Sécurisation des données personnelles

Foire aux questions

Ce document a été élaboré à partir des questions remontées par les adhérents en 2021 notamment lors du webinaire organisé le 1er décembre 2021 sur la sécurisation des données personnelles du secteur de l'inclusion sociale lors duquel sont intervenus :

- La FAS pour une présentation des enjeux dans le secteur de l'inclusion sociale ;
- La CNIL pour une présentation du guide de la sécurité des données personnelles ;
- Un adhérent pour un témoignage sur la sécurisation des données dans sa structure.

1. La teneur de l'obligation de sécuriser les données

- **L'envoi de fichiers (via Outlook, par exemple) n'est pas autorisé ou n'est pas recommandé ? Existe-t-il des canaux d'envoi spécifiques pour les documents contenant des données sensibles ?**

Rappel concernant l'obligation d'assurer la sécurité des données

Le RGPD impose aussi bien au responsable de traitements (= celui qui met en place le traitement) qu'au sous-traitant (= celui qui traite des données dans le cadre de missions confiées par le premier) d'assurer la sécurité des données. Cela implique de prendre toute mesure pour :

- *Assurer la confidentialité des données (= aucune personne non autorisée n'y ait accès)*
- *Assurer l'intégrité des données (= aucune personne non autorisée ne puisse les modifier)*
- *Assurer leur disponibilité (=garantir le bon fonctionnement des SI afin de maintenir l'accessibilité aux données aux seules personnes habilitées)*

Cela implique que le responsable de traitements doit prendre des mesures techniques (ex : mise en place de mots de passe) et organisationnelles (ex : sensibilisation des utilisateurs) pour assurer la sécurité des données. S'il fait appel à un sous-traitant, le responsable de traitements devra lui donner des instructions à ce titre ; le sous-traitant devant être en mesure de les mettre en œuvre.

S'agissant de la confidentialité des données, cela implique de prendre les mesures nécessaires pour la préserver aussi bien en interne (ex : prévoir des restrictions d'accès aux données en fonction des postes) qu'en externe en sécurisant les transmissions de données.

S'agissant de l'envoi d'email contenant des données personnelles en clair, cela pose des difficultés de nature à menacer la confidentialité des données. Il faut prendre des mesures de sécurité comme, par exemple, mettre un mot de passe à un fichier contenant des données personnelles et communiquer le mot de passe par un canal différent des emails (par exemple par téléphone) et chiffrer les emails contenant des données personnelles en clair.

D'autres mesures de sécurité peuvent être prises pour la transmission de documents par voie électronique comme l'utilisation d'un protocole garantissant la confidentialité et l'authentification du serveur destinataire pour les transferts de fichiers en utilisant par exemple HTTPS et la version la plus récente de ce protocole.

Par ailleurs, cela implique de prendre des mesures organisationnelles comme la sensibilisation des utilisateurs (inciter, dans la mesure du possible, à ne pas mettre des données personnelles en clair dans les emails, apprendre à verrouiller des fichiers par mot de passe, etc.).

S'agissant des envois de documents contenant des données sensibles, il n'existe pas de canaux de transmission spécifiques à ces données qui seraient recommandés. En revanche, il convient de faire preuve d'une vigilance supplémentaire en présence de données sensibles. Dans ce contexte, il ne faut pas hésiter à prendre davantage de mesure de sécurité comme le chiffrement de ces documents.

Pour plus d'information, consulter le **guide de la sécurité des données personnelles de la CNIL.**

- **Est-ce au responsable de traitement ou au sous-traitant d'assurer la sensibilisation des utilisateurs pour la sécurisation des données ?**

Cette obligation de sécurisation des données, incombant au responsable de traitement, implique pour ce dernier de prendre toutes les mesures organisationnelles nécessaires (la sensibilisation des utilisateurs constituant une telle mesure).

Il faut noter que la mise en place de sensibilisation peut être déléguée contractuellement au sous-traitant. Par ailleurs, le sous-traitant a ses propres obligations définies par l'article 28.3.f du RGPD : « *[le sous-traitant] aide le responsable du traitement à garantir le respect des obligations [de sécurité] compte tenu de la nature du traitement et des informations à la disposition du sous-traitant* ».

