



Exemple d’article RGPD pour les contrats avec les sous-traitantsRGPD : 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 du GHT  Le | **Validé par :**  Le : | **Vérifié par :**  Mr S. CLAUDE,  DPD du GHT  Le : | **Approuvé par :**  Le : |

Sommaire

[I . Description du document 3](#_Toc523926149)

[II . Pré-requis 3](#_Toc523926150)

[III . Articles 3](#_Toc523926151)

[1 ) Conformité au Règlement Général de Protection des Données (RGPD) 3](#_Toc523926152)

[2 ) sous traitance 5](#_Toc523926153)

[3 ) Respect de la confidentialité 5](#_Toc523926154)

[4 ) Information sur les risques numériques et les moyens de prévention 5](#_Toc523926155)

[5 ) Autres obligations du sous-traitant 6](#_Toc523926156)

[6 ) Droit d’information des personnes concernées 6](#_Toc523926157)

[a / Option A 6](#_Toc523926158)

[b / Option B 6](#_Toc523926159)

[7 ) Exercice des droits des personnes 7](#_Toc523926160)

[a / Option A 7](#_Toc523926161)

[b / Option B 7](#_Toc523926162)

[8 ) Mesures de sécurités 7](#_Toc523926163)

# Description du document

Le présent document propose des articles type à intégrer dans un contrat avec un sous-traitant informatique. Il a été élaboré à partir des documents suivants :

* « DISPOSITIF NATIONAL D’ASSISTANCE AUX VICTIMES DE CYBERMALVEILLANCE » Cybermaveillance.gouv.fr, version 1.0, 30 juin 2017
* « CHARTE CYBERSECURITE DES PRESTATAIRES DE SERVICES INFORMATIQUES ET NUMERIQUES » CCI Métropolitaine Bretagne Ouest ; 07/2017
* « Règlement européen sur la protection des données personnelles - Guide du sous-traitant » ; CNIL - Edition septembre 2017

# Pré-requis

Les éléments présentés ci-dessous sont à valider avec le service juridique de l’[organisme] pour s’assurer de la compatibilité des éléments avec les autres articles du contrat

# Articles

## Conformité au Règlement Général de Protection des Données (RGPD)

Conformément à l'application du règlement européen général de protection des données à caractère personnel et au regard des traitements mis en œuvre le prestataire devra se conformer aux obligations définies par le RGPD à savoir à minima la mise en œuvre des principes suivants :

* respect de la notion de "privacy by design" : il s'agit d'intégrer la sécurité des données dès la conception de la solution et ce même si la solution a été développée avant la mise en application du règlement. A ce titre le prestataire devra donc clairement expliquer comment il met ce concept en œuvre au sein de la solution proposée.
* respect de la notion de privacy by default : tout accès aux données doit être interdit au nouvel utilisateur. Cet accès pourra ensuite être délégué aux personnes qui auront été habilitées.
* L'exercice, par chacun des individus, des droits suivant (tel que défini par le règlement) : le droit d'accès, le droit à la rectification et à l'effacement, le droit d'opposition, et le droit à la portabilité. Le prestataire fournira donc à ce sujet, au délégué à la protection des données (DPD), les procédures permettant d'exercer ces droits (dans un délai maximum de 2 mois) après la signature du contrat.
* La solution doit garantir la protection et la sécurité des données confiées au prestataire pendant toute la durée de la prestation et ce jusqu’à destruction ou restitution des données.
* le prestataire met en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque sur des données sensibles. En effet les traitements mis en jeux se rapportant à des données relatives [Religion, Opinion politique ou syndicale, Sexualité, génétique/biométrique, Santé, NIR, Condamnations Pénales] il est demandé au prestataire d'effectuer une analyse d'impact (PIA) telle que définit par le règlement.
* En cas de violation des données le prestataire devra en informer immédiatement le responsable du Traitement qui lui sera désigné et effectuer les démarches de déclaration auprès de la CNIL dans les 72 heures après détection de l'incident.

Enfin le prestataire fournira au délégué à la protection des données tous les éléments nécessaires à l'enregistrement des traitements dans le registre des traitements. Ces informations sont donc au minimum les suivantes : identification des services opérationnels traitant les données, identification des catégories de données traitées,  lieu où sont hébergées les données, durées de conservation des données, liste des mesures mises en œuvre pour minimiser les risques.

## Sous traitance

Le prestataire ne peut faire appel à un sous-traitant sans l'autorisation écrite préalable, spécifique ou générale, du responsable du traitement. Dans le cas d'une autorisation écrite générale, le prestataire informe le responsable du traitement de tout changement prévu concernant l'ajout ou le remplacement d'un sous-traitant, donnant ainsi au responsable du traitement la possibilité d'émettre des objections à l'encontre de ces changements.

Le traitement par un sous-traitant est régi par un contrat ou un autre acte juridique au titre du droit de l'Union ou du droit d'un État membre, qui lie le sous-traitant à l'égard du responsable du traitement, définit l'objet et la durée du traitement, la nature et la finalité du traitement, le type de données à caractère personnel et les catégories de personnes concernées, et les obligations et les droits du responsable du traitement.

