|  |
| --- |
| **Le RGPD en 10 étapes**  Etape 1- Répertoriez les données que vous traitez |

## **Le RGPD en 10 étapes**

## **Etape 1 – Répertoriez les données que vous traitez**

### Introduction

Chaque entreprise conserve une multitude de données, qu’il s’agisse d’une entreprise unipersonnelle ou d’une multinationale. Et il y a fort à parier que peu d'entreprises sont réellement au fait de toutes les données qu'elles conservent. Pour implémenter le RGPD dans votre entreprise, vous devez donc commencer par le début : répertorier les données que vous traitez. Il est fort probable que vous arriviez au constat que vous traitez plus de données que vous ne le pensiez. C’est justement à cela que cet exercice doit servir et pour lequel nous vous guidons pas à pas. En premier lieu, il convient donc d’identifier ce qui est collecté.

### Qu’est-ce qu’au juste une donnée à caractère personnel ?

Vous avez peut-être remarqué que le RGPD ne s'applique pas à toutes les données, mais uniquement aux données à caractère personnel. Selon le RGPD, une donnée personnelle est toute donnée à l’aide de laquelle une personne physique peut être identifiée.

De cette définition, on peut déduire deux choses :

1. **Seules les données permettant d’identifier une personne physique sont pertinentes**.

Les données qui identifient (uniquement) une personne morale ne sont pas couvertes par le RGPD. Par exemple, une personne physique ne peut être identifiée à partir d'adresses électroniques impersonnelles telles que info@xyz.be. Ces données ne sont donc pas couvertes par le RGPD. En revanche, à partir de l'adresse électronique jean.dupont@xyz.be, une personne physique peut bien être identifiée, celle-ci constitue dès lors bien une donnée « à caractère personnel ».

De la même manière, la dénomination "SPRL Lotus Bleu" n'est pas une donnée personnelle, mais celle de "SPRL Jean Dupont" constitue bien une donnée à caractère personnel.

1. **Toute information à partir de laquelle une personne physique peut être identifiée est une donnée personnelle.**

Cela va donc bien au-delà du nom, du numéro de téléphone ou de l’adresse électronique. Une adresse IP, une plaque d'immatriculation, un numéro de registre national, le numéro de société d'une entreprise individuelle, le numéro de compte bancaire d'une personne physique, etc., sont des données à caractère personnel et doivent donc être reprises dans votre inventaire**.**

### Quelles données traitez-vous ?

Vous pouvez bien sûr examiner tous vos fichiers Excel contenant des listes d'adresses ou votre boîte de réception dans Outlook pour savoir quelles données vous conservez, mais cette méthode risque de ne pas être très efficace pour avoir un aperçu exhaustif de toutes les données que vous traitez.

Nous vous recommandons donc de suivre un certain nombre d'étapes :

#### Déterminez pour quelles données vous êtes « responsable de traitement »

Les données personnelles peuvent être traitées de deux manières : en tant que responsable de traitement ou en tant que sous-traitant.

* Le responsable de traitement est la personne qui détermine la finalité et les moyens de traitement. En d'autres termes, le responsable du traitement décide pourquoi les données doivent être traitées, quelles données doivent être traitées et comment elles sont traitées. En d’autres termes encore, vous êtes le responsable du traitement lorsque vous collectez et traitez des données pour vous-même et déterminez également la façon dont vous effectuez ce traitement.
* Un sous-traitant est la personne qui traite les données *pour le compte* d'un responsable de traitement. Il ne traite donc pas les données pour lui-même, mais pour quelqu'un d'autre. Un exemple typique est l’opérateur postal : il traite les adresses de personnes physiques pour leur livrer du courrier, non pas pour lui-même, mais pour un client. Outlook constitue un autre exemple : le fichier d'adresses que vous stockez dans Outlook est constitué de données personnelles traitées par Outlook. Mais Outlook ne peut pas contacter ces personnes lui-même: Outlook ne peut que traiter ces données pour vous, afin que vous puissiez leur envoyer des courriers électroniques Outlook. D'autres exemples sont les secrétariats sociaux, les sociétés informatiques chargées de la maintenance de vos logiciels ou serveurs, les logiciels de comptabilité, les logiciels de mailing, les services de colis, les agences de mailing publicitaires, etc.

Dans la plupart des cas, les titulaires des professions économiques, sur base notamment de l’indépendance qui les caractérise, seront responsables de traitement.

L’Institut des réviseurs d’entreprises a publié une communication sur le sujet dont nous vous invitons à prendre connaissance [ici](https://www.ibr-ire.be/fr/actualites/news-detail/communication-2018-13).

Ce n’est qu’exceptionnellement, par exemple si vous gérez l’administration des salaires pour le compte d’un client, sans devoir prendre aucune décision quant à la finalité et aux moyens du traitement des données, que vous agissez en qualité de « sous-traitant ».

Si vous agissez en qualité de « sous-traitant » pour certaines activités, vous devez, en tout état de cause, également suivre les différentes étapes de la présente feuille de route pour ces activités.

L’intérêt de la distinction entre la qualification de responsable de traitement et de sous-traitant se situe sur le plan de la responsabilité et des obligations à l’égard de la personne concernée et de l’Autorité de la protection des données

#### Vérifiez à quelles fins vous traitez les données

Les données ne sont pas traitées sans raison, mais toujours pour atteindre une finalité spécifique.

Vous traitez les données de vos clients pour pouvoir remplir les missions qu’ils vous confient.

Vous conservez les données du personnel afin de leur payer un salaire.

