RODRIGUE
LA RÉFÉRENCE

# RGPD

*Règlement Général sur la Protection des Données*

---

La gestion des données personnelles doit se conformer aux

## six principes généraux de la RGPD

- **Légalité, équité et transparence**
- **limitation de but**
- **rétention**
- **intégrité et confidentialité**
- **minimisation des données**
- **précision**

RODRIGUE
LA RÉFÉRENCE

# Ce qui change

| | |
|---|---|
| **Augmentation des pénalités** | Le régulateur peut imposer des pénalités jusqu'à 4 % du Chiffre d'Affaire annuel ou 20 000 000 € (montant maximum) |
| **Preuves de conformité** | • Registre des traitements de données et du respect des principes<br>• Effectuer des études d'impact<br>• Mettre en oeuvre les mesures de sécurité technique |
| **Nouveaux Droits des personnes** | • Droit d'accès et de rectification des données personnelles sous 30 jours<br>• Droit à l'effacement (oubli)<br>• Droit à la portabilité<br>• Droit de contester le profilage et les informations automatisées<br>• Droit de refus du marketing direct |

| | |
|---|---|
| **Protection à la conception et par défaut** | • Intégrer la protection des données à caractère personel dès la conception des projets et durant tout le cycle de vie<br>• Confidentialité en tant que paramètre par défaut et intégrée |
| **Délégué à la protection des données** | • Poste obligatoire pour tout établissement public ou en cas de traitement à risque<br>• Signaler aux plus hauts niveaux de gestion<br>• Ne peut pas être renvoyé ou pénalisé |
| **Etudes d'impact sur la vie privée** | • Obligatoire pour tout traitement susceptible d'exposer les personnes à un risque élevé au regard de leurs droits et libertés<br>• Dans certains cas en consultant l'autorité de supervisation (CNIL) |

RODRIGUE
LA RÉFÉRENCE

| | |
|---|---|
| **Information des personnes & modalité de confidentialité** | • À fournir au moment ou la personne inscrit ses données personnelles<br>• Doivent être concises, transparentes, conpréhensibles et facilement accessibles<br>• Traduites dans le langage local |
| **Déclaration de violation obligatoire** | • Enregistrement de toute violation de données personnelles<br>• Obligation d'informer sans délai l'autorité de supervisation (CNIL)<br>• Information des personnes concernées dans les plus brefs délais |
| **Portée extra-territoriale** | La RGPD s'applique aux propriétaires et responsables de traitement de données personnelles établis en Union européenne et toute organisation ciblant des citoyens résidant en Union européenne |

RODRIGUE
LA RÉFÉRENCE

La RGPD désigne par Data Controler le propriétaire des données et DATA Processor l'entité qui les traite.

# Les obligations du Data Controler

## Délégué à la protection des données

Désigner, si nécessaire (obligatoire pour les établissements publics), un délégué à la protection des données ou une personne qui porte la responsabilité de la conformité avec la RGPD.

## Inventaire des données

Identifier quelles informations personnelles vous traitez, d'où ces informations proviennent et avec qui elles sont partagées, pour quelles raisons vous traitez ces données, sur quelles bases légales, etc.

RODRIGUE
LA RÉFÉRENCE

## Confidentialité dès la conception et DPIA*

Se familiariser avec la notion de confidentialité à la conception (Privacy by Design) et les études d'impact sur la vie privée, regarder comment intégrer ces notions au sein de votre organisation.

** Data Privacy Impact Assessment*

## Gestion des droits des personnes

Vérifier si les procédures dans votre organisation fournissent tous les droits que les personnes concernées peuvent réclamer : droit d'accès, de rectification, droit à la portabilité, retrait du consentement et droit à l'oubli.

## Violation de données

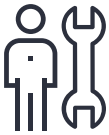
Mettre à jour les mesures techniques de sécurisation des accès aux données, examiner les procédures du personnel accédant aux données et comment des nouvelles demandes d'accès respecteront les termes de la RGPD.

## Légalité du traitement

Documenter les différents traitements sur les données personnelles qui sont effectués, identifier les bases légales et tenir un registre.

RODRIGUE
LA RÉFÉRENCE

# Les obligations du Data Processor



## Délégué à la protection des données

Désigner, si nécessaire (obligatoire pour les établissements publics), un délégué à la protection des données ou une personne qui porte la responsabilité de la conformité avec la RGPD.

## Garantie de sécurité

Fournir les garanties suffisantes de mise en œuvre des techniques appropriées et des mesures organisationnelles pour assurer que les traitements répondent aux exigences de la RGPD (encryptage, anonymisation, DLP : Data Loss Prevention).

RODRIGUE
LA RÉFÉRENCE

## Traitement des données

Traiter les données personnelles conformément aux instructions du Data Controler. Préciser dans le contrat par quels moyens vous obtenez les instructions du Data Controler. Assister et conseiller le Data Controler.

