RGPD AVOIR TOUJOURS LES BONS RÉFLEXES

Fiche n°3

Que faire si quelqu'un demande un accès à ses données personnelles ?

CONTEXTE

La demande d'accès à ses données personnelles (Article 15 du RGPD) est un des 6 droits (droit d'accès, d'opposition, de limitation, de rectification, de portabilité et d'effacement) que peut exercer une personne concernant ses données. Il est à noter que toute personne physique peut effectuer une telle demande auprès d'une société dont elle est cliente, de son employeur, de son médecin, d'une administration ou de tout organisme détenant des Données à Caractère Personnel (DCP) sur elle.

La demande peut se porter sur :
- La nature et finalités du traitement des données la concernant (Quelles informations avez-vous ? Comment et pourquoi sont-elles utilisées ?)
- La durée de conservation des données récoltées.
- La copie partielle ou totale de toutes ses données.
- L'envoi ou la mise à disposition des données à un tiers.

Toute demande d'accès se doit d'être traitée dans le mois suivant celle-ci (sauf exception). Pour y répondre correctement, quelques règles existent et doivent être respectées.

Retrouvez également toutes les recommandations de la CNIL sur l'article suivant :
Professionnels : comment répondre à une demande de droit d'accès ?

L'ESSENTIEL À RETENIR

- **Vérifier** l'identité du demandeur
- **Qualifier** la demande et y répondre sous un 1 mois pouvant être étendu à 3 si la demande le nécessite
- **Avertir** le demandeur de toute action ou évolution de la situation
- **Garder** un registre ou une archive spéciale des demandes reçues et traitées : à minima la demande initiale et la réponse faite pour faciliter le traitement d'une demande ultérieure et similaire.
- **Se renseigner** sur les peines encourues : https://www.cnil.fr/fr/les-sanctions-penales

ACTIONS À RÉALISER

- Étape n°1 : Analyser la pertinence de la personne

La CNIL préconise la vérification de l'identité de la personne avant le traitement de celle-ci. En fonction des données concernées la vérification peut s'avérer utile voire obligatoire.

Si on ne peut pas identifier le demandeur, dans la mesure où les preuves apportées ne sont pas suffisantes (n° client, courrier, etc...), il doit démontrer son identité par d'autres moyens.

Plusieurs acteurs peuvent demander un accès aux données personnelles :
- La personne concernée.
- Une tierce personne avec un mandat démontrant la demande de droit d'accès de la personne concernée, l'identité du mandant et du mandataire.

- Les organismes qui en ont le droit : une autorité administrative, la justice...

Cf. Fiche Réflexe n°4 : Que faire si une autorité demande un accès à des données personnelles ?

- Étape n°2 : Analyser la pertinence de la demande

1. Trier les demandes reçues

Si abusives, excessives, etc... Informer le demandeur qu'il n'y aura pas de suite à ces demandes ou exiger des frais raisonnables qui tiennent compte des coûts administratifs.

2. Déterminer la provenance

La provenance peut influer sur le temps de traitement et les moyens à mettre en place pour y répondre.
Elle peut provenir du support, d'un mail générique RGPD créé pour ces demandes, du DPD (Délégué à la Protection des Données). Ceci doit être transparent pour le demandeur. Privilégier un processus simple et rapide, à partir du moment où la réponse est traitée dans les temps impartis.

3. S'appuyer sur les acteurs concernés

La demande est gérée par le DPD (ou sa cellule) qui s'appuie sur l'organisation mise en place dans son organisme pour traiter ce type de demande : responsable du traitement, référent métier ou Chef de Projet SI des applis concernées par exemple. Cela reste propre à chaque entreprise.

- Étape n°3 : Répondre au demandeur

La réponse doit s'effectuer d'après l'Article 12 (Paragraphe 3) : « (...) dans les meilleurs délais et en tout état de cause dans un délai d'un mois à compter de la réception de la demande ».
Conserver la demande à date de réception par mail.
La demande et la réponse doivent être juridiquement traitées de la même manière.

Délais particuliers : La demande d'une copie partielle ou intégrale des données d'une personne peut nécessiter plus de temps pour réunir tous les documents à fournir. La réponse peut être faite sous 3 mois mais le demandeur doit être averti dans la limite réglementaire de 1 mois.

POINTS DE VIGILANCE

- **Traitement des demandes**

Il est conseillé d'avoir la validation ou l'avis du DPD, en charge de mettre en œuvre la conformité RGPD au sein de l'organisme qui l'a désigné. En cas de non-respect du règlement, la CNIL établit que **le Responsable du Traitement (RT) est le seul responsable** car il est tenu de démontrer que le traitement est conforme aux dispositions qu'il a mises en place.

- **Cas de demandes abusives, répétitives, infondées ou excessives** (article 12, paragraphe 5)

Le Responsable de traitement (RT) peut :

- « Exiger le paiement de frais raisonnables qui tiennent compte des coûts administratifs (...) »
- « Refuser de donner suite à ces demandes »

Le RT doit **prouver que la demande est excessive et en expliquer les raisons.** Afin de se prémunir contre d'éventuels risques judiciaires, il est fortement conseillé d'archiver les demandes et la preuve des abus.

RISQUES

Ne pas vérifier que la demande concerne un tiers

- La réponse doit tenir compte du droit des tiers et toute information transmise pouvant identifier une tierce personne doit être masquée.

Ne pas répondre ou ne pas respecter le délai applicable pour chaque type de demande

Dans ce cas, la CNIL peut :

- Prévoir une amende : Cf. article R 625 – 11 du Code pénal pour les contraventions de la 5e classe, correspondant à un montant de 1 500€.
- Auditer sur le traitement des demandes.
- Ordonner de satisfaire aux demandes d'exercice des droits des personnes, y compris sous astreinte.
- Prononcer un rappel à l'ordre.
- Limiter temporairement ou définitivement le traitement concerné.