

Toute personne physique peut accéder aux données qui la concernent (article 15 du RGPD). La CNIL rappelle les règles à suivre pour répondre correctement à ces demandes.

La loi Informatique et Libertés permet à toute personne d'accéder aux données qui la concernent. Ce droit est renforcé par le Règlement général sur la protection des données (RGPD) qui est entré en application en mai 2018.

Une personne peut exercer son droit d'accès :

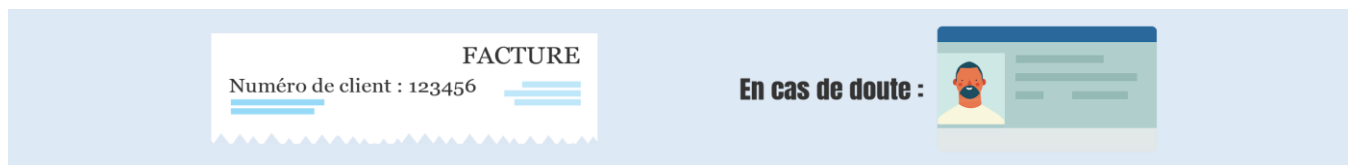
- auprès d'une société dont elle est cliente, par exemple pour avoir la copie de son dossier client ou d'une conversation téléphonique avec le service clients qui a été enregistrée ;
- auprès de son employeur pour accéder aux données de son dossier administratif ;
- auprès de son médecin pour obtenir une copie des données de son dossier médical ;
- auprès d'une administration pour obtenir la confirmation que des données la concernant sont traitées.

En résumé : comment répondre à une demande en 4 étapes ?

Une personne peut vous demander :

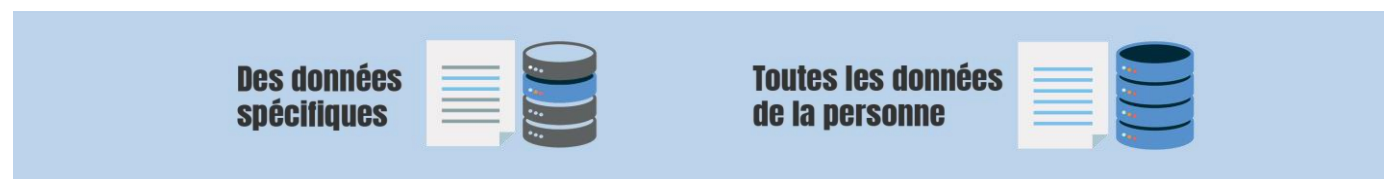
- l'accès à l'information sur le traitement éventuel de données la concernant (« avez-vous des données me concernant ? Pour quoi faire ? Combien de temps les conservez-vous ? À qui les transmettez-vous ? » etc.) ;
- l'obtention d'une copie de ces données.

1. Si nécessaire, vérifiez l'identité de la personne qui exerce sa demande



Êtes-vous sûr de l'identité de la personne qui exerce sa demande ? Procédez à cette vérification si nécessaire (voir « Quels justificatifs demander »).

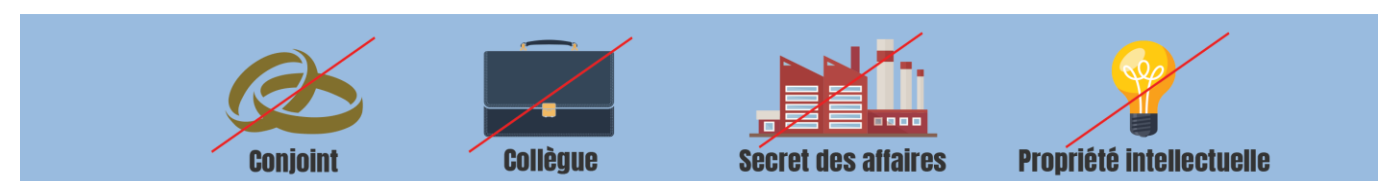
2. Si nécessaire, demandez sur quelles données portent la demande



Il arrive que certaines demandes concernent l'ensemble des données traitées par un organisme. Dans ce type de cas, si la demande porte sur une grande quantité de données, vous pouvez demander à la personne concernée de préciser sur quelles données ou quelles opérations de traitement porte sa demande (considérant 63 du RGPD).

