour éviter qu'une telle violation ne se (re)produise

- Chiffrer tous les appareils mobiles
- Mettre en place pour chaque appareil des mots de passe robustes (comprenant un minimum de 12 caractères, des lettres majuscules et minuscules, des chiffres et des caractères spéciaux)
- Utiliser des solutions de gestion des appareils mobiles (MDM)
- Utiliser des filtres anti-reflets
- Si possible, sauvegarder les données personnelles non sur l'appareil mobile mais sur un serveur central
- Utiliser un VPN sécurisé
- Sensibiliser les employés aux risques de perte ou de vol des appareils mobiles
- (…)

Rançongiciel (ou ransomware en anglais)

Considéré aujourd'hui comme une des cybermenaces les plus plébiscitées par les pirates informatiques, le rançongiciel est un logiciel malveillant qui prend en otage les données contenues dans un système informatique puisqu'il chiffre et bloque les fichiers contenus sur serveurs (système d'information) et n'envoie la clé permettant le déchiffrement que lorsque (théoriquement) l'utilisateur a payé une rançon.

1er scénario : Système d'Information (SI) protégé (chiffrement + sauvegarde)

Dans ce scénario, le responsable du traitement utilise le chiffrement au repos qui permet de s'assurer que lorsque des données stockées dans le SI tombent entre les mains d'un pirate informatique, ledit pirate ne peut pas les lire sans avoir accès aux clés de chiffrement.

Par ailleurs, toutes les données étaient sauvegardées.

Quel est l'impact de la violation ?

Aucun risque réel. En effet, il n'y a pas **ni violation de la confidentialité des données, ni violation de leur intégrité** car les données étant chiffrées, elles ne sont pas accessibles par le pirate informatique sans les clés de déchiffrement et ne peuvent donc être altérées.

Par ailleurs, il n'y **a pas de violation de la disponibilité des données** puisque même si le pirate a chiffré les données, celles-ci sont rapidement restaurées grâce aux sauvegardes effectuées.

L'APDP doit-elle être notifiée ?

Non. Dès lors que les données étaient protégées grâce au chiffrement au repos contre tout accès non autorisé et que les données ont été rapidement restaurées grâce aux sauvegardes effectuées, il est peu probable que cette violation entraîne un risque pour les droits et libertés des personnes concernées.

Les personnes concernées doivent-elles être informées ?

Non. En l'**absence de risque élevé** pour les droits et libertés des personnes concernées, celles-ci n'ont pas à être informées de cette violation.

2ème scénario : Système d'Information (SI) non protégé

Dans ce scénario, les données n'étaient ni chiffrées au repos ni sauvegardées.

Quel est l'impact de la violation ?

Violation de la disponibilité et potentiellement de la confidentialité et de l'intégrité.

En effet, en l'absence de sauvegardes effectuées par le responsable du traitement, il y a **violation de la disponibilité des données**. Celles-ci ayant été chiffrées par le pirate, elles ne pourront pas être restaurées si le responsable du traitement n'a pas de copie papier ou sur d'autre(s) support(s).

Par ailleurs, en l'absence de chiffrement au repos des données stockées, le responsable du traitement devra mener un examen approfondi afin de déterminer si le pirate a pu avoir accès auxdites données, ce qui conduirait également à une **violation de leur confidentialité**.

Enfin, s'il y a eu extraction des données, il est également possible qu'il y ait eu une **violation de leur intégrité** si elles ont été altérées durant leur collecte, exploitation, transfert, etc.

L'APDP doit-elle être notifiée ?

Oui, très probablement. L'absence de mesures élémentaires de protection (non chiffrement au repos des données stockées et absence de sauvegardes régulières) entraîne un risque pour les personnes concernées affectées par la violation. Ce risque peut être d'autant plus important **si ces personnes peuvent être facilement identifiées, si elles sont vulnérables, que leur nombre est important et/ou que les données concernées sont sensibles.**

Les personnes concernées doivent-elles être informées ?

Oui, très probablement. Là encore, le responsable du traitement devra prendre en compte la **nature**, le **caractère sensible** et/ou le **volume** des données concernées par la violation ainsi que la **gravité des conséquences** pour les personnes concernées.

En effet, en l'absence de sauvegarde, les données peuvent être perdues et devront être à nouveau collectées, à moins qu'une autre source ne soit disponible (fichier papier par exemple). Cela peut avoir des conséquences particulièrement dramatiques pour les personnes concernées lorsque les données sont par exemple des données de santé.

Par ailleurs, certaines données, en fonction de leur nature (documents d'identité ou données financière par exemple) peuvent être utilisées à des fins d'usurpation d'identité ou de fraude.

Mesures organisationnelles et techniques pour éviter qu'une telle violation ne se (re)produise

- Limiter le nombre de tentatives d'accès à un compte
- Installer un pare-feu et un système de détection et de prévention des intrusions appropriés, actualisés, efficaces et intégrés
- Utiliser des antivirus régulièrement mis à jour
- Installer sans délai les mises à jour critiques (correctifs de sécurité)
- Chiffrer au repos les données stockées sur tous supports et systèmes
- Effectuer des audits réguliers des systèmes d'informations pour vérifier la conformité aux politiques de sécurité et identifier les éventuelles vulnérabilités
- Instaurer des procédures de sauvegardes régulières des données pour prévenir les pertes de données en cas d'attaques
- Former le personnel aux méthodes de reconnaissance et de prévention des attaques informatiques
- Effectuer des tests de vulnérabilité et d'intrusion de façon périodique
- (…)

Pour conclure : Quelques mesures préventives recommandées

- formation du personnel
- vérification des destinataires avant envoi
- utilisation de moyens de communication sécurisés
- chiffrement des appareils et des données
- sauvegardes régulières
- authentification forte
- surveillance des accès et des flux
- mise à jour des logiciels et antivirus
- application du principe du moindre privilège

[Pour plus d'information, voir **Comment gérer une violation de données ?**]