Le RGPD pour les TPE

Description

Avec l'entrée en vigueur du Règlement Général sur la Protection des Données (RGPD), les TPE comme de nombreuses entreprises ont dû **adapter leurs procédures et leurs pratiques**. En effet, la nouvelle réglementation les a contraint à se mettre en conformité avec le RGPD, et ainsi à respecter de nouvelles obligations.

Ainsi, il est utile pour les dirigeants de TPE de **se familiariser avec ces nouvelles obligations**, afin d'éviter les sanctions liées au RGPD.

Obtenir un devis gratuit RGPD

Les TPE sont-elles concernées par l'application du RGPD ?

Le RGPD a pour principal objectif d'**encadrer le traitement des données personnelles**. Il fixe ainsi les conditions dans lesquelles ces données sont collectées, conservées et exploitées.

C'est pourquoi, les personnes concernées par le RGPD sont les **organismes amenés à traiter des données personnelles**. Le traitement de ces données doit permettre à l'organisme de fonctionner correctement ou d'assurer la gestion de ses activités.

A noter : L'article 4 du RGPD définit une donnée personnelle comme une information permettant d'identifier directement ou indirectement une personne physique.

Ainsi, tous les organismes publics ou privés sont concernés par le RGPD. C'est pourquoi, **les TPE traitant des données personnelles** sont dans l'obligation de respecter les principes imposés par le RGPD. Il importe donc peu la taille de l'entreprise, sa forme juridique ou son nombre de salariés.

Bon à savoir : Lorsque la TPE a recours à un sous-traitant pour le traitement des données personnelles, celui-ci doit également se soumettre aux obligations imposées par le RGPD.

Quelles sont les obligations des TPE au regard du

RGPD ?

Le RGPD, entré en vigueur en 2018, **impose de nombreuses obligations aux TPE**. En effet, celles-ci doivent veiller à respecter plusieurs principes.

Les principes instaurés par le RGPD

De nombreux principes ont été instaurés par le RGPD visant à **garantir la protection des données personnelles**. C'est pourquoi il appartient aux TPE d'adapter le traitement des données personnelles aux nouvelles règles imposées par le RGPD.

Ainsi, les TPE sont dans l'obligation de respecter les principes suivant :

- **la licéité du traitement** : l'article 6-1 du RGPD prévoit en effet six conditions dans lesquelles le traitement des données personnelles est permis. Les TPE doivent ainsi veiller à ce que le traitement des données entre dans ces conditions.

Attention : Si le traitement des données personnelles de la TPE ne répond pas aux six conditions, celui-ci ne sera pas licite.

- **la minimisation des données** : la TPE a l'obligation de limiter la collecte des données à celles étant strictement nécessaires par rapport à la finalité du traitement. Ainsi, la collecte des données doit uniquement répondre à l'objectif défini.
- le principe d'accountability : les entreprises sont responsables en cas de non-respect des principes posés par le RGPD. Ainsi, les TPE doivent mettre en place des mesures pour garantir les principes du RGPD.
- le principe de "privacy by design" : dès la conception d'un produit ou service, la TPE doit veiller à prendre en compte la protection des données personnelles.

Le respect des droits des personnes

Le RGPD confère de **nombreux droits** aux personnes dont les données sont collectées. En effet, celles-ci disposent notamment d'un droit :

- **d'accès** ;
- **de rectification** ;
- à la portabilité : toute personne a le droit de récupérer les données qu'elle a fournies à un responsables de traitement.

Les TPE sont ainsi dans l'**obligation de mettre en place des mesures** veillant à

respecter ces droits.

Par ailleurs, elles doivent veiller dans de **nombreuses situations** à recueillir le consentement dans le cadre du RGPD des personnes concernées.

A noter : Les TPE doivent également respecter les règles strictes imposées en matière de profilage par le RGPD.

Comment mettre en conformité sa TPE avec le RGPD ?

La mise en conformité de la TPE avec le RGPD nécessite **le respect de plusieurs étapes**. En effet, les TPE ont l'obligation de mettre en place plusieurs mesures afin de garantir au mieux le respect des principes précédemment listés.

Etape 1 : Constituer un registre du traitement des données

La mise en conformité au RGPD implique une **documentation détaillée des opérations** liées aux données personnelles. Ainsi, les TPE doivent disposer d'**un registre des activités de traitement**. Ce dernier permet le recensement des traitements des données personnelles et fournie une vue d'ensemble sur l'utilisation des données personnelles.

