RGPD : comment répondre à une demande de droit d’accès ?

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

Toute personne physique qui en fait la demande a le droit d'obtenir la confirmation que des données la concernant sont traitées et peut obtenir la copie de ses données faisant l'objet d'un traitement. Ce droit est renforcé par le Règlement Général sur la Protection des Données (RGPD).
Par exemple, une personne exercer son droit d'accès :
• auprès de son employeur : pour accéder aux données de son dossier personnel ;
• 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 tant que responsable du traitement de données personnelles, vous devez :
• **Informer** les personnes concernées sur l'existence de leur droit d'accès au moment où vous collectez leurs données ;
• **Donner accès aux personnes concernées à des modalités pratiques** (formulaire, coordonnées) pour exercer leur droit d'accès facilement ;
• **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 en interne 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 à ses données personnelles) et du mandataire (son identité). Elle doit justifier de son identité et de celle du demandeur.
Pour les mineurs et les incapables majeurs, ce sont, selon les cas, les parents, le détenteur de l'autorité parentale ou le tuteur qui effectuent la démarche.

Les limites au droit d'accès

Le droit d'accès doit s'exercer dans le **respect du droit des tiers** : par exemple, il n'est pas possible de demander à accéder aux données concernant son conjoint ; un salarié d'une entreprise ne peut obtenir des données relatives à un autre salarié.
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).

Les délais pour répondre à une demande

Actuellement, vous devez répondre dans les **meilleurs délais** à une demande de droit d'accès, dans un délai maximum d'**un mois** (article 12.3). Cependant, 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).

A retenir : que vous répondiez à la demande de droit d'accès ou décidiez de prolonger le délai de deux mois, il vous faudra nécessairement revenir vers 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).

Les 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 pouvez demander le paiement de « frais raisonnables basés sur les coûts administratifs » :
• 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.*

Les modalités de la communication des données

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 appropriée 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 …).*
*Afin de vous aider pour le chiffrement des données, **vous pouvez consulter les conseils de la CNIL en la matière**.*
***Et mon sous-traitant ?** Le règlement prévoit que le sous-traitant aide le responsable de traitement à s'acquitter de ses obligations en matière de droit d'accès (article 28 e). Par exemple : un employeur pourrait demander à son sous-traitant lui ayant fourni un dispositif de géolocalisation, son appui afin de fournir aux employés qui en feraient la demande, des données de géolocalisations « sous une forme accessible » ; lorsque le responsable de traitement ne dispose que d'une analyse des données, il pourrait se rapprocher du sous-traitant qui aurait conservé les données identifiantes.*

Les refus

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 de nouveau communication de ses données auxquelles elle a déjà eu accès ne doit pas être considéré systématiquement comme une demande excessive. En effet, il faut notamment apprécier le délai entre les deux demandes, la possibilité que des nouvelles données aient été collectées 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.*

Accompagnant depuis 2012 de nombreux établissements, Denis JACOPINI, Expert informatique diplômé en cybercriminalité, certifié en gestion des risques sur les systèmes d'information (ISO 27005) et formé par la CNIL depuis 2011 sur une trentaine de thèmes, est en mesure de vous accompagner dans votre démarche de mise en conformité RGPD.

DÉSIGNATION N° DPO-15945

Numéro de formateur 93 84 03041 84 — Liberté • Égalité • Fraternité — RÉPUBLIQUE FRANÇAISE

Datadock — Organisme validé et référencé

Besoin d'un expert pour vous mettre en conformité avec le RGPD ?

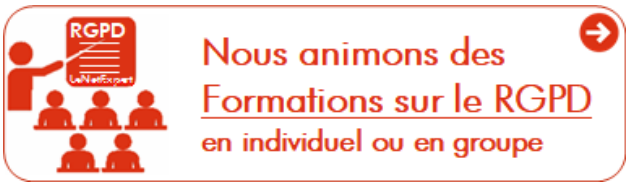
Contactez-nous

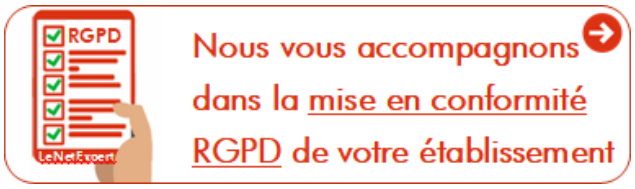
Accompagné de son équipe d'auditeurs et de formateurs, notre Expert, Denis JACOPINI est spécialisé en cybercriminalité et en protection des Données à Caractère Personnel, formateur depuis 1998 et consultant depuis 1996. Avec bientôt une **expérience d'une dizaine d'années** dans la mise en conformité

avec la réglementation relative à la Protection des Données à Caractère Personnel, de formation d'abord technique, Correspondant CNIL en 2012 (CIL : Correspondant Informatique et Libertés) puis en 2018 Délégué à la Protection des Données, en tant que praticien de la mise en conformité et formateur, il lui est ainsi aisé d'accompagner les organismes dans leur démarche de **mise en conformité avec le RGPD**.

« *Mon objectif, vous assurer une démarche de mise en conformité validée par la CNIL.* ».

Nous vous aidons à vous mettre en conformité avec le RGPD de 2 manières :





Quelques articles sélectionnés par nos Experts :

Comment se mettre en conformité avec le RGPD
Accompagnement à la mise en conformité avec le RGPD de votre établissement
Formation RGPD : L'essentiel sur le règlement Européen pour la Protection des Données Personnelles
Comment devenir DPO Délégué à la Protection des Données
Des guides gratuits pour vous aider à vous mettre en conformité avec le RGPD et la CNIL
Mise en conformité RGPD : Mode d'emploi
Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016
DIRECTIVE (UE) 2016/680 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 27 avril 2016
Comprendre le Règlement Européen sur les données personnelles

en 6 étapes
Notre sélection d'articles sur le RGPD (Règlement Européen sur la Protection des données Personnelles) et les DPO (Délégués à la Protection des Données)

[block id="24761" title="Pied de page HAUT"]

Original : *Professionnels : comment répondre à une demande de droit d’accès ? | CNIL*