



R.G.P.D

Comment devenir conforme
en 9 points.



Sommaire

Cet ebook est composé de 9 points permettant de **comprendre RGPD** et mettre en place les **pratiques requises** pour y être **conforme**.

Les principes de RGPD	2
Mon organisation est-elle concernée ?	3
Mon organisation doit-elle nommer un DPD ?	4
Sommes-nous responsables du traitement de la donnée ?	5
Comment respecter les droits des utilisateurs ?	6
Comment respecter l'Accountability ?	7
Comment documenter la sécurité et gérer les failles ?	8
Comment transférer des données hors UE ?	9
Poursuites et sanctions	10

Les principes de RGPD

RGPD : régulation européenne sur la protection et la circulation des données à caractère personnel. Applicable à compter du 25 mai 2018.

Le but de ce e-book est de clarifier l'application de RGPD pour les entreprises.

La vérification et la précision de l'application du règlement sera faite par les organismes nationaux compétents. Dans le cas de la France, la CNIL sera la référence. Chaque état membre pourra adopter des règles spécifiques en plus de RGPD.

Les principes de RGDP :

1. **Licéité, loyauté et transparence** du traitement des données.
2. **Limitation des finalités** : les finalités du traitement doivent être déterminées, et ne peuvent pas être modifiées ultérieurement.
3. **Minimisation** : les données doivent être pertinentes, adéquates et limitées à ce qui est nécessaire aux finalités.
4. **Exactitude** : les données doivent être exactes et à jour.
5. **Limitation de la conservation** : les données ne peuvent pas être conservées après la durée nécessaire pour les finalités.
6. **Sécurité, intégrité et confidentialité** : les données doivent être traitées de façon à garantir une sécurité appropriée.

Mon organisation est-elle concernée?

Les organisations concernées « traitent des données à caractère personnel de personnes physiques ». Définition des termes :

« Organisation » :

- **Un responsable du traitement** : celui qui détermine les finalités et les moyens du traitement. Une personne physique ou morale, autorité publique, service ou autre organisme (il n'y a pas de forme juridique spécifique).
- **Un sous-traitant du traitement** : celui qui traite les données pour le responsable du traitement.

« Traitement » :

Collecte, enregistrement, utilisation, consultation, communication, organisation, conservation, modification, extraction, diffusion, limitation, effacement, destruction. **Les « moyens » de traitement** : automatique, manuel, écrit, non digital, digital.

« Donnée personnelle » :

Une information qui se rapporte (directement ou indirectement) à une personne physique (ex : identité, coordonnées, numéro d'identifiant, données de localisation, informations relatives à la vie professionnelle, habitudes de consommation, adresse IP...).

- **Les données réellement anonymisées ne sont pas soumises à RGPD.** C'est à dire, les données ne pouvant pas (même indirectement) être rattachées à une personne physique identifiable.

« Personne physique » :

Clients, prospects, fournisseurs, salariés, partenaires...

Quelques exemples :

Gestion des rémunérations, annuaire d'entreprise, fournisseurs, comptabilité, clients, opérations de prospection, gestion des outils informatiques, surveillance vidéo, contrôle des accès.

Lien avec le territoire de l'Union Européenne

- L'offre est disponible sur le territoire (en ligne ou hors ligne)
- Le lieu d'établissement de l'entité est sur le territoire
- La personne concernée se trouve sur le territoire
- Il y a un suivi du comportement utilisateur sur le territoire (ex : navigation, comportements...)

Mon organisation doit-elle nommer un DPD (Délégué à la Protection des Données) ?

Quelles entreprises doivent nommer un DPD ?

- Entreprises dans le secteur public
- Si il y a un suivi régulier, systématique et à grande échelle de personnes
- Si traitement à grande échelle de données sensibles ou relatives à des condamnations pénales ou infractions

C'est à l'entreprise d'interpréter les termes : « régulier et systématique », « à grande échelle » et « sensibles ».

Quelles personnes peuvent être DPD ?

