# Pix+Droit Domaine 3

## Leçon 3.4.2 : 3.4.2. Connaître les droits des personnes sur leurs données personnelles

, Mathieu LE BESCOND DE COATPONT (dir.)

, Aurélien FORTUNATO

, Marcel MORITZ

, Audrey DEQUESNES

## Table des matières




UNJF - Tous droits réservés

# Introduction

**Pour identifier un traitement de données à caractère personnel**, il faut tout d'abord intégrer deux concepts essentiels, tous deux définis dans le règlement européen 2016/679 du 27 avril 2016 (le RGPD) :

- **La donnée à caractère personnel (DACP)** ;
- **Le traitement**.

**- La notion de DACP.**

Selon l'article 2 du RGPD une **donnée à caractère personnel (DACP)** est une **donnée se rapportant à une personne physique identifiée ou identifiable** :

- Information permettant d'identifier directement ou indirectement, **voire simplement de l'individualiser** parmi d'autres.

> ***Exemple***
> Par exemple un nom, un numéro d'identification, une adresse, une photo, une date de naissance, des données de localisation, un identifiant en ligne, un numéro de compte bancaire…

- La notion de « personne physique » exclut les personnes morales (par exemple une société, une association) et les personnes décédées.

***En savoir plus : Approfondissements***

- Lisez le considérant 26 du RGPD.
- Faites quelques recherches sur les travaux de Latanya Sweeney, notamment son célèbre article « *Simple Demographics Often Identify People Uniquely* » (Carnegie Mellon University, *Data Privacy Working Paper 3*. Pittsburgh 2000).
- Cherchez l'avis du G29 05/2014 sur les techniques d'anonymisation (une donnée anonyme ou anonymisée n'est plus une DACP. *A contrario*, une donnée non anonyme ou non anonymisée est une DACP). Quels sont les critères permettant de distinguer donnée anonyme ou anonymisée et, au contraire, DACP ?
- Lisez cette position de la CNIL sur les dispositifs de mesure d'audience. Qu'en déduisez-vous ?

***En savoir plus : Réponse***

- La notion de DACP est très large.
- Les données pseudonymisées restent des DACP.
- Une donnée ne doit pas être prise isolément mais analysée au regard des autres données disponibles (exemple du genre dans l'expérience de L. Sweeney).
- Les possibilités de réidentification sont nombreuses.
- Une donnée simplement individualisante est une DACP (donc même si on ne peut pas connaître l'identité de l'individu, mais qu'on est capable de le suivre, de le profiler). C'est une différence entre la DACP et les « informations nominatives » (terme initialement employé par la loi « informatique et libertés » de 1978).

**- Les DACP dites « sensibles ».**

Certaines DACP engendrent des risques spécifiques et constituent des catégories particulières de données, qui sont traitées avec des contraintes juridiques particulières. Ce sont des données dites "sensibles" :

- Les données révélant une **origine raciale ou ethnique**.
- Les données relatives aux **opinions politiques, philosophiques ou religieuses**.


UNJF - Tous droits réservés

- L'appartenance **syndicale**.
- Les **données de santé** ou révélant l'**orientation sexuelle**.
- Les données **génétiques ou biométriques**.
- Les données concernant les **infractions** et les **condamnations pénales**.

Ces DACP sensibles sont soumises à l'article 9 du RGPD.

Elles ne sont normalement pas susceptibles d'être traitées sauf dans les cas prévus par le texte (dont le consentement explicite de la personne pour une ou plusieurs finalités spécifiques, ou encore si « *le traitement est nécessaire pour des motifs d'intérêt public important* »).

Nous pouvons aussi distinguer les données concernant les **infractions** et les **condamnations pénales**, qui ne peuvent être traitées que sous contrôle de l'autorité publique, ou dans des conditions particulières (article 10).

**- La notion de traitement.**

Le traitement englobe « *toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel* » :

- La collecte, l'enregistrement ;
- L'organisation, la structuration, la conservation ;
- La modification, l'extraction, la consultation, l'utilisation, le rapprochement ou l'interconnexion ;
- La communication par transmission, la diffusion, la mise à disposition ;
- La limitation, l'effacement ou la destruction .


UNJF - Tous droits réservés

# 1. Le RGPD : quelle (r)évolution ?

Il s'agit du Règlement Général sur la Protection des Données, ou Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016.
C'est un règlement européen, donc un outil puissant d'harmonisation du droit au sein de l'ensemble des pays de l'UE.

