



La gestion des droits relatifs aux données personnellesRGPD : articles types à intégrer dans la charte informatique

Rédigé Par:

**Sébastien CLAUDE**

Délégué à la protection des données

***Date de publication: 05/09/2018***

|  |
| --- |
| **Historique** |
| Version | Date de modification | Champ des modifications |
| 01 | 05/09/2018 | Création  |
|  |  |  |

|  |
| --- |
| **Légitimité** |
| **Rédigé par :** Le  | **Validé par :** Le :  | **Vérifié par :** Mr S. CLAUDE, Dirigeant ASC2SILe :  | **Approuvé par :**Le : |

Sommaire

[I . Description du document 3](#_Toc523929358)

[II . Rappel sur les droits des individus 3](#_Toc523929359)

[1 ) Le droit à l’information 3](#_Toc523929360)

[2 ) Le recueil du consentement 3](#_Toc523929361)

[3 ) Le droit d’opposition 4](#_Toc523929362)

[4 ) Les droits d’accès et de rectification 4](#_Toc523929363)

[5 ) Comment présenter les données ? 5](#_Toc523929364)

[6 ) Les limites au droit d’accès 5](#_Toc523929365)

[7 ) Concrètement, comment faire ? 6](#_Toc523929366)

[III . Organisation pratique 6](#_Toc523929367)

[1 ) Les étapes essentielles du traitement d’une demande 6](#_Toc523929368)

[2 ) La gouvernance du dispositif 7](#_Toc523929369)

[3 ) Les moyens techniques susceptibles de vous aider 8](#_Toc523929370)

# Description du document

Le présent document décrit l’organisation à mettre place pour permettre aux demandeurs d’exercer leurs droits relatifs au RGPD. Il a été élaboré à partir des documents suivants :

 • <https://www.cnil.fr/fr/respecter-les-droits-des-personnes> ; CNIL

# Rappel sur les droits des individus

L’enjeu de ce document est de mettre en place au sein de l’organisme une organisation qui va permettre de respecter les délais définis par le RGPD au regard des droits suivants :

## Le droit à l’information

Pour être loyale et licite, la collecte de données personnelles doit s’accompagner d’une information claire et précise des personnes sur :

* l’identité du responsable du traitement ;
* la finalité du traitement ;
* le caractère obligatoire ou facultatif des réponses et des conséquences d’un défaut de réponse ;
* les destinataires des données ;
* leurs droits relatifs au traitement considéré (droit d’accès, de rectification, et d’opposition) ;
* les éventuels transferts de données vers des pays hors UE.

L’information est préalable à la collecte des données. Le support de cette information varie en fonction des caractéristiques du traitement (exemple, panneau d’information pour une vidéosurveillance, mention d’information sur un formulaire, lecture de cette information en cas de recueil de données par téléphone.)

## Le recueil du consentement

Le consentement est une démarche active de l’utilisateur, explicite et de préférence écrite, qui doit être libre, spécifique, et informée. Dans un formulaire en ligne, il peut se matérialiser, par exemple, par une case à cocher non cochée par défaut.

Le consentement est "préalable" à la collecte des données. Le consentement préalable de la personne concernée est notamment requis :

* En cas de collecte de données sensibles
* De réutilisation des données à d’autres fins
* D'utilisation de cookies pour certaines finalités
* D'utilisation des données à des fins de prospection commerciale par voie électronique.

## Le droit d’opposition

Les personnes doivent pouvoir s’opposer à la réutilisation par le responsable du traitement de leurs coordonnées à des fins de sollicitations, notamment commerciales, lors d’une commande ou de la signature d’un contrat. Une case à cocher, non cochée par défaut !, doit leur permettre d’exprimer leur choix directement sur le formulaire ou le bon de commande à remplir. La simple mention de l’existence de ce droit dans les conditions générales n’est pas suffisante.

Toute personne a le droit de s’opposer, pour des motifs légitimes, au traitement de ses données, sauf si celui-ci répond à une obligation légale (ex : fichiers des impôts).

## Les droits d’accès et de rectification

Toute personne peut :

* accéder à l’ensemble des informations la concernant => il s’agit du droit d’accès,
* connaître l’origine des informations le concernant,
* accéder aux informations sur lesquelles le responsable du fichier s’est fondé pour prendre une décision le concernant (par exemple, les éléments qui auraient servi pour ne pas vous accorder une promotion ou le score attribué par une banque et qui a conduit au rejet de votre demande de crédit),
* en obtenir la copie, (des frais n’excédant pas le coût de la reproduction peuvent être demandés) => c’est le droit à la portabilité
* exiger que ses données soient, selon les cas, rectifiées, complétées, mises à jour=> il s’agit du droit à la rectification
* demander la suppression de ses informations => le droit à l’oubli

Le droit d’accès peut s’exercer :

* Par écrit : courrier postal, accompagné d’une copie d’une pièce d’identité. Idéalement, en recommandé avec accusé de réception
* Sur place : avec présentation d'une pièce d’identité. Il est possible de se faire accompagner par la personne de son choix. La consultation doit durer suffisamment longtemps pour prendre note commodément et complètement. Il est possible de demander une copie des données.

