Juillet 2025

Les notifications de violations de données personnelles

La Loi n° 1.565 du 3 décembre 2024 introduit une nouvelle obligation à la charge du responsable du traitement : la notification de **toute violation des données à caractère personnel dont il a connaissance** dès lors que celle-ci est **susceptible** d'engendrer un **risque pour les droits et libertés des personnes concernées.**

Cette notification se fait **obligatoirement** auprès de **l'APDP** afin d'assurer la préservation des droits et libertés des personnes concernées par la violation.

La notification peut également être accompagnée, dans certains cas, d'une **communication** auprès des **personnes concernées par cette violation.**

Une violation de données est un incident de sécurité mais tout incident ne constitue pas une violation de données.

Aussi, il est important de comprendre au préalable ce que la Loi entend par violation de données avant de déterminer si une notification de l'incident est nécessaire et, pour les cas les plus graves, si une communication aux personnes concernées doit être effectuée.

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

Une violation de données est un incident de sécurité, survenu de manière accidentelle ou illicite, qui affecte l'intégrité, la confidentialité ou la disponibilité des données personnelles traitées par un responsable du traitement.

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.

Exemples :

- le vol de l'ordinateur portable professionnel d'un avocat contenant les dossiers de ses clients
- l'envoi par erreur d'un e-mail contenant des données personnelles à de mauvais destinataires
- la publication en ligne des données personnelles d'une entreprise après un piratage informatique
- la récupération par un tiers non autorisé de données personnelles figurant sur des documents jetés à la poubelle

La « ***violation de l'intégrité*** » : se produit en cas d'altération non autorisée ou accidentelle de données personnelles.

Exemples :

- un tiers non autorisé accède à un fichier et en modifie/supprime le contenu
- un employé saisit par inadvertance (erreur humaine lors de la saisie) des informations incorrectes dans une base de données (exemples : mauvaise date de naissance ou numéro de sécurité sociale erroné)
- lors d'un export ou d'une migration de données (conversion de format erronée), des champs sont mal interprétés ou tronqués, entraînant une perte de précision

La « ***violation de la disponibilité*** » : correspond à la perte ou destruction accidentelle/ malveillante de données personnelles, ou à leur chiffrement par un tiers non autorisé.

Exemples :

- un pirate informatique chiffre la base de données clients d'un responsable du traitement qui n'en a aucune autre copie
- la seule copie des données personnelles dont dispose un responsable du traitement a été supprimée par un pirate informatique
- une base de données non dupliquée est indisponible pour des raisons techniques

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

Quels sont les principaux types de violations de données ?

Les principaux types de violations de données sont les suivants :

- **Accès non autorisé** : des personnes obtiennent un accès aux données sans permission, souvent *via* le piratage ou l'usurpation d'identité.
- **Fuite accidentelle** : des données sont partagées ou exposées par erreur, par exemple via un e-mail envoyé au mauvais destinataire ou un système mal configuré.
- **Vol de données** : des informations sont dérobées intentionnellement, souvent dans un but de fraude, de chantage, ou de revente de ces données.
- **Perte de données :** des données sont supprimées ou disparaissent suite à une défaillance technique, une erreur humaine ou un sinistre physique.
- **Ransomware :** des logiciels malveillants chiffrent les données d'un système en contrepartie d'une rançon pour leur restitution.
- **Intrusion dans le cloud :** des données hébergées dans des environnements de stockage en ligne sont compromises.
- **Violations internes :** des employés ou partenaires non autorisés accèdent ou divulguent des données.

Quelles violations de données sont concernées par cette obligation de notification ?

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.**

Qu'entend-on par « avoir connaissance d'une violation » ?

Le Groupe de travail européen indépendant « *Article 29* »[1] a considéré dans ses « *Lignes directrices sur la notification de violations de données à caractère personnel en vertu du règlement (UE) 2016/679* » que le responsable du traitement a pris connaissance d'une violation lorsqu'il est **raisonnablement certain** qu'un incident de sécurité s'est produit et que ledit accident a compromis des données personnelles.

Ce moment dépendra **des circonstances de la violation** en question.

En effet, si dans certains cas, il sera relativement clair dès le début qu'une violation s'est produite, dans d'autres cas, un certain temps pourrait être nécessaire avant de pouvoir déterminer si des données personnelles ont été compromises.