L'article précité n'a pas fait l'objet d'une interprétation «officielle» (une décision du juge, un avis d'une autorité de contrôle). Sous réserve de décision officielle, on peut déduire de cet article qu'il oblige le sous-traitant à fournir les informations nécessaires au responsable de traitements notamment pour les actions de sensibilisation.

2. La responsabilité des acteurs

- **Que risque une structure si des données personnelles sont perdues ou s'il y a une violation de données ?**

Le droit prévoit des familles de responsabilité différentes notamment celle de droit commun (responsabilité pour faute prévue à l'article 1240 du code civil) et celle prévue par le RGPD (responsabilité du responsable de traitements vis-à-vis de l'autorité de contrôle soit la CNIL au niveau national).

Sur cette dernière famille de responsabilité, le responsable de traitements correspond à la structure qui met en place le traitement de données personnelles en définissant ses finalités et ses moyens. En cas de violation du RGPD (comme la perte de données), c'est le responsable de traitements qui sera tenu responsable et non ses préposés soit les salariés, stagiaires, bénévoles, etc. Sauf exception (cas de figure très rare), il n'y aura pas de responsabilité individuelle de ces derniers retenue.

- **Dans le cadre de demandes de communication de données par des tiers (financeurs, services déconcentrés de l'Etat notamment) des données de salariés sont demandées, qu'en est-il de l'autorisation de ces derniers ?**

En cas de demande de communication par des tiers, l'autorisation des salariés n'est pas pertinente. En effet, le RT doit garantir la sécurité des données (incluant leur confidentialité) et doit s'assurer de la légalité des demandes de communication de tiers ; le tiers devant à son tour la justifier. Le RT doit vérifier que :

- Une base juridique autorise la communication des données ;
- La finalité de transmission des données personnelles ;
- L'adéquation entre le périmètre des données demandées et la finalité de transmission ;
- Les mesures de sécurité prévues pour la transmission des données.

Si la demande de communication ne contient pas les éléments précités, le RT est tout à fait légitime à les demander (cf. modèle de réponse à une demande de communication en annexe). Si le tiers ne justifie pas sa demande suite à la demande des éléments précités par le RT, ce dernier est fondé à ne pas y répondre. Il pourra être envisagé d'adresser des données anonymisées permettant au tiers financeur d'exercer ses missions de contrôle.

Par ailleurs, lorsque la demande est fondée, il faut bien s'assurer de transmettre que les données nécessaires (ce qui implique de faire un tri préalable).

Face aux demandes de communication de données (que ce soit de salariés ou de personnes accompagnées), n'hésitez pas à solliciter la FAS et/ou la CNIL pour assistance (les demandes de conseil à la CNIL étant confidentielles) notamment lorsque la demande concerne des données sensibles (qui doivent faire l'objet d'une vigilance accrue).

Pour plus d'informations, consultez le **guide des tiers autorisés** / **recueil de procédures**.

Annexe : modèle de réponse à une demande de communication de données

Ce modèle est à adresser en cas de demande de communication d'un tiers ne présentant pas les justifications nécessaires que la CNIL impose.

« Nous avons bien reçu votre demande visant à ce que nous vous transmettions des données à caractère personnel des personnes accueillies par notre structure. En tant que responsable du traitement des données et en application du RGPD, nous sommes contraints de vous demander des informations complémentaires avant toute transmission. Par conséquent, pourriez-vous nous préciser :

Quelle est la base juridique autorisant la demande de communication des données ?

Quelle est la finalité de la transmission des données demandées ?

Quelles sont précisément les données personnelles dont vous souhaitez la communication ?

Quelles sont les mesures de sécurité mises en place pour l'envoi de ces données et leur traitement ?

Nous restons à votre disposition pour toute question complémentaire, »

Fédération
des acteurs de
la solidarité

https://www.federationsolidarite.org/

@FederationSolidarite

@FedeSolidarite

@federationsolidarite

Cette action est cofinancée par l'Union Européenne.

RÉPUBLIQUE
FRANÇAISE
Liberté
Égalité
Fraternité

Direction générale de la cohésion sociale
Délégation générale à l'emploi
et à la formation professionnelle