> ***En savoir plus : Définition du règlement européen***
> Pour en savoir plus, consultez le site EUR-Lex sur le règlement de l'Union européenne.

Il est entré en application dans les pays de l'Union européenne le 25 mai 2018.

Aussi appelé GDPR pour l'anglais « *General Data Protection Regulation* ».

Il est possible de le consulter par exemple sur EUR-Lex, ou sur le site de la CNIL.

# Une exclusivité de la LIL : les directives anticipées

**Attention** : certains (rares) éléments de la loi française « informatique et libertés » complètent le RGPD.

> ***Exemple***
> En France, il existe depuis la loi n° 2016-1321 du 7 octobre 2016 (loi pour une République numérique) un droit à donner des directives sur le sort *post mortem* de ses DACP.
> Ce droit, qui figure à l'article 85 de la LIL, est absent du RGPD. Il est possible de définir des directives relatives à la conservation, à l'effacement et à la communication de ses données à caractère personnel après son décès.
> Ces directives peuvent concerner :
> - l'ensemble des DACP de la personne et être inscrites sur un registre unique,
> - ou des DACP mentionnées, enregistrées auprès des responsables de traitement concernés.

> ***En savoir plus : Mort numérique***
> Voir « Mort numérique : peut-on demander l'effacement des informations d'une personne décédée ? », 28 octobre 2020, accessible sur le site de la CNIL.

# Le RGPD : une uniformisation à l'échelle européenne

Il renforce les droits des personnes se trouvant en Europe et leur en octroie de nouveaux, pour leur permettre mieux contrôler leurs données personnelles.

Il s'applique à toutes les entreprises, leurs sous-traitants, les organismes publics et associations, qui sont sur le territoire de l'UE, mais aussi à ceux qui sont en dehors de l'UE mais qui :

1. offrent des biens ou des services à aux personnes situées dans l'Union,
2. suivent le comportement de personnes, dans la mesure où il s'agit d'un comportement qui a lieu au sein de l'Union.

C'est un enjeu politique majeur car cela signifie que de très nombreuses entreprises étrangères dont le siège est hors de l'UE sont soumises au RGPD.


UNJF - Tous droits réservés

> ***Exemple***
> Par exemple une entreprise malgache qui fait de la prospection téléphonique vers la France (il y a de nombreux centres d'appel à Madagascar) est soumise au RGPD : elle offre des biens ou des services aux personnes situées dans l'Union.

# Le RGPD : quelles évolutions par rapport à la LIL ?

Pour les personnes, le RGPD apporte :

- **Un consentement renforcé.**
  - Les données collectées et la façon dont elles seront traitées sont explicitement exposées à la personne concernée. Le consentement doit pouvoir être librement révoqué.
  - Certains traitements peuvent toutefois reposer sur une base légale autre que le consentement.

> ***En savoir plus : Les bases légales***
> Consultez le site de la CNIL sur les bases légales.

- De **nouveaux droits**, qui seront détaillés en troisième partie « Les droits nouveaux portés par le RGPD ».

Un **accompagnement**, mais aussi des **sanctions** renforcées :

- En accompagnant les organismes qui traitent des données, et grâce à la nomination de délégués à la protection des données, la CNIL renforce l'application de la loi et des bonnes pratiques.
- A l'issue de contrôle ou de plaintes, en cas de manquements, la CNIL peut aller jusqu'à prononcer des sanctions à l'égard des responsables de traitements qui ne respecteraient pas la loi. Avec le RGPD le montant des sanctions pécuniaires peut s'élever jusqu'à **20 millions d'euros** ou dans le cas d'une entreprise jusqu'à **4 % du chiffre d'affaires annuel mondial**.

> ***En savoir plus : Exemples de sanctions prononcées par la CNIL et ses équivalents dans l'UE***
> Certaines sanctions prononcées par la CNIL et ses équivalents dans l'UE sont rendues publiques. Exemples :
>
> - La CNIL prononce dix nouvelles sanctions dans le cadre de sa procédure simplifiée, 7 novembre 2023 ;
> - Prospection commerciale et droits des personnes : sanction de 600 000 euros à l'encontre du GROUPE CANAL+, 19 octobre 2023 ;
> - L'autorité luxembourgeoise de protection des données a prononcé à l'encontre d'Amazon Europe Core une amende de 746 millions d'euros.


