



Contrat d’engagement du responsable de traitementRGPD : 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 :**  Mr S. CLAUDE,  DPD GHT  Le | **Validé par :**  Le : | **Vérifié par :**  Mr S. CLAUDE,  DPD GHT  Le : | **Approuvé par :**  Le : |

Sommaire

[05/09/2018 2](#_Toc523926922)

[I . Description du document 4](#_Toc523926923)

[II . Les définitions essentiels 4](#_Toc523926924)

[1 ) Qu'est-ce qu'une donnée personnelle ? 4](#_Toc523926925)

[2 ) Qu’est-ce qu’un traitement de données personnelles ? 4](#_Toc523926926)

[III . Les obligations du responsable de traitement 5](#_Toc523926927)

[IV . Lettre d’engagement type 7](#_Toc523926928)

# Description du document

Le présent document a pour but de rappeler aux responsables de traitement de données à caractère personnel (DCP) leurs obligations au regard du règlement général de protection des données et d’engager l’organisme dans une démarche qualité dans la gestion de ces DCP aux regards des individus. Il a été élaboré à partir des documents suivants :

• <https://www.cnil.fr/fr/rgpd-de-quoi-parle-t-on>  ; CNIL

# Les définitions essentiels

## Qu'est-ce qu'une donnée personnelle ?

La notion de « données personnelles » est à comprendre de façon très large. Une « donnée personnelle » est « toute information se rapportant à une personne physique identifiée ou identifiable ».

Une personne peut être identifiée :

* directement (exemple : nom, prénom)
* ou indirectement (exemple : par un identifiant (n° client), un numéro (de téléphone), une donnée biométrique, plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale, mais aussi la voix ou l’image).

L’identification d’une personne physique peut être réalisée :

* à partir d’une seule donnée (exemple : numéro de sécurité sociale, ADN)
* à partir du croisement d’un ensemble de données (exemple : une femme vivant à telle adresse, née tel jour, abonnée à tel magazine et militant dans telle association)

Exemple : une base marketing contenant de nombreuses informations précises sur la localisation, l’âge, les goûts et les comportements d’achats de consommateurs, y-compris si leur nom n’est pas stocké, est considérée comme un traitement de données personnelles, dès lors qu’il est possible de remonter à une personne physique déterminée en se basant sur ces informations.

## Qu’est-ce qu’un traitement de données personnelles ?

Un « traitement de données personnelles » est une opération, ou ensemble d'opérations, portant sur des données personnelles, quel que soit le procédé utilisé (collecte, enregistrement, organisation, conservation, adaptation, modification, extraction, consultation, utilisation, communication par transmission diffusion ou toute autre forme de mise à disposition, rapprochement).

Exemple : tenue d’un fichier de ses clients, collecte de coordonnées de prospects via un questionnaire, mise à jour d’un fichier de fournisseurs, etc.

Par contre, un fichier ne contenant que des coordonnées d’entreprises (par exemple, entreprise « Compagnie A » avec son adresse postale, le numéro de téléphone de son standard et un email de contact générique « compagnieA@email.fr ») n’est pas un traitement de données personnelles.

Un traitement de données personnelles n’est pas nécessairement informatisé : les fichiers papier sont également concernés et doivent être protégés dans les mêmes conditions.

# Les obligations du responsable de traitement

Le responsable est la personne qui définit la finalité d’un traitement de données à caractère personnel. C’est donc à ce titre qu’il est responsable des moyens mis en œuvre pour assurer la sécurité des DCP utilisé ainsi que de la possibilité des personnes d’exercer leurs droits. Ces obligations sont donc les suivantes :

* Informer les personnes :
* justifier de la licéité du traitement : il n’est licite que si l’une des conditions suivantes est remplie :
  + la personne a donné son consentement,
  + il est nécessaire au regard de l’exécution d’un contrat,
  + ce traitement est nécessaire pour le respect d’une obligation légale,
  + il permet la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne physique;
  + il s’agit d’une mission d'intérêt public ou relevant de l'exercice de l'autorité publique
  + le traitement est nécessaire aux fins des intérêts légitimes poursuivis par le responsable du traitement (non valable pour une autorité publique)
* recueillir le consentement si nécessaire
* Minimiser le recueil des données au strict nécessaire et définir leur durée de conservation minimum
* Assurer la sécurité et la confidentialité des données personnelles collectées
* Dans certains cas, mener des évaluations d’impact (PIA) sur la vie privée pour certains traitements plus sensibles.
* Faciliter aux personnes l’exercice de leurs droits : accès, rectification,…
* Informer les personnes sur le traitement de leurs demandes : motivation si refus, délais d’obtention, … le tout sous 1 mois maximum

# Lettre d’engagement type

[Nom de l’organisme]

[Adresse]

[Nom du RT]

[Fonction au sein de l’organisme]

à [lieu], le [date]

Objet : lettre d’engagement en tant que responsable de Traitement

Je soussigné [Nom, Prénom], m’engage auprès de [l’organisme] et des [définir les personnes concernées] à mettre en place les mesures de sécurité nécessaire pour garantir la sécurité des données à caractère personnel mise en œuvre au sein du traitement :

* [Nom du traitement]
* [Caractéristique du traitement] : finalité, typologie de données, durée de conservation

Par la présente j’atteste faire le nécessaire afin de :

* permettre aux personnes concernées par ce traitement d’exercer leurs droits d’accès, de rectification, de suppression et de portabilité à leurs données personnelles conformément au RGPD,
* mettre en place les mesures techniques et organisationnelles pour respecter les délais de réponses aux sollicitations des personnes
* garantir la sécurité dans l’accès, le stockage et le transfert des DCP

Ainsi en accord avec le règlement général de protection des données et avec l’aide du délégué à protection des données de l’organisme, je contribuerai à diffuser au sein de notre structure la politique de protection des données accessible sur le site internet <http://www.societeABC.fr/politique-protection-donnees>.

M. Mme [Nom du RT]

Signature