- Une personne avec des connaissances :
 - spécialisées du droit
 - en matière de protection des données
 - de l'entreprise, du produit et du secteur
- Possibilité qu'elle soit :
 - assistée par d'autres personnes qualifiés
 - externe (contrat de prestation de services)
 - mutualisée au sein d'un groupe d'entreprises

Profil idéal : personne juridique disposant de connaissances techniques, ou un risk manager.

La mission du DPD (formalisée dans une lettre de mission ou fiche de poste)

- Diffuser une « culture Informatique et libertés »
- Contrôler la conformité des traitements et le respect du règlement
- Conseiller sur la protection des données
- Participer à la création et vérifier l'exécution d'analyses d'impact du traitement des données sur la sécurité
- Être le point de contact avec l'autorité de contrôle et les personnes concernées

L'organisation avec un DPD

- Associer le DPD aux questions relatives à la protection des données "de manière appropriée et en temps utile"
- Le DPD doit être indépendant et avoir à disposition les moyens techniques, financiers, humains et organisationnels nécessaires pour mener à bien sa mission

Sommes-nous responsables du traitement de la donnée ?

Un acteur du traitement peut être :

- **Un responsable du traitement** : il détermine les finalités et moyens du traitement
- **Un sous-traitant du traitement** : il traite les données pour le responsable. Si nécessaire, il doit conseiller, assister et informer le responsable

Les responsabilités :

- Le responsable du traitement est responsable des dommages causés
- Le sous-traitant est responsable s'il n'a pas respecté les obligations du règlement ou s'il a agi en dehors des instructions du responsable

Il peut y avoir des responsables conjoints du traitement :

- S'ils **déterminent ensemble les finalités et les moyens** du traitement
- **Un contrat**, un accord ou une convention doit prévoir les rôles respectifs pendant le traitement et les relations avec les personnes concernées
- **Les mêmes droits et devoirs** s'appliquent aux responsables conjoints

Relations entre responsable et sous-traitant :

- Le responsable doit s'assurer que le sous-traitant "présente les garanties nécessaires pour appliquer les mesures appropriées au traitement"
- Éléments devant figurer dans le contrat (ou acte juridique)
 - **Définition** du traitement
 - Obligations du **sous-traitant** :
 - Aider le responsable de traitement dans le cadre d'une demande
 - Avoir une autorisation écrite du responsable pour le recrutement d'un nouveau sous-traitant. Les sous-traitants ultérieurs ont les mêmes obligations que le sous-traitant initial
 - Confidentialité pour les personnes autorisées à traiter les données chez le sous-traitant
 - Au terme de la prestation, supprimer ou restituer les données
 - Respect des exigences de sécurité et de confidentialité
 - Mettre à disposition du responsable les informations nécessaires pour prouver le respect des obligations et permettre la réalisation d'audits
 - Obligations du **responsable** :
 - Documenter ses instructions de sécurité pour le sous-traitant

Comment respecter les droits des utilisateurs ?

Quelles informations fournir à la personne concernée (ex: l'utilisateur)?

- Sur l'entreprise :
 - Identité du responsable de traitement
 - Coordonnées du DPD
- Sur les données :
 - Finalité du traitement (à quoi sert le traitement)
 - Destinataire(s) des données
 - Durée de conservation
 - Caractère réglementaire ou contractuel de la demande des données
 - Conséquence de la non-fourniture des données
 - Existence de transferts de données hors UE
 - **Existence des droits d'accès, de rectification, d'effacement, de limitation, d'opposition au traitement, du droit à la portabilité, du droit d'introduire une réclamation auprès d'une autorité de contrôle, de retirer son consentement**
 - Existence d'une prise de décision automatisée (ex: profilage)

Quand informer l'utilisateur ?

- Si **responsable du traitement**, directement après le captage de la donnée.
- Si **sous-traitant du traitement**, dans le mois suite au captage de donnée.

Quand fournir les informations ?