Si le prestataire recrute un sous-traitant pour mener des activités de traitement spécifiques pour le compte du responsable du traitement, les mêmes obligations en matière de protection de données que celles fixées dans le contrat ou un autre acte juridique entre le responsable du traitement et le sous-traitant sont imposées à cet autre sous-traitant

## Respect de la confidentialité

Le prestataire s’engage à respecter la confidentialité de l’ensemble des données et renseignements confiés par l’[organisme] ou l’usager, qu’il s’agisse de la sécurité des moyens de paiement ou des données à caractère personnel et confidentiel. Il prend toutes les mesures raisonnables et nécessaires pour en assurer la protection. Aucune de ces informations ne peuvent être transmises à des tiers non autorisés contractuellement.

## Information sur les risques numériques et les moyens de prévention

Le prestataire se tient régulièrement informé des risques numériques et des moyens de prévention. Dans le cadre de son activité, le prestataire informe par tout moyen adapté ses clients ou les usagers sur les risques numériques encourus. Il pourra notamment s’appuyer sur la documentation fournie par le dispositif national.

Dans la mesure de ses possibilités, le prestataire participe aux échanges avec la communauté des signataires du présent contrat, ainsi qu’avec les autres professionnels publics ou privés, sur le plan local ou si possible au plan régional voire national.

Le sous-traitant à l’obligation d’informer, conseiller et assister l’[organisme] sur le respect des obligations définies par le RGPD si il constatait une pratique non-conforme.

## Autres obligations du sous-traitant

Le sous-traitant à l’obligation de garantir la sécurité des données traitées. Il se doit donc :

* Ses employés qui traitent les données confiées doivent être soumis à une obligation de confidentialité.
* doit notifier à l’[organisme] toute violation de ses données.
* doit prendre toute mesure pour garantir un niveau de sécurité adapté aux risques.
* au terme de la prestation et selon les instructions contractuelles définies il doit :
  + supprimer toutes les données ou les restituer à l’[organisme]
  + détruire les copies existantes sauf obligation légale de les conserver.

## Droit d’information des personnes concernées

Choisir l’une des deux options

### Option A

Il appartient au responsable de traitement de fournir l’information aux personnes concernées par les opérations de traitement au moment de la collecte des données.

### Option B

Le sous-traitant, au moment de la collecte des données, doit fournir aux personnes

concernées par les opérations de traitement l’information relative aux traitements de données qu’il réalise. La formulation et le format de l’information doit être convenue avec le responsable de traitement avant la collecte de données.

## Exercice des droits des personnes

Dans la mesure du possible, le sous-traitant doit aider le responsable de traitement à s’acquitter de son obligation de donner suite aux demandes d’exercice des droits des personnes concernées : droit d’accès, de rectification, d’effacement et d’opposition, droit à la limitation du traitement, droit à la portabilité des données, droit de ne pas faire l’objet d’une décision individuelle automatisée (y compris le profilage).

Choisir l’une des deux options

### Option A

Lorsque les personnes concernées exercent auprès du sous-traitant des demandes d’exercice de leurs droits, le sous-traitant doit adresser ces demandes dès réception par courrier électronique à [...] (indiquer un contact au sein du responsable de traitement).

### Option B

Le sous-traitant doit répondre, au nom et pour le compte du responsable de traitement et dans les délais prévus par le règlement européen sur la protection des données aux demandes des personnes concernées en cas d’exercice de leurs droits, s’agissant des données faisant l’objet de la sous-traitance prévue par le présent contrat.

## Mesures de sécurités

Le sous-traitant fournira la liste des éléments de sécurité mis en œuvre pour garantir la sécurité des sonnées qui lui sont confiées.

Le sous-traitant communique au responsable de traitement le nom et les coordonnées de son délégué à la protection des données, s’il en a désigné un conformément à l’article 37 du règlement européen sur la protection des données.

Le sous-traitant déclare tenir par écrit un registre de toutes les catégories d’activités de traitement effectuées pour le compte du responsable de traitement comprenant :

* le nom et les coordonnées du responsable de traitement pour le compte duquel il agit, des éventuels sous-traitants et, le cas échéant, du délégué à la protection des données;
* les catégories de traitements effectués pour le compte du responsable du traitement;
* le cas échéant, les transferts de données à caractère personnel vers un pays tiers ou à une organisation internationale, y compris l'identification de ce pays tiers ou de cette organisation internationale et, dans le cas des transferts visés à l'article 49, paragraphe 1, deuxième alinéa du règlement européen sur la protection des données, les documents attestant de l'existence de garanties appropriées;
* dans la mesure du possible, une description générale des mesures de sécurité techniques et organisationnelles, y compris entre autres, selon les besoins :
  + la pseudonymisation et le chiffrement des données à caractère personnel;
  + des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement;
  + des moyens permettant de rétablir la disponibilité des données à caractère personnel et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique;
  + une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement.