



Afin d'éviter toute perte de saisie, veuillez à bien sauvegarder le formulaire sur votre terminal avant de le remplir.

2.4 Mesures techniques et organisationnelles appliquées par le responsable de traitement à la violation de données à caractère personnel

Mesures de protection technologiques appropriées mises en œuvre, préalablement à la violation, pour rendre les données incompréhensibles à toute personne non autorisée à y avoir accès¹ :
(décrire ces mesures et les dispositions prises pour leur conférer une pleine efficacité)

Le cas échéant, références du dossier de formalités accomplies auprès de la CNIL préalablement à la mise en œuvre du traitement et dans lequel ces mesures sont décrites :

Autres mesures préventives mises en œuvre :

Mesures prises par le responsable de traitement en réaction immédiate à la violation :

2.5 Recours à un tiers pour fournir le service concerné par la violation

oui, préciser le nom du tiers et sa qualité : sous-traitant, prestataire, fournisseur...

non

3 Informations supplémentaires

(à fournir dans le cas d'une notification complète ou complémentaire)

3.1 Informations sur la violation

3.1.1 Résumé de l'incident à l'origine de la violation

Description générale :

¹ Les données sont considérées comme incompréhensibles si :

elles ont été chiffrées en mode sécurisé à l'aide d'un algorithme normalisé et la clé utilisée pour les décrypter n'a été compromise dans aucune violation de sécurité et a été générée de façon à ne pouvoir être trouvée, par aucun moyen technologique existant, par quelqu'un qui n'est pas autorisé à l'utiliser ; ou elles ont été remplacées par leur valeur hachée, calculée à l'aide d'une fonction de hachage normalisée à clé cryptographique, et la clé utilisée pour les hacher n'a été compromise dans aucune violation de sécurité et a été générée de façon à ne pouvoir être trouvée, par aucun moyen technologique existant, par quelqu'un qui n'est pas autorisé à l'utiliser.

Lieu de la violation :

Supports des données concernées par la violation (serveur, poste fixe, ordinateur portable, disque de sauvegarde, document papier...)

3.1.2 Nombre de personnes concernées par la violation

3.1.3 Conséquences potentielles (impacts sur les données)

Les données ont été, ou pourraient vraisemblablement être (il est possible de cocher plusieurs cases) :

En cas de perte de confidentialité :

... **diffusées plus que nécessaire** et avoir échappé à la maîtrise des personnes concernées (ex. : diffusion plus ou moins large, diffusion non désirée d'une photo sur Internet, perte de contrôle d'informations publiées un réseau social...);

... **corrélées** avec d'autres informations relatives aux personnes concernées (ex. : corrélation d'adresses de résidence et de données de géolocalisation en temps réel...);

... **exploitées à d'autres fins** que celles prévues et/ou de manière injuste (ex. : fins commerciales, usurpation d'identité, utilisation à l'encontre des personnes concernées...).

En cas de perte d'intégrité :

... **modifiées en des données invalides**, qui ne seront pas utilisées de manière correcte, le traitement pouvant engendrer des erreurs, des dysfonctionnements, ou ne plus fournir le service attendu (ex. : altération du bon déroulement de démarches importantes...);

... **modifiées en d'autres données valides**, de telle sorte que les traitements soient détournés (ex. : exploitation pour usurper des identités en changeant la relation entre l'identité des personnes et les données biométriques d'autres personnes...).

En cas de perte de disponibilité :

... **manquantes à des traitements qui ne peuvent plus du tout fournir le service attendu** (ex. : ralentissement ou blocage de processus administratifs ou commerciaux, impossibilité de fournir des soins du fait de la disparition de dossiers médicaux, impossibilité pour des personnes concernées d'exercer leurs droits...);

... **manquantes à des traitements et générer des erreurs, des dysfonctionnements, ou fournir un service différent de celui attendu**

(ex. : certaines allergies ne sont plus signalées dans un dossier médical, certaines informations figurant dans des déclarations de revenus ont disparu, ce qui empêche le calcul du montant des impôts...).