Exemple 1 : un responsable du traitement est contacté par un pirate informatique lui demandant une rançon pour récupérer ses données

Si après une vérification de son système, le responsable du traitement constate que celui-ci a effectivement été piraté, il dispose alors de **preuves claires** qu'une violation de données s'est produite, et il sera considéré comme ayant connaissance de ladite violation.

Exemple 2 : un employé informe son employeur qu'il a perdu une clé USB non chiffrée. Ledit employeur est réputé avoir pris connaissance de cette violation à ce moment-là même s'il n'est pas encore en mesure de savoir si des personnes non autorisées ont eu accès aux données que contenait cette clé.

Exemple 3 : un tiers informe un responsable du traitement qu'il a reçu un e-mail de sa part qui ne lui est pas destiné. Le responsable du traitement peut alors avoir besoin d'un peu de temps pour vérifier que cet email a effectivement été envoyé à un destinataire par erreur.

Le responsable du traitement sera considéré comme ayant eu connaissance de la violation une fois ces vérifications faites.

Lorsque le responsable du traitement doit mener une enquête afin de déterminer si une violation a effectivement eu lieu, cette période d'enquête initiale doit débuter **aussi rapidement que possible** après l'alerte.

[1] Groupe de travail européen indépendant qui traitait les questions relatives à la protection de la vie privée et aux données à caractère personnel jusqu'au 25 mai 2018 avant d'être remplacé par le Comité européen de la protection des données

Qu'entend-on par « violation susceptible d'engendrer un risque pour les droits et libertés » ?

Dans certains cas, la **violation peut n'avoir aucune conséquence** sur les droits et libertés des personnes concernées.

Exemples :

- les données personnelles concernées par la violation sont déjà disponibles pour le public
- la suppression de données sauvegardées et immédiatement restaurées
- la perte de données protégées par un algorithme de chiffrement à l'état de l'art, si la clé de chiffrement n'est pas compromise et si une copie des données reste disponible
- les opérations d'une entreprise sont perturbées par une panne électrique qui rend les données personnelles indisponibles pendant quelques minutes à peine

En raison de son absence de risque pour les personnes concernées, une telle violation n'a pas à être notifiée à l'APDP. Elle doit toutefois être consignée dans le registre des violations de données que tient le responsable du traitement.

Dans d'autres cas en revanche la violation présente un risque **faible, moyen ou élevé** pour les droits et libertés des personnes concernées, et doit être notifiée à l'APDP.

Exemples de risque élevé :

- les dossiers patients détenus par un hôpital ne sont pas disponibles pendant plus de 24 heures suite à un piratage informatique
- les données bancaires des clients d'une société sont volées et publiées en ligne
- les données de rémunération des salariés d'une grosse entreprise sont envoyées à une mauvaise liste qui comprend de très nombreux destinataires

Si la notification peut ne pas être requise dans un premier temps car il n'existe pas de risque **probable** pour les droits et libertés des personnes, un risque peut apparaître avec le temps.

Exemple : lorsqu'un employé informe son employeur qu'il a perdu une clé USB chiffrée, le responsable du traitement peut décider de ne pas notifier la violation de données lorsque la clé de cryptage reste en sa possession et que les données personnelles affectées ne constituent pas une copie unique.

En revanche, s'il se rend compte par la suite que la clé de cryptage a été comprise, les données personnelles deviennent alors accessibles. Il devra donc notifier cette violation en raison du risque que ladite violation est susceptible d'engendrer pour les droits et libertés des personnes concernées.

Il est donc important de **toujours réévaluer** cette absence de risque initial.

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

Quand procéder à la notification ?

Une fois qu'il a connaissance de la violation, le responsable du traitement doit la notifier à l'APDP **dans les meilleurs délais**, et si possible dans un délai maximum de **72 heures après en avoir pris connaissance**.

Quid du sous-traitant
Le sous-traitant **doit notifier** au responsable du traitement **toute violation** de données personnelles **dès qu'il en a connaissance.** Il n'a toutefois pas à évaluer la probabilité qu'un risque découle d'une violation avant de la notifier. Le responsable du traitement reste responsable de la notification à l'APDP, même si la violation a eu lieu chez le sous-traitant.

Il arrive que le responsable du traitement ne dispose pas de toutes les informations concernant une violation dans les 72 heures après en avoir pris connaissance, notamment en cas de violation complexe. Une **notification échelonnée** est alors possible avec une notification préalable de l'APDP dans les 72 heures avec un résumé succinct de l'incident puis par la suite la fourniture d'éléments complémentaires et plus détaillés.

Lorsque la notification n'a pas lieu dans les 72 heures, elle est accompagnée des motifs du retard.