Ainsi, le registre doit contenir :

- les types des traitements ;
- les différents traitements effectués ;
- les acteurs traitant des données ;
- les types de données recueillies et utilisées (leur origine, leur catégorie, un transfert éventuel des données de l'étranger ou à l'étranger) ;
- la durée de conservation des données personnelles ;
- les conditions d'exécution du traitement ;

Il est par ailleurs recommandé de confier la tenue du registre **au délégué à la protection des données** (DPO RGPD). Celui-ci aura alors pour mission de le mettre à jour régulièrement.

A noter : Ce registre doit pouvoir être communiqué à la CNIL lorsqu'elle le demande.

Etape 2 : Trier les données

Trier les données, c'est permettre de collecter les données **uniquement nécessaires** au traitement.

En effet, les TPE ne doivent collecter que les données dont elles ont strictement besoin en :

- **ne collectant les données que si elles ont un lien direct avec la finalité du traitement**
- **limitant la collecte aux données strictement nécessaires par rapport à la finalité du traitement**

Bon à savoir : La finalité du traitement se définit comme l'objectif en vue duquel les données sont collectées ou exploitées par l'organisme. Elle doit impérativement être définie par les entreprises.

Etape 3 : Sécuriser les données personnelles

La sécurisation des données personnelles est un principe posé par l'article 32-1 du RGPD. Ainsi, les TPE doivent **mettre en œuvre les mesures techniques appropriées**. Celles-ci permettent alors de garantir un niveau adapté aux risques.

La sécurisation des données s'appuie sur les principes suivant :

- **confidentialité** : seules les personnes autorisées ont accès aux données.
- **intégrité** : les données ne doivent pas subir d'altération ou de modification.
- **disponibilité** : les données doivent être accessibles aux personnes autorisées, et ce en permanence.

L'adoption de plusieurs mesures est possible pour garantir la sécurité. Ainsi, les TPE peuvent mettre en place le **chiffrement des données**. Cela permet alors de garantir la confidentialité d'une information. Elles peuvent également procéder à **la pseudonymisation des données**. Elle consiste à remplacer une donnée personnelle par un pseudonyme.

A noter : Outre les étapes mentionnées, les TPE peuvent également avoir recours à une formation RGPD. Celle-ci permet alors de mettre en place des mesures assurant la mise en conformité au RGPD de l'entreprise.

Quelles sont les sanctions en cas de non-respect du RGPD par les TPE ?

L'accountability RGPD contraint les TPE à rendre des comptes auprès de la CNIL, autorité de contrôle en France. De **lourdes sanctions** peuvent être prononcées en cas de non-respect des normes, notamment le manquement aux droits des personnes.

En effet, si les mesures adéquates ne sont pas mises en place pour assurer la protection des données personnelles, l'entreprise peut être sanctionnée d'une amende. Cette dernière peut s'élever jusqu'à **20 millions d'euros ou 4 % du chiffre d'affaires annuel mondial.**

Toutefois, **les autorités de contrôle peuvent également appliquer des sanctions administratives** conséquentes et dissuasives, à savoir :

- **Imposer l'obligation de conformité** ;
- **Réaliser un rappel à l'ordre** ;
- **Limiter définitivement ou temporairement le traitement des données.**

Attention : ces mesures répressives peuvent également avoir de graves conséquences sur l'image de la TPE concernée. En effet, elles peuvent faire l'objet d'une publication.

FAQ

Comment mettre sa TPE en conformité avec le RGPD ?

Afin d'être conforme au RGPD, les TPE sont dans l'obligation d'adapter leurs procédures et leurs pratiques. Elles doivent ainsi mettre en place plusieurs mesures telles que la tenue d'un registre du traitement des données ou la sécurisation des données personnelles.

Quelles sont les obligations à respecter par les TPE selon le RGPD ?

Les TPE doivent veiller à respecter les principes posés par le RGPD. En effet, celles-

ci sont considérées comme responsables du respect des grands principes du RGPD. Elles doivent ainsi respecter par exemple le principe de licéité du traitement des données ou la minimisation des données.

Quelles sont les sanctions en cas de non-respect du RGPD ?

Les entreprises peuvent faire l'objet de plusieurs types de sanctions en cas de non-respect du RGPD. La CNIL peut par exemple prononcer des amendes allant jusqu'à 20 millions d'euros ou 4% du chiffres d'affaires. Elle peut également prononcer des sanctions administratives telles qu'un rappel à l'ordre ou le retrait d'une certification.