UNJF - Tous droits réservés

# 2. Les droits « historiques » des personnes sur les traitements de leurs DACP

En pratique, de nombreux droits prévus par le RGPD préexistaient déjà en France, dans la loi de 1978 :

- **Droit d'accès et de communication**.
- **Droit de rectification**.
- **Droit d'opposition**.
- **Droit à l'effacement**.

Les droits présents dans la LIL dès 1978, et qui se retrouvent dans le RGPD :

| | | |
|---|---|---|
| **Droit d'accès** | Article 15 | Permet d'accéder à la liste des DACP traitées, aux finalités, et aux destinataires, mais aussi d'obtenir une copie de toutes ces données. |
| **Droit de rectification** | Article 16 | Permet de faire rectifier des données inexactes ou de compléter des informations. |


UNJF - Tous droits réservés

| | | |
|---|---|---|
| **Droit à l'effacement** | Article 17 | Permet de faire effacer des données si :<br>• elles ne sont plus nécessaires,<br>• le consentement est retiré,<br>• elles ont été traitées de façon illicite,<br>• elles concernent un mineur,<br>• elles doivent être effacées pour respecter une obligation légale,<br>• il s'agit d'un traitement relevant de l'exercice de l'autorité publique, et qu'il n'y a pas de motif légitime impérieux pour ce traitement (art. 21-1) ou lorsque les données sont recueillies à des fins de prospection.<br>Ne s'applique pas si le traitement est nécessaire :<br>• à la liberté d'expression ou d'information,<br>• au respect d'une obligation légale,<br>• à la santé publique,<br>• à des fins de recherche scientifique, historique ou statistiques,<br>• à la constatation, à l'exercice ou à la défense des droits en justice. |
| **Droit d'opposition** | Article 21 | Permet de s'opposer à tout moment au traitement de données fondé sur la nécessité pour l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique, ou sur la base de l'intérêt légitime, à moins que le responsable de traitement ne démontre que son motif légitime prévaut sur les intérêts et les droits et libertés de la personne. |


UNJF - Tous droits réservés

# 3. Les droits nouveaux portés par le RGPD

- **Droit à la portabilité** : chacun pouvait déjà obtenir communication de ses données collectées, connaître le but de leur traitement, et maintenant il peut aussi demander à les exporter vers un autre service.
- **Droit à la limitation** : il est possible de demander la limitation d'un traitement, c'est-à-dire son arrêt temporaire, par exemple si les données concernant la personne sont inexactes.
- **Droit au refus du profilage** : il est possible de s'opposer au profilage à des fins de prospection, ou à une décision prise entièrement de façon automatisée.
- Droit à l'effacement (ou « droit à l'oubli »), qui existait déjà dans la loi « informatique et libertés » de 1978, est élargi avec le **droit au déréférencement** : il est possible, sous conditions, de demander l'effacement de DACP, et de solliciter d'un moteur de recherche qu'il ne présente plus un résultat de recherche qui porte préjudice à la personne concernée.

| | | |
|---|---|---|
| **Droit d'information** | Article 13 | Permet d'obtenir une information claire sur l'utilisation des données et sur l'exercice des droits. |
| **Droit à la limitation du traitement** | Article 18 | Permet d'arrêter momentanément un traitement lorsque l'on conteste l'exactitude des données, ou définitivement si le traitement est illicite mais que la personne souhaite que ses données ne soit pas effacées, par exemple pour faire valoir ses droits en justice. Lorsqu'il s'agit d'un traitement relevant de l'exercice de l'autorité publique, le traitement peut être limité durant le temps de la vérification de la légitimité du motif. |
| **Droit à la portabilité des données** | Article 20 | Une personne peut obtenir ses données dans un format structuré qu'elle pourra transmettre à un autre responsable de traitement, si ses données ont été collectées sur la base du consentement, et que le traitement est effectué à l'aide de procédés automatisés. Elle peut demander le transfert de ses données directement à un autre responsable de traitement, par exemple une entreprise qui propose un service équivalent. |
| **Droit opposition** | Article 21 | Permet de s'opposer à tout moment au traitement |


UNJF - Tous droits réservés

| | | |
|---|---|---|
| | | de données fondé sur la nécessité pour l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique, ou sur la base de l'intérêt légitime, à moins que le responsable de traitement ne démontre que son motif légitime prévaut sur les intérêts et les droits et libertés de la personne. |
| **Opposition à la décision individuelle automatisée et au profilage** | Article 22 | Permet à la personne de ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé, y compris le profilage, produisant des effets juridiques la concernant ou l'affectant de manière significative.<br>Si la base légale est le contrat ou le consentement, le responsable de traitement doit au moins donner à la personne le droit à une intervention humaine, à l'expression de son point de vue, et à contester la décision.<br>Aucune de ces décisions ne peut être fondée sur des catégories particulières de DACP (origine raciale, ethnique, opinions, santé, sexualité...), à moins que la personne ait donné sont consentement explicite pour ce traitement, ou qu'il soit nécessaire à des motifs « d'intérêt public important ». |