- **Manière** : Concise, transparente, compréhensible, accessible
- **Moyens** : Écrit ou électronique ou orale
- **Supports** :
 - Formulaires de collecte de données
 - Documents contractuels
 - Support marketing
 - Courrier dédié
 - Dans « privacy policy » d'un site web
 - Si l'information est donnée à l'orale, il faut doubler par un écrit;
- **Cas spécial** : le droit d'opposition doit être donné à la personne concernée lors de la première communication séparément des autres informations.

Quand fournir les informations ?

- **Délais** : 1 mois pour répondre. Si le délai est dépassé, il faut justifier le retard.
- **Moyens** : Réponse écrite ou électronique ou oral.
- **Facturation** : **il est illégal de demander un paiement pour cette activité** mais il est possible de faire payer le coût administratif des copies supplémentaires.

Comment respecter l'Accountability ?

Accountability : des mesures appropriées, des processus permanents et dynamiques pour un traitement conforme.

Documents à synthétiser (format écrit ou électronique)

- Un **rappor sur les mesures internes** de protection des données et leur vérification
- Une **charte de conformité** d'utilisation des données
- Un **rappor mensuel et un bilan annuel** sur l'organisation "Informatique et libertés"
- Une **cartographie des risques** du traitements sur l'atteinte à la vie privée des personnes concernées
- **Un registre des traitements**
 - **Obligatoire** si l'entreprise a plus de 250 salariés et/ou si les traitements comportent un risque pour les droits et libertés des personnes
 - **Contenu du registre**
 - Identité et coordonnées
 - du responsable de traitement et de son représentant
 - du DPD
 - Lister les finalités du traitement, les catégories de personnes concernées, les données, et les destinataires
 - Existence de transferts de données hors UE et référence aux garanties associées
 - Durée de conservation des données
 - Description des mesures de sécurité mises en place

Systèmes internes à mettre en place :

- **Formation** et sensibilisation au traitement des données
- Création d'un **code de conduite**
- Désignation d'un **DPD** (si nécessaire)
- Création d'un **comité de pilotage** "Informatique et libertés"
- Mise en place d'une **procédure de gestion des demandes** utilisateur
- Implémentation de "**Privacy by design**"
 - Protection des données dès l'origine d'un projet (par ex : un cahier des charges des contraintes à respecter pour un nouveau projet)
- Implémentation de "**Privacy by default**"
 - Seules les données qui sont **nécessaires** à la finalité du traitement sont collectées et utilisées

Comment documenter la sécurité et la confidentialité ?

Réaliser une étude des risques sur les données, documentant les points suivants :

- Destruction, perte, altération, divulgation non autorisée, accès non autorisé aux données
- Confidentialité des données
- Intégrité des données
- Disponibilité des données
- Résilience des données
- Traçabilité et journalisation des accès aux données et actions sur les données
- Archivage et sauvegarde des données

Réaliser une étude des risques sur les personnes, documentant les points suivants :

- Méthode d'identification et d'authentification des utilisateurs
- La gestion des habilitations (qui est autorisé à accéder à certaines données)
- Sensibilisation des utilisateurs au traitement de leurs données

Réaliser une étude des risques sur l'entreprise, documentant les points suivants :

- Sécurisation des appareils électroniques
- Plans de continuation / de reprise d'activité et/ou plan de secours informatique
- Gestion des incidents
- Sécurisation des locaux, du réseau interne, des serveurs et des applications
- Sécurisation des échanges avec les tiers
- Mise à jour des logiciels
- Surveillance de l'activité du réseau
- Interdiction de toute communication directe entre des postes internes et l'extérieur
- Cloisonnement des réseaux en sous-réseaux

Gérer une faille en tant que responsable du traitement (au plus vite, sous 72H si possible)

- Notifier l'autorité de contrôle. Contenu de la notification :
 - Les mesures prises pour remédier à la faille
 - Documentation de la faille de sécurité
- Notifier la personne concernée
 - Si risque élevé pour les droits et les libertés de la personne concernée
 - Langage clair et simple

Gérer une faille en tant que sous-traitant

Prévenir le responsable du traitement (qui lui préviendra les personnes concernées).