Que doit contenir la notification ?

Les mentions obligatoires

La notification faite à l'APDP doit contenir les informations suivantes :

- **la nature de la violation** y compris, dans la mesure du possible, **les catégories et le nombre approximatif de personnes concernées** par la violation ;
- le **nom et les coordonnées du délégué à la protection des données** lorsque celui-ci a été désigné ou d'un **autre point de contact** auprès duquel des **informations supplémentaires** peuvent être obtenues ;
- les **conséquences probables** de la violation ;
- les **mesures prises** ou celles que le responsable du traitement propose de prendre pour **remédier à la violation,** y compris le cas échéant, les mesures pour en atténuer les éventuelles conséquences négatives.

Outre ces informations obligatoires, le responsable du traitement peut également fournir des conseils spécifiques aux personnes affectées concernant la façon de se protéger des possibles conséquences de la violation.

Exemple : réinitialisation des mots de passe

Registre des violations de données

Le responsable du traitement **doit documenter** toute violation de données personnelles, même quand il n'est pas tenu de notifier l'APDP.

Cette documentation doit indiquer :

- **les faits** concernant la violation,
- **ses effets** et
- **les mesures** prises pour y remédier.
-

Il est recommandé de documenter également les **décisions prises en réaction à la violation**, notamment lorsque le responsable du traitement n'a pas notifié la violation de données, les raisons pour lesquelles il a estimé que cette violation n'engendre pas de risque pour les personnes concernées.

Ce registre des violations de données peut être un registre spécifique ou bien faire partie d'un registre plus global relatif aux incidents de sécurité.

Dans quel cas les personnes concernées par la violation doivent-elles être informées ?

Si 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.**

L'appréciation du risque élevé se fait à la lumière d'un incident particulier et repose sur les conséquences qui en découlent.

Elle tient ainsi compte, notamment :

- du **type** de violation
- des **catégories** et du **volume** des données
- de la **facilité d'identification** des personnes concernées
- de la **gravité des conséquences** pour les personnes concernées
- de la **probabilité qu'elle se reproduise**

En cas de doute, le responsable du traitement devrait opter pour la prudence et procéder à une communication.

Que doit contenir l'information des personnes concernées ?

L'information des personnes concernées doit décrire la **nature** de la violation en des **termes clairs** et doit contenir les informations suivantes :

- le **nom** et les **coordonnées du délégué à la protection des données** lorsque celui-ci a été désigné ou d'un **autre point de contact** auprès duquel des informations supplémentaires peuvent être obtenues ;
- les **conséquences probables** de la violation et
- les **mesures prises** ou celles que le responsable du traitement propose de prendre pour **remédier** à la violation, y compris le cas échéant, les mesures pour en atténuer les éventuelles conséquences négatives.

Si le responsable du traitement n'a pas communiqué la violation des données aux personnes concernées, **l'APDP peut lui ordonner de le faire**.

Cette information peut être **complétée** de recommandations à destination des personnes pour atténuer les effets négatifs potentiels de la violation et leur permettre de prendre les précautions qui s'imposent.

Comment s'effectue par la communication auprès des personnes concernées ?

La communication doit en principe s'effectuer **directement** auprès des personnes concernées, à moins que cela n'exige des efforts disproportionnés.

Cette information doit être **claire** et **transparente**. Il est ainsi recommandé qu'elle ne contienne pas d'autres informations afin de ne pas diluer le message.

Exemples :

- messages directs (e-mail, SMS, message directe)
- notifications ou bannières bien visibles sur le site Internet
- communications postales
- annonces bien visibles dans des médias imprimés

En fonction des circonstances, le responsable du traitement devra utiliser **plusieurs méthodes de communication**, à défaut d'un seul canal, afin de **maximiser la probabilité que les informations soient effectivement communiquées.**

Dans quel cas la communication aux personnes concernées n'a-t-elle pas à être effectuée ?

La communication d'une violation de données n'a pas à être effectuée **si l'une des 3 conditions suivantes** est remplie :

Condition 1 : les données affectées par la violation ont **préalablement** fait l'objet de **mesures de protection technique et organisationnelle** qui rendent lesdites données **incompréhensibles** pour toute personne n'étant pas autorisée à y accéder

Exemple : chiffrement des données

Condition 2 : le devoir d'informer individuellement la personne concernée nécessiterait des **efforts disproportionnés**

Exemple : le responsable du traitement n'a aucune information permettant de contacter les personnes

Dans ce cas, il est recommandé de procéder à une **communication publique** ou à une mesure similaire permettant aux personnes concernées d'être informées de manière tout aussi efficace.