**Sur le droit au déréférencement.**

Ce droit découle du « Droit à l'oubli », à l'article 17 du RGPD. Il a été consacré par l'arrêt « Google Spain » de la CJUE duquel on tire deux enseignements majeurs :

- Les activités des moteurs de recherches sont des traitements de données à caractère personnel.
- Ils doivent donc permettre à la personne concernée de faire supprimer les données qu'elle ne souhaite pas voir apparaitre (sous réserve de remplir les conditions citées à l'article 17 du RGPD).

Si la CNIL avait d'abord prêté à ce droit une portée mondiale, cette interprétation a été invalidée par l'arrêt de la CJUE du 24 septembre 2019 et la décision du Conseil d'Etat du 27 mars 2020, qui réduisent la portée de ce droit au territoire européen.

Le **droit au déréférencement** permet donc de dissimuler un contenu dans les résultats d'une recherche. C'est très utile si ce résultat porte préjudice à la personne ! Mais il suffit de changer de moteur de recherche ou d'effectuer la recherche en dehors du territoire où le déréférencement s'applique (physiquement ou virtuellement à travers un VPN) pour que le résultat apparaisse de nouveau.

La CNIL donne toutes les informations pour exercer ce droit.


UNJF - Tous droits réservés

**Sur le droit au refus du profilage.**
Le RGPD vise à limiter les risques des conséquences négatives du profilage des personnes, tels que les analyses et prédictions inexactes, les refus de services injustifiés ou autres décisions défavorables aux personnes, la perpétuation des stéréotypes et l'enfermement des personnes dans leurs choix.

Le profilage y est défini a l'article 4 comme « *toute forme de traitement automatisé de données à caractère personnel consistant à utiliser ces données à caractère personnel pour évaluer certains aspects personnels relatifs à une personne physique, notamment pour analyser ou prédire des éléments concernant le rendement au travail, la situation économique, la santé, les préférences personnelles, les intérêts, la fiabilité, le comportement, la localisation ou les déplacements de cette personne physique* ».

Il peut être utilisé dans la vie quotidienne à des fins très variées. Une personne a le droit de ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé, conformément à l'article 22 §1 du RGPD, y compris le profilage, lorsque cette décision produit des effets juridiques ou l'affecte de manière significative.

***En savoir plus : Pour mieux connaître vos droits face au profilage***
Voir « Vos droits à l'intervention humaine face à votre profilage ou à une décision automatisée » accessible sur le site de la CNIL.

Le profilage est entendu comme un traitement individualisé : les traitements statistiques ou à l'échelle d'un groupe n'en font donc pas partie.

De la même façon, le paragraphe 1 de l'article 22 « *ne s'applique pas lorsque la décision* :

- *est nécessaire à la conclusion ou à l'exécution d'un contrat entre la personne concernée et un responsable du traitement ;*
- *est autorisée par le droit de l'Union ou le droit de l'État membre auquel le responsable du traitement est soumis et qui prévoit également des mesures appropriées pour la sauvegarde des droits et libertés et des intérêts légitimes de la personne concernée ; ou*
- *est fondée sur le consentement explicite de la personne concernée.* »

Dans ces trois cas, les décisions **ne peuvent être fondées sur une catégorie particulière de DACP** (les données dites « sensibles »), sauf si la personne a donné son **consentement**, ou en cas de nécessité pour **motif d'intérêt public important**.
Dans le premier et le troisième cas, le responsable de traitement garantit au moins le droit de la personne concernée d'obtenir une intervention humaine de la part du responsable du traitement, d'exprimer son point de vue et de contester la décision.

Cependant, profilage et décision automatisée ne sont pas synonymes : une décision entièrement automatisée est une décision qui a été prise par un algorithme, sans aucune intervention humaine. Elle peut découler d'un profilage, mais ce n'est pas systématique : cette décision peut être prise sans qu'un profil ait été construit au préalable.

***En savoir plus : Pour en savoir plus sur ce type de décision***
Consultez :

- « Profilage et décision entièrement automatisée », 29 mai 2018, accessible sur le site de la CNIL
- et l'avis du G29 sur ce sujet.