Comment transférer des données hors UE ?

Documentation nécessaire pour un transfert de données hors UE

L'entreprise doit **documenter un niveau de sécurité adéquat** au regard de la criticité des données.

La loi ne donne pas d'information à propos de la structure ou même du niveau de précision de la documentation requise.

Exceptions et dérogations à la documentation

- **Pays où une documentation n'est pas nécessaire** : Suisse, Canada, Argentine, Guernesey, Ile de Man, Jersey, Andorre, Iles Féroé, Israël, Uruguay, Nouvelle-Zélande, Norvège, Iceland, Liechtenstein.
- **Le cas des États-Unis** : transfert sans documentation si **EU-US Privacy Shield**
- Si il y a **consentement explicite** de la personne concernée
- Si le transfert est nécessaire :
 - à l'exécution du **contrat entre la personne concernée et le responsable de traitement**
 - à l'exécution d'un **contrat entre le responsable de traitement et un tiers**
 - pour des motifs d'intérêt public
 - à la constatation, à l'exercice ou à la défense de **droits en justice**
 - à la sauvegarde des **intérêts vitaux** de la personne concernée
- Si les conditions suivantes sont **cumulativement** respectées :
 - Transfert non répétitif
 - Nombre limité de personnes concernées
 - Transfert nécessaire aux fins des intérêts légitimes poursuivis par le responsable de traitement
 - Évaluation du responsable de traitement que les garanties appropriées sont respectées
 - Information à l'autorité de contrôle et à la personne concernée

Poursuites et sanctions

Enquête préliminaire

- **Origines possibles d'une enquête :**
 - Infos reçues par une autre autorité de contrôle ou une autorité publique
 - Réclamation d'une personne concernée
 - A la propre initiative de l'autorité de contrôle
- **Pendant l'enquête, l'autorité de contrôle peut :**
 - Demander la communication de toute information
 - Procéder à des audits
 - Procéder à un examen des certifications
 - Obtenir l'accès aux : locaux, installations, et moyens de traitement

8 mesures correctrices

1. Avertissement
2. Rappel à l'ordre
3. Ordre de mise en conformité
4. Ordre de respecter les droits des personnes
5. Limitation ou interdiction de traitement
6. Retrait de certification
7. Suspension des flux hors UE
8. **Amendes** (en complément ou à la place des autres mesures correctrices)
 - **2 types d'amendes** : le montant le plus élevé est retenu entre % et fixe
 - Type 1 : 10 m€ ou 2% du CA annuel mondial de N-1
 - Type 2 : 20 m€ ou 4% du CA annuel mondial de N-1
 - **Type 1 appliqué si :**
 - Privacy « by design » et/ou « by default » non respecté
 - Registre des activités de traitement innexistant ou mal tenu
 - Notification à l'autorité de contrôle ou à la personne pas envoyée
 - Mesures de sécurité des données inexistantes ou insuffisantes
 - Analyse d'impact non réalisée
 - Pas de contrat avec un responsable conjoint du traitement ou avec un sous-traitant
 - Pas de DPD
 - **Type 2 appliqué si :**
 - Principes de base des traitements de données non respectées (loyauté, transparence, limitation des finalités, minimisation des données, durée de conservation...)
 - Licéité du traitement non respectée
 - Droits des personnes non respectés (information, accès, rectification, effacement, etc.)
 - Conditions de traitements de données non respectées
 - Transferts de données vers des pays tiers sans respect des conditions requises.
 - Injonction prononcée par l'autorité de contrôle non respectée.



EASE.SPACE

Sécurité de mots de passe pour les équipes



Benjamin Prigent
CEO d'Ease.space

*Merci à Bold Avocats pour leur aide dans l'analyse
des textes de loi et la rédaction de cet ebook.*