Condition 3 : les mesures ultérieures prises par le responsable du traitement **garantissent que le risque n'est plus susceptible de se matérialiser**

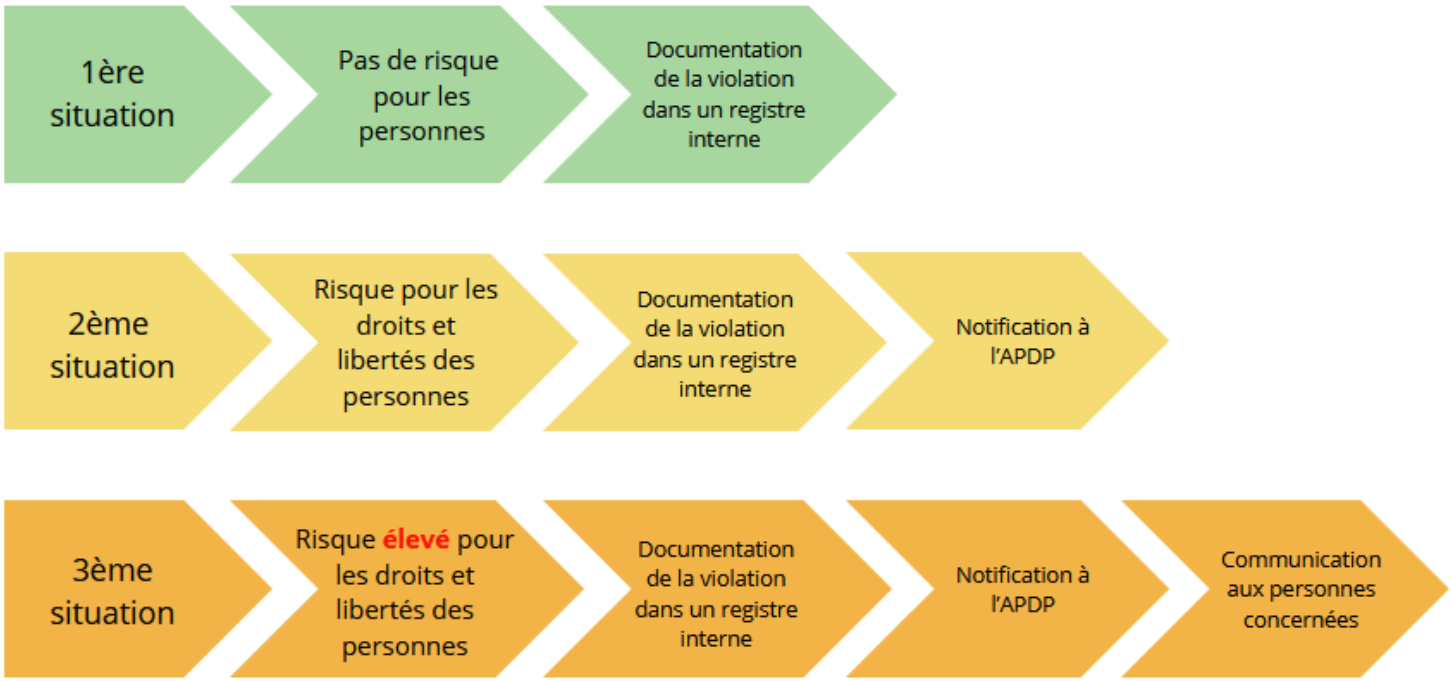
Exemple : réinitialisation de mots de passe qui ont été volés

Quelle sanction en cas de manquement à l'obligation de notification ?

En cas de manquement à **l'obligation de notifier une violation de données,** et le cas échéant, de la **communiquer aux personnes concernées**, l'organisme peut encourir une amende administrative ne pouvant excéder **5.000.000 euros ou, dans le cas d'une entreprise, jusqu'à 2% du chiffre d'affaires annuel mondial total de l'exercice précédent, le montant le plus élevé étant retenu.**

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

En résumé :


1ère situation
Pas de risque pour les personnes
Documentation de la violation dans un registre interne
2ème situation
Risque pour les droits et libertés des personnes
Documentation de la violation dans un registre interne
Notification à l'APDP
3ème situation
Risque élevé pour les droits et libertés des personnes
Documentation de la violation dans un registre interne
Notification à l'APDP
Communication aux personnes concernées