Il vous faudra revenir vers elle dans un délai maximum d'un mois (voir « Les délais pour répondre à une demande »).

3. Vérifiez que la demande ne concerne pas un tiers



Lorsque vous recevez une demande de droit d'accès, vous devez vérifier qu'il s'exerce dans le respect du droit des tiers. Par exemple, il n'est pas possible de demander l'accès aux données concernant son conjoint ; un salarié d'une entreprise ne peut obtenir des données relatives à un collègue.

De même, le droit d'accès ne peut porter atteinte au secret des affaires ou à la propriété intellectuelle (droit d'auteur protégeant le logiciel par exemple).

En pratique, cela peut par exemple conduire à masquer, dans ce qui est envoyé au demandeur, l'identité de tiers ou des éléments permettant indirectement de les identifier.

4. Répondez à la demande en respectant les délais

The infographic is a blue rectangular box with white text and icons. It is divided into four sections. The first section shows an hourglass icon, the text '1 mois max.', and 'Demande simple'. The second section shows a green medical cross icon, the text '8 jours max.', and 'Données de santé'. The third section shows a blue database cylinder icon, the text '3 mois max.', and 'Demande complexe (par ex. beaucoup de données)'. The fourth section shows a red flag icon, the text 'Vous pouvez refuser si', and two bullet points: '- la demande est infondée ou excessive' and '- les données ont été effacées'. At the bottom of the box, there is a white megaphone icon followed by the text 'Dans tous les cas, informez la personne sous un mois maximum'.

La personne demande-t-elle seulement des informations la concernant ou également une copie de ses données ?

- Si vous traitez des données concernant le demandeur, vous devez lui fournir les [informations prévues aux articles 13 ou 14 du RGPD](#) qui figurent en principe sur tout support de collecte que vous utilisez.
- Si la personne demande la copie de ses données, vous devez les lui communiquer, quel que soit le support sur lequel ces données sont enregistrées (document papier ou électronique, enregistrement vidéo, sonore, etc.). Le fait que des données soient contenues dans un document ne les rend pas pour autant non communicables. Il faudra, lors de la réponse, prendre en compte le droit des tiers.

Attention : Vous ne pouvez pas répondre à une demande d'accès en indiquant seulement à la personne que vous disposez des données qu'elle vous avait communiquées ou en listant seulement les catégories de données dont vous disposez.

Les données personnelles présentes dans un document (courrier, note, rapport, enregistrement vocal ou visuel, etc.) peuvent être communiquées par la copie du document en lui-même ou par une retranscription fidèle sur un autre support.

Les données personnelles enregistrées dans un logiciel métier (CRM, gestion RH, etc.) peuvent être communiquées par la transmission d'impressions d'écrans ou d'une retranscription fidèle sur un autre support.

Peut-on refuser de répondre à un droit d'accès ?

Dans certains cas, vous pouvez refuser de répondre à des demandes de droit d'accès, mais vous devrez justifier cette décision.

Vous n'êtes pas tenus de répondre aux demandes de droit d'accès si :

- elles sont manifestement infondées ou excessives notamment par leur caractère répétitif (par exemple, demandes multiples et rapprochées dans le temps d'une copie déjà fournie) ;
- les données ne sont plus conservées / ont été effacées : dans ce cas, l'accès est impossible (ex. : les enregistrements réalisés par un dispositif de vidéosurveillance sont conservés normalement 30 jours maximum. Ils sont détruits à l'issue de ce délai).

A noter : le fait qu'une personne demande communication de données dont elle dispose déjà ne doit pas être considéré systématiquement comme une demande excessive. Il faut notamment apprécier le délai entre les deux demandes, la possibilité que des nouvelles données aient été collectées ou que les données ont été modifiées, etc.