UNJF - Tous droits réservés

# Conclusion / Pour aller plus loin

La loi « informatique et libertés » de 1978 garantissait déjà des **droits essentiels** aux personnes sur leurs données à caractère personnel. Pour faire face aux **évolutions des pratiques et des technologies**, ces droits ont été **repris** et parfois **améliorés** dans le RGPD, et de **nouveaux** ont été créés.

Ces droits sont à mettre en relation avec les grands principes du RGPD mais aussi avec les obligations des responsables de traitement, dans le module 4.1.1.

**Les nouveaux règlements européens sur le numérique.**
Ces dernières années, de nombreuses propositions de réglementation du marché en ligne, des services en ligne, du partage des données, de la cybersécurité ou encore de l'intelligence artificielle ont vu le jour, et une partie a déjà été adoptée.

- Le Règlement sur les services numériques (DSA) vise entres autres à améliorer la transparence des grands services en ligne, et à lutter contre les contenus et produits illicites, et la désinformation.
- Le Règlement sur les marchés numériques (DMA) régule principalement la concurrence et les pouvoirs des géants du numérique. Concernant la vie privée, il impose un consentement explicite pour la diffusion de publicité ciblée.
- Le Règlement sur la gouvernance des données (DGA) donne les règles du partage et de la réutilisation des données non-personnelles.
- Le Règlement sur l'équité de l'accès aux données (*Data Act*) établit un cadre pour la réutilisation des données, personnelles et non-personnelles, notamment générées par l'utilisation d'objets connectés.

En cas de conflit entre les textes, il est spécifié, à la demande des autorités européennes de protection des données, que le RGPD prévaudrait sur le DGA, et que le Data Act s'appliquait sans préjudice du RGPD.

***En savoir plus : Exercer ses droits en pratique***
La CNIL propose sur son site internet des cas pratiques et toutes les informations nécessaires pour l'exercice des droits des personnes.

Elle propose également des formulaires très utiles pour créer des courriers personnalisés afin d'exercer ces droits.

Les principaux droits des personnes sont rappelés dans le tableau suivant.

| | | |
|---|---|---|
| **Droit d'accès** | Article 15 | Permet d'accéder à la liste des DACP traitées, aux finalités, et aux destinataires, mais aussi d'obtenir une copie de toutes ces données. |
| **Droit de rectification** | Article 16 | Permet de faire rectifier des données inexactes ou de compléter des informations. |


UNJF - Tous droits réservés

| | | |
|---|---|---|
| **Droit à l'effacement** | Article 17 | Permet de faire effacer des données si :<br>• elles ne sont plus nécessaires,<br>• le consentement est retiré,<br>• elles ont été traitées de façon illicite,<br>• elles concernent un mineur,<br>• elles doivent être effacées pour respecter une obligation légale,<br>• il s'agit d'un traitement relevant de l'exercice de l'autorité publique, et qu'il n'y a pas de motif légitime impérieux pour ce traitement (art. 21-1) ou lorsque les données sont recueillies à des fins de prospection.<br>Ne s'applique pas si le traitement est nécessaire :<br>• à la liberté d'expression ou d'information,<br>• au respect d'une obligation légale,<br>• à la santé publique,<br>• à des fins de recherche scientifique, historique ou statistiques,<br>• à la constatation, à l'exercice ou à la défense des droits en justice. |


UNJF - Tous droits réservés

| | | |
|---|---|---|
| **Droit à la limitation du traitement** | Article 18 | Permet d'arrêter momentanément un traitement lorsque l'on conteste l'exactitude des données, ou définitivement si le traitement est illicite mais que la personne souhaite que ses données ne soit pas effacées, par exemple pour faire valoir ses droits en justice. Lorsqu'il s'agit d'un traitement relevant de l'exercice de l'autorité publique, le traitement peut être limité durant le temps de la vérification de la légitimité du motif. |
| **Droit à la portabilité des données** | Article 20 | Une personne peut obtenir ses données dans un format structuré qu'elle pourra transmettre à un autre responsable de traitement, si ses données ont été collectées sur la base du consentement, et que le traitement est effectué à l'aide de procédés automatisés. Elle peut demander le transfert de ses données directement à un autre responsable de traitement, par exemple une entreprise qui propose un service équivalent. |
| **Droit opposition** | Article 21 | Permet de s'opposer à tout moment au traitement de données fondé sur la nécessité pour l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique, ou sur la base de l'intérêt légitime, à moins que le responsable de traitement ne démontre que son motif légitime prévaut sur les intérêts et les droits et libertés de la personne. |