## Sous-traitant

Le sous-traitant ne peut nommer un autre sous-traitant sans l'autorisation écrite du responsable du traitement. Le traitement par un sous-traitant est régi par un contrat.

## Violation de données

Avertir le Data Controler de toute violation de données personnelles sans délai.

## Enregistrement

Conserver un enregistrement et tenir un registre de tous les traitements effectués au nom du Data Controler.

Si Rodrigue peut dans certain cas être désigné comme Data Processor, il n'est en aucun cas Data Controler, vous portez dans la plupart des cas la responsabilité des deux entités.

Par exemple, si vos données sont hébergées sur nos serveurs alors nous devont les protéger de tous risques de violation. Dans ce cadre nous sommes alors désignés comme Data Processor.

Nous avons dans ce même cadre l'obligation d'informer les autorités et notre client d'une quelconque violation des données hébergées dès la prise de connaissance de l'incident.

Votre obligation consiste à prévenir les personnes concernées par la violation et ce dans les meilleurs délais.

Nous n'avons bien entendu pas attendu la nouvelle réglementation pour protéger les données hébergées sur nos datacenters. Pour preuve, nous sommes certifiés experts dans l'administration et la gestion de pare-feu.

# La mise en conformité

Tout d'abord la mise en conformité concerne la protection des données, la transparence sur la collecte et le traitement des données ainsi que la gestion des droits des personnes (droit d'accès, de rectification, droit à la portabilité, retrait du consentement et droit à l'oubli).

Il s'applique à l'ensemble des fichiers de données personnelles, ce qui comprend les salariés, bénévoles ou encore le protocole, etc.

D'après la CNIL (*source Goeffrey Delcroix du @LINCnil Innovation & Foresight Project Manager at CNIL*) si vous êtes respectueux de sa réglementation actuellement en vigueur, vous êtes à 80 % respectueux de la nouvelle réglementation RGPD.

Nous ne sommes pas experts en la matière (il existe de nombreuses agences qui se sont positionnées sur l'accompagnement à la mise en conformité) et nous ne pouvons que vous transmettre ce qui à nos yeux et dans le contexte de la billetterie a été ajouté à l'actuelle réglementation.

La désignation d'un Délégué à la Protection des Données (DPD) est obligatoire pour les établissements publics, et seulement dans certains contextes pour les autres. Son rôle est de valider tous les traitements de données personnelles tels que la collecte, l'envoi de mail, le profiling, etc. Il doit valider que chaque traitement est respectueux de la réglementation européenne.

Chaque traitement doit être enregistré et consigné dans un registre (voir exemple sur le site de la CNIL).

La validation et la consignation représente l'aspect 'Policy by design' de la RGPD. Elle concerne à la fois les traitements, les outils de gestion des données personnelles ainsi que la diffusion aux salariées d'un guide de bonne conduite.

**Transparence :**

Il s'agit d'informer les personnes concernées par la collecte d'informations personnelles de la raison de la collecte pour chaque champs (minimisation des données collectées), de la durée de conservation des données en la motivant et des modalités de respect des droits d'accès, de rectification, du droit à la portabilité, du retrait du consentement et du droit à l'oubli.

Il faut recueillir un agrément actif de la personne concernée (boite à cocher/cliquer sur Internet, signature d'un formulaire à conserver pour preuve au guichet).

# Engagements

Pour sa part, Rodrigue s'engage à vous fournir les outils nécessaires à la mise en conformité des solutions qu'il vous apporte comme :

**Export dans un format exploitable des données générales de la fiche client et de son historique simplifié pour répondre à la portabilité des informations personnelles.**

**Cryptage irréversible des données d'une fiche client suite à une demande de droit à l'oubli ou de la fin d'une période légale de conservation**

**Enregistrement des traitements effectués sur les données personnelles au titre de la maintenance.**

Pour rappel, les solutions Rodrigue intègrent déjà toutes les fonctionnalités vous permettant d'être conforme à la réglementation actuelle de la CNIL.

En tant qu'entreprise concernée, Rodrigue s'engage également à la mise en œuvre en interne des mesures nécessaires au respect de la nouvelle réglementation entrant en vigueur le 25 mai 2018.

RODRIGUE
LA RÉFÉRENCE

# Ressources et liens utiles

https://www.cnil.fr/fr/reglement-europeen-protection-donnees

https://www.afcdp.net/IMG/pdf/rgpd_annote_et_indexe_afcdp_v3.pdf

http://www.techinfrance.fr/publications/categorie/livre-blanc/article/entreprises-les-cles-d-une-application-reussie_1

Madame Elise Dufour présidente de Cyberlex http://www.cyberlex.org/
Of Counsel cabinet Bignon Lebray

Monsieur Goeffrey Delcroix du @LINCnil Innovation & Foresight Project Manager at CNIL https://linc.cnil.fr/