Si vous ne donnez pas suite à une demande, vous devez motiver votre décision et informer le demandeur des voies et délais de recours pour contester cette décision.

L'exercice du droit d'accès n'est pas conditionné. **Cela signifie qu'une personne n'a pas à motiver sa demande** et qu'elle peut exercer son droit d'accès en parallèle d'une procédure contentieuse (devant le conseil des prud'hommes par exemple) ou administrative en cours, sous réserve de ne pas porter atteinte au droit des tiers. Le refus de communication sur ce fondement ne serait pas valable.

Quelles sont les obligations du responsable de traitement ?

En tant que responsable du traitement de données personnelles, vous devez :

- **Inform** les personnes concernées de l'existence de leur droit d'accès au moment où vous collectez leurs données ;
- **Permettre aux personnes d'exercer leur droit d'accès grâce à des modalités pratiques** (formulaire en ligne, coordonnées dédiées) ;
- **Mettre en place un parcours interne efficace** au sein de votre entité pour le traitement des demandes de droit d'accès. Cela nécessite de prévoir des procédures permettant de remonter les demandes de droit d'accès au bon interlocuteur afin d'être en mesure de traiter la demande dans les délais impartis ;
- Prévoir des modalités de réponse auprès des personnes concernées qui soient **compréhensibles, accessibles, formulées en des termes clairs et simples**.

Qui peut exercer cette demande ?

C'est à la personne voulant accéder à ses données personnelles de vous saisir.

Cette personne peut donner un **mandat** à une personne de son choix pour exercer son droit d'accès. Dans ce cas, la personne choisie doit présenter un courrier précisant :

- l'objet du mandat (exercice du droit d'accès) ;
- l'identité du mandant (identité du demandeur qui exerce son droit d'accès aux données le concernant) ;
- l'identité du mandataire (son identité).

Elle doit justifier de son identité et de celle du demandeur.

Pour les mineurs et les majeurs incapables d'exercer leurs droits, ce sont, selon les cas, les parents, le(s) détenteur(s) de l'autorité parentale ou le tuteur qui effectuent la démarche.

Quels justificatifs d'identité demander ?

Le principe : pas de pièce d'identité, sauf en cas de doute raisonnable.

Pour exercer ses droits, la personne doit justifier de son identité. Par principe, cette justification peut intervenir « par tout moyen ». Ainsi, il n'est pas nécessaire de joindre une photocopie d'un titre d'identité en cas d'exercice d'un droit dès lors que l'identité de la personne est suffisamment établie (par exemple, par la fourniture d'informations supplémentaires à celles relatives à l'identité, comme un numéro client ou adhérent, etc.).

Par ailleurs, dans un environnement numérique, le fait d'exercer ses droits depuis un espace où la personne s'est authentifiée peut-être suffisant, en fonction des données d'identité numériques demandées (par exemple FranceConnect).

Néanmoins, si vous avez un « doute raisonnable » sur l'identité du demandeur, vous pouvez lui demander de joindre tout autre document permettant de prouver son identité, comme par exemple, si cela est nécessaire, une photocopie d'une pièce d'identité.

Le niveau des vérifications à effectuer peut varier en fonction de la nature de la demande, de la sensibilité des informations communiquées et du contexte dans lequel la demande est faite.

Quels sont les délais pour répondre à une demande ?

Le principe :

- 1 mois maximum pour une demande simple ;

- 3 mois maximum pour une demande complexe (par exemple si une personne demande une copie de l'intégralité de ses données) ;
- 8 jours maximum pour des données de santé.

Quelle que soit la situation, il faut informer la personne des suites sous un mois maximum.

Vous devez répondre dans les **meilleurs délais** à une demande de droit d'accès, et dans un délai maximum d'**un mois** (article 12.3 du RGPD). Une possibilité de prolonger de deux mois ce délai est prévue, « compte tenu de la complexité et du nombre de demandes », à condition d'en informer la personne concernée dans le délai d'un mois suivant la réception de la demande (article 12.3 du RGPD).