Le responsable du traitement dispose d’un délai de réponse de 1 mois à compter de la date de réception de la demande. Ce délai peut être porté à 2 mois si le nombre de demandes à traiter est important ou si la complexité à lui fournir l’information le justifie.

Si la demande exercée sur place ne peut être satisfaite immédiatement, un avis de réception daté et signé doit être remis au demandeur.

Si la demande est incomplète (absence de la pièce d’identité par exemple), le responsable du traitement est en droit de demander des compléments : le délai est alors suspendu et courre à nouveau une fois ces éléments fournis.

## Comment présenter les données ?

Les éléments communiqués doivent être aisément compréhensibles. Les codes, les sigles et les abréviations utilisés doivent être expliqués (éventuellement par le biais d’un lexique).

Par exemple, « Segmentation : A+ » signifie que vous êtes considéré comme un client VIP

## Les limites au droit d’accès

Le responsable du traitement peut :

* refuser la demande d’accès : dans ce cas, il doit motiver sa décision et informer le demandeur des voies et délais de recours permettant de la contester.
* Ne pas répondre aux demandes qui sont manifestement abusives notamment par leur nombre, leur caractère répétitif ou systématique (par exemple, demande d’une copie intégrale d’un enregistrement toutes les semaines).

Lorsque le responsable de traitement ne dispose d’aucune donnée sur la personne qui exerce son droit d’accès (ex : les données ont été supprimées ou l’organisme ne dispose d’aucune donnée sur la personne), il doit néanmoins répondre au demandeur dans le délai de 1 mois.

Le droit d’accès doit s’exercer dans le respect du droit des tiers : un salarié d’une entreprise ne peut obtenir des données relatives à un autre salarié.

Les valeurs de classement annuel ou de potentiel de carrière sont communicables lorsqu’elles ont servi à prendre une décision. L’employeur n’est pas tenu de les communiquer lorsqu’elles sont encore prévisionnelles.

## Concrètement, comment faire ?

* Mettre en place une organisation chargée de traiter les demandes informatique et libertés.
* Contacter le DPD si l'organisme concerné en a désigné un
* Surveiller les délais de réponses

# Organisation pratique

## Les étapes essentielles du traitement d’une demande

**Recevoir une demande :** il est préconisé de mettre à disposition de l’usager un moyen permettant de cadrer sa demande : formulaire en ligne ou papier.

**Valider la demande**: il est indispensable de s ‘assurer que tous les éléments nécessaires ont été recueillis pour permettre au responsable de Traitement de fournir les éléments de réponses. Pour cela vérifier l’identité du demandeur et sa légitimité. En notifier systématiquement, la prise en compte ou lui demander des informations complémentaires. Si la demande est incomplète : les délais de réponse sont suspendu en attendant que la personne est fournie les éléments manquants.

**Transmettre au responsable de traitement** : c’est le RT qui est chargé de fournir à l’usager les informations demandées. Dans le cas d’un droit à la rectification ou à l’oubli il se chargera également de fournir la preuve que la demande a été exécutée.

**Effectuer le suivi et l’avancement des demandes** : Pour tenir les délais imposés par le RGPD il convient de tenir un tableau de bord avec l’ensemble des demandes et l’information permettant de calculer les indicateurs de retard, d’avancement, statuts,..

Notifier la fin de la demande et informé l’usager : une fois la demande effectuée il conviendra de la clôturer et d’informer la personne de la durée de conservation des informations relatives à cette demande.



## La gouvernance du dispositif

L’ensemble de ce dispositif se doit d’être piloté par une personne unique. Si l’organisme a désigné un DPD, il est le plus qualifié pour cette tâche.

Il se chargera de :

* centraliser et dispatcher les demandes aux RT
* suivre l’avancement des différentes demandes
* notifier l’usager de l’avancement de celle-ci
* relancer les RT en cas de besoin
* tenir à jour le tableau de bord de pilotage du dispositif
* diffuser les informations aux dirigeants de l’organisme

## Les moyens techniques susceptibles de vous aider

Afin de mettre en place un dispositif le plus efficient possible il conviendra d’utiliser les outils suivants

* un formulaire en ligne permettant à l’usager de faire une demande. Ce formulaire contiendra à minima les éléments suivant : identité de la personne (avec un moyen d’en faire la preuve : copie de CI à fournir en PJ mais qui ne sera pas conservée après que la demande soit qualifiée), moyen de contacter la personne (mail, téléphone,..), le contexte considéré (par exemple une correspondance avec la liste des traitements), la typologie de droit exercé, un champ de description.
* Un formulaire papier avec les informations identiques à celle du formulaire en ligne.
* Un tableau de bord de suivi des demandes (à minima un fichier Excel avec les informations permettant le suivi des demandes.
* Un workflow automatisé intégrant des dispositifs de transfert des demandes en fonction du contexte sélectionné par l’usager. Ainsi que des notifications et rappels automatiques.

Vous pouvez vous référer au conseil de la CNIL pour des éléments plus techniques : <https://www.cnil.fr/fr/webmaster-ou-responsables-de-sites-comment-repondre-aux-demandes-deffacement-de-donnees-personnelles>