3.1.4 Préjudices potentiels (impacts sur les personnes concernées)

Description générale :

Estimation du niveau de la gravité (choisir le niveau le plus approprié au vu de la description et des exemples) :

Niveau	Description du niveau	Préjudices potentiels représentatifs du niveau
Négligeable	Les personnes concernées ne seront pas impactées ou pourraient connaître quelques désagréments, sans difficulté	Perte de temps pour réitérer des démarches ou pour attendre de les réaliser, simple contrariété...
Limité	Les personnes concernées pourraient connaître des désagréments significatifs, qu'elles pourraient surmonter malgré quelques difficultés	Frais supplémentaires, refus d'accès à des prestations commerciales, peur, affection physique ou psychologique mineure...
Important	Les personnes concernées pourraient connaître des conséquences significatives, qu'elles pourraient surmonter, mais avec de sérieuses difficultés	Détournements d'argent, interdiction bancaire, dégradation de biens, perte d'emploi, assignation en justice, affection physique ou psychologique grave...
Maximal	Les personnes concernées pourraient connaître des conséquences significatives, voire irrémédiables, qu'elles pourraient ne pas surmonter	Péril financier tel que des dettes importantes ou une impossibilité de travailler, affection physique ou psychologique de longue durée ou permanente, décès...

3.1.5 Mesure techniques et organisationnelles prises par le responsable de traitement suite à la violation

Mesures conseillées aux personnes concernées :

Autres mesures prises ou prévues pour réduire l'impact sur les personnes concernées :

Mesures prises ou prévues pour revenir à une situation normale :

Mesures prises ou prévues pour éviter que la violation se reproduise :

3.2 Information des personnes concernées par la violation (l'information de la personne doit être effectuée sans retard injustifié après la constatation de la violation)

3.2.1 Fourniture d'une information aux personnes concernées

Oui, les personnes ont été informées le (date) :

Non, mais elles le seront le (date) :

Non, car des mesures de protection technologiques appropriées ont été mises en œuvre, préalablement à la violation, pour rendre les données incompréhensibles à toute personne non autorisée à y avoir accès².

Non, car :

le responsable de traitement considère qu'il y a un risque que la notification nuise à l'efficacité de l'enquête sur la violation³ (détailler) : _____

le responsable de traitement n'étant pas en mesure d'identifier toutes les personnes concernées dans le délai, il a procédé, sans retard injustifié, à l'information de ces personnes par des avis dans de grands médias nationaux ou régionaux, tout en continuant à tenter d'identifier ces personnes afin de les informer individuellement dès que possible (détailler) : _____

3.2.2 Contenu de l'information fournie aux personnes concernées

Joindre à votre notification une copie du contenu de l'information fournie aux personnes concernées.

3.2.3 Moyen de communication utilisé pour informer les personnes concernées⁴

Information par voie postale.

Information par courrier électronique.

Autre moyen d'information : _____

3.2.4 Nombre de personnes informées

3.3 Violations concernant des personnes localisées dans d'autres pays de l'Union européenne (UE)

Violation de données concernant des personnes localisées dans d'autres pays de l'UE.

Notification de la violation à d'autres autorités compétentes dans un ou plusieurs pays de l'UE.

Liste des autorités notifiées : _____

Observations

Indiquer à la CNIL toute information utile à l'instruction de la notification.

² Dans ce cas, il convient de s'assurer que le point 2.4 ci-dessus a bien été complété car seules les mesures validées par la CNIL peuvent dispenser d'informer les personnes concernées.

³ Dans ce cas, le responsable de traitement doit obtenir l'accord de la CNIL pour retarder l'information des personnes concernées.

⁴ La notification doit être rédigée dans une langue claire et aisément compréhensible et les informations concernant la violation ne doivent pas être associées à d'autres informations (être mentionnées sur la facture adressée aux personnes concernées, par exemple). En outre, la notification doit être adressée à la personne par tout moyen permettant au responsable de traitement d'apporter la preuve de l'accomplissement de cette notification. Enfin, le moyen de communication utilisé doit garantir une réception rapide de l'information et doit être sécurisé conformément aux règles de l'art.