UNJF - Tous droits réservés

| | | |
|---|---|---|
| **Opposition à la décision individuelle automatisée et au profilage** | Article 22 | Permet à la personne de ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé, y compris le profilage, produisant des effets juridiques la concernant ou l'affectant de manière significative.<br>Si la base légale est le contrat ou le consentement, le responsable de traitement doit au moins donner à la personne le droit à une intervention humaine, à l'expression de son point de vue, et à contester la décision.<br>Aucune de ces décisions ne peut être fondée sur des catégories particulières de DACP (origine raciale, ethnique, opinions, santé, sexualité...), à moins que la personne ait donné sont consentement explicite pour ce traitement, ou qu'il soit nécessaire à des motifs « d'intérêt public important ». |

**Sur le RGPD : 8 principes fondamentaux relatifs au traitement des DACP**.

**Sur la base légale et le consentement.**
Comme indiqué précédemment, tout traitement de DACP doit reposer sur une base légale.
Il s'agit souvent (mais pas toujours) du consentement de la personne concernée par le traitement : il existe 6 bases légales pour traiter des DACP.

- **La base légale :**
  - Le **consentement**.

    > ***Exemple***
    > Faire partie d'une base de données de clients et recevoir de la prospection commerciale.

  - L'**intérêt légitime** du responsable de traitement.

    > ***Exemple***
    > Garantir la sécurité du réseau et des informations.

  - Le traitement est nécessaire à l'exécution d'un **contrat**.

    > ***Exemple***
    > Collecter l'adresse postale pour assurer une livraison.

  - Le traitement est nécessaire au respect d'une **obligation légale**.

    > ***Exemple***
    > Transmettre les revenus d'un salarié aux autorités fiscales pour le calcul de l'impôt.

  - Le traitement est nécessaire à la **sauvegarde des intérêts vitaux** de la personne ou d'une autre personne physique.


UNJF - Tous droits réservés

> ***Exemple***
> Accident, intervention des secours.

- Le traitement est nécessaire à l'**intérêt public**. La mission d'intérêt public doit être définie dans des dispositions légales pour fonder ces traitements.

> ***En savoir plus : Pour en savoir plus sur les bases légales***
> Consultez le site de la CNIL sur les bases légales.

- **Le consentement :**
  - Il doit être **libre et éclairé** : aucune contrainte ne doit forcer à accepter ce traitement, il doit être demandé assez clairement pour que les personnes comprennent le traitement qui sera fait de leurs données, par qui et à quelles fins.
  - Il est accordé pour une finalité **spécifique**. Si le traitement comporte plusieurs finalités, les personnes doivent pouvoir choisir indépendamment les finalités pour lesquelles elles consentent.
  - Il peut être **retiré** aussi simplement qu'il a été donné, à tout moment.
  - Il doit être **univoque**. Il est recueilli par un moyen qui ne laisse pas d'ambiguïté : une case à cocher qui n'est pas pré-cochée, une ligne manuscrite, etc.
  - Il est accordé conjointement par l'enfant et par les parents pour les **mineurs** de moins de 15 ans, en France. Cet âge peut être compris entre 13 et 16 ans dans les autres États membres de l'UE.

**Sur les obligations des responsables de traitement pour garantir l'exercice effectif des droits des personnes.**

Les personnes dont les données sont traitées disposent de droits :

- Le responsable du traitement doit les **informer** de ces droits .
- Il doit leur expliquer **comment exercer leurs droits**, et donner accès à des **modalités pratiques**, par exemple en leur fournissant un formulaire ou une adresse à contacter.
- Il doit mettre en place un **parcours interne efficace** pour le traitement des demandes de droit d'accès, afin d'être en mesure de traiter la demande dans les délais impartis .
- Le responsable de traitement a un mois pour donner une **réponse** à la personne.
- Il doit prévoir des **modalités de réponse** auprès des personnes concernées qui soient compréhensibles, accessibles, formulées en des termes clairs et simples.
- Il doit aussi prévenir les destinataires à qui il a transmis les données, afin qu'elles puissent être effacées, rectifiées, ou les traitements limités.
- La personne qui veut exercer ses droits doit en **faire la demande** et justifier de don identité. Elle peut donner mandat.
- Ce sont **les parents ou les tuteurs** qui peuvent faire ces demandes pour les mineurs et incapables majeurs.


UNJF - Tous droits réservés