# Glossaire RGPD
# Les notions essentielles pour les dirigeants de PME

Le RGPD s'appuie sur un vocabulaire spécifique, souvent perçu comme juridique ou technique. Pourtant, comprendre ces termes est indispensable pour piloter efficacement la protection des données au sein d'une PME, dialoguer avec ses prestataires et sécuriser ses pratiques.

Ce glossaire RGPD s'adresse aux **dirigeants de PME, PMI, associations et structures de proximité**. Il regroupe les notions clés rencontrées lors d'un **audit RGPD**, d'une **mise en conformité** ou dans le cadre d'un **DPO externalisé**. Les définitions sont volontairement synthétiques, concrètes et orientées usage professionnel.

## Glossaire RGPD : 30 définitions clés

**RGPD (Règlement Général sur la Protection des Données)**
Règlement européen encadrant la collecte, l'utilisation et la protection des données personnelles par les entreprises et organisations.

**Donnée personnelle**
Toute information permettant d'identifier directement ou indirectement une personne physique, comme un nom, email, numéro client ou IP.

**Traitement de données**
Toute opération réalisée sur des données personnelles : collecte, stockage, consultation, modification, transmission ou suppression.

**Responsable de traitement**
Entité qui détermine les finalités et les moyens du traitement des données personnelles, généralement l'entreprise elle-même.

**Sous-traitant**
Prestataire traitant des données personnelles pour le compte du responsable de traitement, selon un contrat encadré par le RGPD.

**DPO (Délégué à la Protection des Données)**
Professionnel chargé de piloter la conformité RGPD, conseiller l'entreprise et assurer la liaison avec la CNIL.

**DPO externalisé**
Solution consistant à confier la fonction DPO à un expert externe, adaptée aux PME sans ressources internes dédiées.

**Registre des traitements**
Document obligatoire recensant l'ensemble des traitements de données réalisés par l'organisation et leurs caractéristiques principales.

**Base légale**
Fondement juridique autorisant un traitement de données : contrat, obligation légale, consentement, intérêt légitime ou mission d'intérêt public.

**Consentement**
Accord libre, éclairé et explicite donné par une personne pour l'utilisation de ses données personnelles.

**Intérêt légitime**
Base légale permettant un traitement nécessaire aux intérêts de l'entreprise, sous réserve de respecter les droits des personnes.

**Finalité**
Objectif précis et légitime poursuivi par un traitement de données, défini avant la collecte des informations.

**Minimisation des données**
Principe imposant de collecter uniquement les données strictement nécessaires à la finalité du traitement.

**Durée de conservation**
Période pendant laquelle les données personnelles peuvent être conservées avant suppression ou archivage sécurisé.

**Exactitude des données**
Obligation de maintenir des données à jour et correctes afin d'éviter erreurs, litiges ou décisions inappropriées.

**Sécurité des données**
Mesures techniques et organisationnelles visant à protéger les données contre l'accès non autorisé, la perte ou la divulgation.

**Violation de données (Data breach)**
Incident de sécurité entraînant la perte, l'altération ou l'accès non autorisé à des données personnelles.

**Notification de violation**
Obligation de signaler certaines violations de données à la CNIL et, dans certains cas, aux personnes concernées.

**Droits des personnes**
Ensemble des droits RGPD : accès, rectification, effacement, opposition, limitation et portabilité des données.

**Analyse d'impact (AIPD / DPIA)**
Étude visant à évaluer les risques d'un traitement à fort impact sur la vie privée des personnes.

**Cookies**
Fichiers déposés sur le terminal d'un utilisateur pour mesurer l'audience, personnaliser l'expérience ou proposer de la publicité.

**Traceurs**
Technologies permettant de suivre le comportement des utilisateurs sur un site ou une application.

**Bandeau cookies**
Dispositif d'information et de recueil du consentement des utilisateurs pour les cookies non essentiels.

**CNIL**
Autorité française chargée de veiller au respect du RGPD et de sanctionner les manquements constatés.

**Audit RGPD**
Diagnostic structuré évaluant le niveau de conformité RGPD d'une organisation et identifiant les risques prioritaires.

**Mise en conformité RGPD**
Processus global visant à aligner durablement les pratiques de l'entreprise avec les exigences réglementaires.

**Accountability (Responsabilité)**
Principe obligeant l'entreprise à démontrer concrètement sa conformité RGPD à tout moment.

**Politique de protection des données**
Document interne ou externe décrivant les engagements et pratiques de l'entreprise en matière de données personnelles.

## Autres acronymes utiles :

ACP : Action corrective permanente
AELE : Association européenne de libre-échange
AIPD : Analyse d'impact relative à la protection des données
DPA (Data Protection Authority) : Autorité de protection des données
EDPB (European Data Protection Board) : Comité Européen de la Protection des Données
IDS (Intrusion Detection System) : Système de détection d'intrusion
IIP : Information d'identification personnelle
ISO : Organisation internationale de normalisation
LIA (Legitimate Interests Assessment) : Évaluation des intérêts légitimes
MQT : Management de la qualité totale
NAC (Network Access Control) : Contrôle d'accès au réseau
PIA (Privacy Impact Assessment) : Étude d'impact sur la vie privée
PIMS (Privacy Information Management System) : Système de management de la protection de la vie privée
RoC (Return on Control) : Retour sur la mesure de sécurité
RSI : Responsable de la sécurité de l'information

Ce glossaire RGPD constitue une base de compréhension essentielle pour les dirigeants de PME. Toutefois, chaque organisation présente des spécificités métiers, techniques et humaines. Un **audit RGPD personnalisé** ou l'accompagnement d'un **DPO externalisé** permet de transformer ces notions en actions concrètes et sécurisées.

---

**Vous souhaitez évaluer votre niveau de conformité ou être accompagné par un DPO externalisé ? Contactez-moi : eric@dponormandie.fr**