Que vous répondiez à la demande de droit d'accès ou décidiez de prolonger le délai de deux mois, vous devrez informer la personne concernée dans un délai maximum d'**un mois**.

Focus sur le droit d'accès à des données de santé : En ce qui concerne l'accès aux données de santé, les délais sont différents. La communication des données de santé (exemple : dossier médical) doit être faite au plus tard dans les 8 jours suivant la demande et au plus tôt – compte tenu du délai de réflexion prévu par la loi dans l'intérêt de la personne – dans les 48 heures. Si les informations remontent à plus de cinq ans, le délai est porté à 2 mois (article L.1111-7 du Code de la santé publique).

Est-il possible de demander des frais de reproduction ?

Le RGPD prévoit un **principe de gratuité** pour les copies fournies dans le cadre d'une demande d'accès (article 12.5).

Vous ne pouvez demander le paiement de « frais raisonnables basés sur les coûts administratifs » que :

- pour toute copie supplémentaire demandée par la personne concernée ;
- si la demande est manifestement infondée ou excessive.

Attention : le coût des « frais raisonnables basés sur les coûts administratifs » ne doit pas être une entrave à l'exercice du droit d'accès.

De quelle manière les données peuvent-elles être communiquées ?

Les demandes peuvent être faites sur place ou par écrit (voie postale ou électronique).

- **Si la demande est formulée sur place** et que vous ne pouvez pas y apporter une réponse immédiatement, vous devez remettre au demandeur un avis de réception daté et signé.
- **Si la demande est formulée par voie électronique**, les informations sont fournies sous une forme électronique d'usage courant, à moins que la personne concernée ne demande qu'il en soit autrement (article 12.3). Dans ce cas, attention aux modalités de transmission des informations qui doivent se faire de manière **sécurisée**.
- **Si la demande est faite par écrit** et que vous avez besoin de précisions ou de compléments pour y répondre, vous devez prendre contact avec le demandeur (courrier postal ou électronique).
- **Si vous envoyez les données personnelles par voie postale**, il est souhaitable de le faire par le biais d'un courrier recommandé avec accusé de réception.
- **Si les données sont communiquées par clé USB**, vous pouvez remettre la clé USB en main propre à la personne qui vous a saisi ou l'envoyer par courrier. Vous devez prendre des mesures appropriées pour protéger les données contenues sur ce support, en particulier s'il s'agit de données sensibles. Afin d'éviter que ces données soient accessibles à tous, il est ainsi possible de les chiffrer. Le code de déchiffrement devra alors être communiqué dans un autre courrier ou par un autre moyen (SMS, courriel, etc.).

Afin de vous aider pour le chiffrement des données, [vous pouvez consulter les conseils de la CNIL en la matière](#).

Répondre à une demande de droit d'accès

Toute personne peut obtenir

Des informations la concernant, de manière claire :

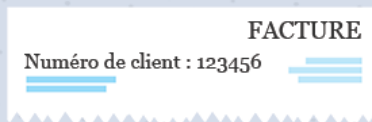
- Quelles données collectées ?
- Quelles durées de conservation ?
- Quels destinataires ?
- etc.



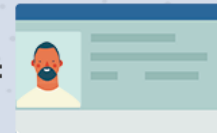
Une copie de ses données, quel que soit leur support de conservation



1 Si nécessaire, vérifiez qui est le demandeur



En cas de doute :



2 Si nécessaire, demandez si la demande concerne

Des données spécifiques



Toutes les données de la personne



3 Vérifiez que la demande ne concerne pas un tiers



Conjoint



Collègue



Secret des affaires



Propriété intellectuelle

4 Répondez à la demande



1 mois max.

Demande simple



8 jours max.

Données de santé



3 mois max.

Demande complexe (par ex. beaucoup de données)



Vous pouvez refuser si

- la demande est infondée ou excessive
- les données ont été effacées



Dans tous les cas, informez la personne sous un mois maximum