



Exemple d’article RGPD pour la charte informatique de l’établissementRGPD : 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 GHTLe  | **Validé par :** Le :  | **Vérifié par :** Mr S. CLAUDE, DPD du GHTLe :  | **Approuvé par :**Le : |

Sommaire

[I . Description du document 3](#_Toc523924084)

[II . Pré-requis 3](#_Toc523924085)

[III . Articles 4](#_Toc523924086)

[1 ) introduction 4](#_Toc523924087)

[2 ) Le délégué à protection des données 4](#_Toc523924088)

[3 ) Responsabilité 5](#_Toc523924089)

[4 ) Déclaration d’un incident 5](#_Toc523924090)

# Description du document

Le présent document propose des articles type à intégrer dans une charte informatique. Il a été élaboré à partir des documents suivants :

* « CHARTE D’UTILISATION DES MOYENS INFORMATIQUES ET DES OUTILS NUMÉRIQUES » ; ANSSI , version 1,0 06/2017
* « Guide pour les employeurs et les salariés » ;CNIL, édition 2010 — https://www.cnil.fr/
* « Recommandations de sécurité concernant l’analyse des flux HTTPS »; ANSSI, note technique, octobre 2014 — https://www.ssi.gouv.fr/analyse-https/
* « Recommandations de sécurité pour la mise en œuvre d’un système de journalisation »; ANSSI, note technique, décembre 2013 — https://www.ssi.gouv.fr/journalisation

# Pré-requis

Un certain nombre d’éléments devant figurer dans la charte en standard ils sont rappelés ci-dessous :

* Définir les termes clés du document au travers d’un lexique.
* Préciser les droits et devoirs de l’utilisateur.
* Intégrer des éléments spécifiques pour les administrateurs
* Définir clairement les sanctions encourus par les utilisateurs : Il est impératif de prévoir une échelle des sanctions disciplinaires.
* Définir les règles au regard des dispositifs personnels
* Lister les pratiques autorisées et celle qui sont interdites
* rappeler quelques principes essentiels :
	+ la confidentialité,
	+ la discrétion,
	+ la loyauté
	+ la vigilance.
* Les mesures de contrôle que l’entité peut mettre en place peuvent être étendues, pourvu qu’elles aient fait l’objet d’une information préalable des utilisateurs (via la charte) et qu’elles soient conformes au droit en vigueur. lister les mesures et les conditions dans lesquelles elles sont mises en œuvre (conservation des données de connexion, chiffrement des données, déchiffrement de flux https, gestion stricte des accès, contrôle des messageries professionnelles, etc.).

# Articles

## Introduction

En tant [qu'organisme public/ société privé] le [nom de l’organisme] est depuis le 25 mai 2018 soumis au Règlement Général de Protection des Données (RGPD). Au travers de cette réglementation l'ensemble des [agents/salariés] est donc impacté dans l'exercice de ses fonctions et se doit d'appliquer les préconisations définit par la Direction des systèmes d’information en matière de sécurisation des données. Il est donc de la responsabilité de chacun de se conformer à la politique générale de sécurité du système d'information et plus particulièrement aux éléments se rapportant à la sécurisation des données. Il est donc rappelé qu'en cas de manquant ou de non-respect de ces règles tout [agent/salarié] pourra faire l'objet de sanction disciplinaire.

## Le délégué à protection des données

L’[organisme] a nommé un Délégué à la Protection des Données (DPD) chargé des missions suivante :

* informer et de conseiller le responsable de traitement ou le sous-traitant, ainsi que les agents ;
* contrôler le respect du règlement et du droit national en matière de protection des données ;
* conseiller le département et en particulier les responsables de traitement sur la réalisation d’une analyse d'impact relative à la protection des données et d’en vérifier l’exécution ;
* coopérer avec l’autorité de contrôle (CNIL) et d’être le point de contact de celle-ci.

Vous pouvez donc prendre contact directement avec le DPD par email : rgpd@organisme.fr ou par téléphone à 04 77 00 11 22,

## Responsabilité

Il est rappelé aux [agents/salariés] qu’il est de leur de devoir de concourir à la sécurisation du système d’information et en particulier des données personnelles (DCP) que chacun peut être amené à utiliser. L’organisme s’est engagé dans une démarche de respect du règlement général de protection des données (RGPD).

Les obligations à respecter en la matière sont donc les suivantes :

* Collecte de DCP : informer la personne sur l’usage qu’il sera fait des informations recueillies, la durée de conservation et les modalités d’exercices de ses droits,
* Utilisation de DCP : veiller à n’utiliser ses informations que pour l’usage initial qui a été convenu avec les personnes
* Transfert de DCP : si vous étiez amené à fournir des DCP à d’autres collaborateurs ou organismes. Assurez-vous que le transfert soit sécurisé et que le destinataire s’assure lui aussi de la sécurité des données.
* Vigilance : en cas de doutes, n’hésitez pas à avertir le DPD, votre hiérarchique ou la DSI de l’[organisme]

## Déclaration d’un incident

Les [agents/salariés] ont l’obligation de prévenir sans délais le DPD ou la DSI en cas d’incident constaté pouvant engager la sécurité des données à caractère personnel des individus. [Rappeler les coordonnées de ses deux entités]