

# Procédure et synthèse : RGPD et cybersécurité

---

## 1. Introduction au RGPD

Le Règlement Général sur la Protection des Données (RGPD) est une loi européenne entrée en application le 25 mai 2018. Son objectif est de renforcer la protection des données personnelles des citoyens européens et d'harmoniser les pratiques au sein de l'Union Européenne. Il s'applique à toute organisation publique ou privée traitant des données personnelles, qu'elle soit établie dans l'UE ou qu'elle cible des résidents européens.



## 2. Objectifs du RGPD

1. Renforcer les droits des personnes
2. Responsabiliser les acteurs traitant des données
3. Crédibiliser la régulation

## 3. Concepts clés

- Accountability : principe de responsabilité
- Privacy by design & by default : vie privée intégrée dès la conception
- Registre des traitements : documentation obligatoire des traitements de données



#### 4. Données concernées

Données personnelles : nom, prénom, email, IP, géolocalisation, etc.

Données sensibles : santé, orientation sexuelle, opinions politiques, etc.

#### 5. Bases légales d'un traitement

- Consentement explicite
- Exécution d'un contrat
- Obligation légale
- Sauvegarde des intérêts vitaux
- Mission d'intérêt public
- Intérêt légitime

#### 6. Droits des personnes

1. Droit d'accès
2. Droit de rectification
3. Droit à l'effacement (oubli)
4. Droit à la portabilité
5. Droit à la limitation

## 6. Droit d'opposition

## 7. Procédure en cas de fuite de données

1. Mise en place d'une cellule de crise
2. Contenir et résoudre la faille
3. Notifier la CNIL sous 72h
4. Informer les personnes concernées si nécessaire



### Loyauté et transparence

Vous devez informer les personnes concernées que vous traitez leurs données et comment vous le faites (art. 13 en cas de collecte directe et art. 14 en cas de collecte indirecte). Vous devez leur donner les informations suivantes :

Information	Exemples illustratifs
<b>Vos coordonnées</b> – le cas échéant les coordonnées de votre délégué à la protection des données	Votre adresse email et ou postale, un numéro de téléphone,...
<b>La finalité</b> du traitement (i.e. pourquoi vous traitez leurs données)	Gestion des salaires, prospection,....
<b>La base juridique</b> de votre traitement (cf. comme évoqué toute à l'heure). Si la base est votre intérêt légitime – vous devez indiquer quels sont ces intérêts	Cf. voir page précédente
<b>Les destinataires</b> / catégories de destinataires s'ils existent	CNS, Contributions directes, agence marketing, fiduciaire,...
Votre éventuelle <b>intention de transférer leurs données à un pays tiers</b>	Système IT opéré aux Etats-Unis

## 8. Acteurs clés

- RT : Responsable de traitement
- DPO : Délégué à la protection des données
- RSSI : Responsable de la sécurité des systèmes d'information



### Les principales missions du DPO

- **Inform**er et de **conseiller** le responsable de traitement de l'organisation et/ou le sous-traitant,
- Diffuser une **culture Informatique & Libertés** au sein de l'organisation ;
- **Contrôler** le **respect** du règlement et du droit national en matière de protection des données,
- **Conseiller** l'**organisation** sur la réalisation d'une analyse d'impact relative à la prot. des données,
- **Coopérer** avec la CNIL et d'être le point de contact de celle-ci.
- S'assurer de la **bonne tenue** de la documentation relative aux traitements
- **Répondre** aux **demandes des utilisateurs** faisant valoir leurs droits (oubli, portabilité,...)

## 9. Traitements à risque

Exemples : surveillance, données de santé, données sensibles, transferts hors UE, etc.

## 10. Exemple de registre de traitement



### Le registre comme index (art. 30)

Le registre se présente sous une forme écrite ou électronique

- Le registre est un outil de l'accountability (responsabilité)
- C'est un outil de pilotage et de démonstration de la conformité
- Les sous-traitants doivent également tenir un registre
- Le registre n'est pas lié à la désignation d'un DPD
- Il permet d'identifier et de hiérarchiser les risques

Nom du traitement	Finalité	Base légale	Sensibilité
Gestion des salariés	Païement des salaires	Intérêt contractuel	Oui
Transmission aux impôts	Païement impôts	Intérêt légal	Non
Commandes fournisseurs	Réapprovisionnement	Intérêt contractuel	Non
Newsletter	Comprendre le client	Consentement	Non
Traitement client	Suivi commercial	Intérêt légitime	Oui

## 11. Documentation obligatoire

- Registre des traitements
- Mentions légales et politiques de confidentialité
- Courriers de notification
- Études d'impact et transferts hors UE

## RGPD : se préparer en 6 étapes

<b>ETAPE 1</b> DÉSIGNER UN PILOTE	<b>DÉSIGNER UN PILOTE</b> Pour piloter la gouvernance des données personnelles de votre structure, vous aurez besoin d'un véritable chef d'orchestre qui exercera une mission d'information, de conseil et de contrôle en interne : le délégué à la protection des données. En attendant 2018, vous pouvez d'ores et déjà désigner un « correspondant informatique et libertés », qui vous donnera un temps d'avance et vous permettra d'organiser les actions à mener. > <a href="#">En savoir plus</a>
<b>ETAPE 2</b> CARTOGRAPHIER	<b>CARTOGRAPHIER VOS TRAITEMENTS DE DONNÉES PERSONNELLES</b> Pour mesurer concrètement l'impact du règlement européen sur la protection des données que vous traitez, commencez par recenser de façon précise vos traitements de données personnelles. L'élaboration d'un registre des traitements vous permet de faire le point. > <a href="#">En savoir plus</a>
<b>ETAPE 3</b> PRIORISER	<b>PRIORISER LES ACTIONS À MENER</b> Sur la base de votre registre, identifiez les actions à mener pour vous conformer aux obligations actuelles et à venir. Priorisez ces actions au regard des risques que font peser vos traitements sur les droits et les libertés des personnes concernées. > <a href="#">En savoir plus</a>
<b>ETAPE 4</b> GÉRER LES RISQUES	<b>GÉRER LES RISQUES</b> Si vous avez identifié des traitements de données personnelles susceptibles d'engendrer des risques élevés pour les droits et libertés des personnes concernées, vous devez mener, pour chacun de ces traitements, une analyse d'impact sur la protection des données (PIA). > <a href="#">En savoir plus</a>
<b>ETAPE 5</b> ORGANISER	<b>ORGANISER LES PROCESSUS INTERNES</b> Pour assurer un haut niveau de protection des données personnelles en permanence, mettez en place des procédures internes qui garantissent la prise en compte de la protection des données à tout moment, en prenant en compte l'ensemble des événements qui peuvent survenir au cours de la vie d'un traitement (ex : faille de sécurité, gestion des demandes de rectification ou d'accès, modification des données collectées, changement de prestataire). > <a href="#">En savoir plus</a>
<b>ETAPE 6</b> DOCUMENTER	<b>DOCUMENTER LA CONFORMITÉ</b> Pour prouver votre conformité au règlement, vous devez constituer et regrouper la documentation nécessaire. Les actions et documents réalisés à chaque étape doivent être réexaminés et actualisés régulièrement pour assurer une protection des données en continu. > <a href="#">En savoir plus</a>