Par "finalité", nous entendons la raison pour laquelle vous traitez ces données. Nous ne visons pas ici les systèmes dans lesquels vous conservez les données (la finalité constitue par exemple le traitement comptable mais non le système, ni le cloud ou le document excel sur lequel vous conservez les données.)

**Dans le contexte du RGPD, il est très important que vous examiniez attentivement les finalités de vos traitements de données**. C’est l’une des étapes les plus importantes du RGPD. La finalité retenue, formera la base de toutes les autres étapes de l’implémentation du RGPD et déterminera ce que vous pouvez faire avec vos données, combien de temps vous pouvez les garder, ....

Une entreprise "standard" poursuit une moyenne de 5 à 7 finalités, selon qu’elle emploie du personnel ou non, et / ou qu’une surveillance à l’aide de caméras est utilisée :

1. La gestion des relations avec les clients (vos clients personnels)
2. La gestion des relations avec les fournisseurs (vos propres fournisseurs)
3. La gestion des clients et des fournisseurs du cabinet
4. Le Direct Marketing (ou la gestion des prospects)
5. La Communication / Public Relations
6. La gestion du personnel (si d’application)
7. Les caméras de surveillance (si d’application)
8. …autres

Ces finalités ne sont bien entendu pas les seules finalités possibles. Il est parfaitement possible que vous traitiez des données au sein de votre entreprise à d’autres fins (inscription du visiteur dans le registre des visiteurs ou comportement de navigation sur le site Web par exemple). Dans ce cas, vous devrez donc simplement les ajouter à votre liste des finalités.

**TO DO**

1. Vérifiez si vous exercez vos missions en qualité de responsable de traitement ou de sous-traitant.
2. Répertoriez bien les finalités justifiant les traitements de données à caractère personnel que vous opérez
3. Pour chaque finalité identifiée, répertoriez ensuite quelles sont les données que vous traitez (voyez ci-dessous).

#### Quelles catégories de données traitez-vous ?

**Astuce**

Il n'est pas nécessaire de décrire en détail les données que vous traitez. Il suffit de travailler avec des « catégories» de données. Il n'est donc pas nécessaire de dire "je collecte les nom, prénom, adresse postale, adresse e-mail, numéro de téléphone, ...", mais il suffit de dire "je collecte les données d'identification"

Lorsque vous traitez des données à caractère personnel, vous devez tenir compte du fait que certaines données peuvent être perçues comme « sensibles » par la personne concernée. Il s’agit de données qui sont **sensibles par nature**. Un exemple typique est le salaire d'un employé. Parmi ces données sensibles par nature, il y a en particulier les données de groupes vulnérables, tels que les employés, les couches vulnérables de la population (tels que les malades mentaux, les demandeurs d'asile, les personnes âgées, les patients, les enfants), etc. Par conséquent, si vous traitez des données de ces groupes plus vulnérables, il vous incombe de les considérer comme des données sensibles. Vous devrez également essayer d'estimer quelles données peuvent être perçues comme sensibles par les personnes concernées. Il est important que vous fassiez cet exercice car, dans les étapes suivantes, nous verrons que ces données sensibles nécessitent une vigilance accrue. Dans notre secteur, il est clair que beaucoup de données seront perçues comme sensibles.

En outre, vous devez également prendre en compte les « **catégories spéciales de données à caractère personnel** ». Celles-ci sont clairement définies dans le RGPD. Cela concerne :

1. Les données relatives à la race, l'origine ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance à un syndicat, le comportement sexuel ou l'orientation sexuelle,
2. Les données sanitaires, données génétiques et données biométriques

Vous devez également détecter correctement ces données, car le RGPD interdit le traitement de ces données, sauf dans des cas très strictement définis.

Exemples de données à caractère personnel

* + Données d'identification personnelles (nom, adresse, téléphone, courrier)
  + Numéro de registre national / numéro d'identification de sécurité sociale
  + Données d'identification électronique (adresse IP, cookies)

Données d'identification financière (numéro de compte bancaire)

* + Transactions financières (paiements que la personne a effectués ou doit encore effectuer)
  + Activité professionnelle (employeur, titre, ...)
  + Données personnelles spécifiques (âge, sexe, date de naissance, lieu de naissance, état civil, nationalité, ...)
  + Composition de la famille (nom du partenaire, numéro, enfants, ...)
  + Loisirs et intérêts (loisirs, sports, autres intérêts)
  + Affiliation à un syndicat
  + Appartenance à un parti politique
  + Appartenance à une autre association
  + Formation et éducation
  + Enregistrement video
  + Comptes de réseaux sociaux (données relatives à Facebook, Twitter, Linked-In, ...)
  + ...
  + Données des groupes vulnérables?
  + Catégories spéciales de données à caractère personnel (race, santé, données biométriques / génétiques, orientation sexuelle, ...)?

#### Quelles sont les personnes dont vous traitez les données ?

Les « personnes concernées» sont les personnes physiques à propos desquelles des données à caractère personnel sont traitées. Elles ne doivent pas être désignées par leur nom. Il suffit de les décrire à travers des catégories générales telles que "clients", "fournisseurs", "prospects", "employés", "candidats",

### *Comment avez-vous collecté ces données ?*

Enfin, assurez-vous de savoir comment vous avez obtenu ces données. Le client, par exemple, a-t-il fourni les données lui-même ? Avez-vous acheté ou recherché des fichiers d'adresses sur Internet ? Suivez-vous les personnes qui visitent votre site Web ?

Si vous avez cartographié tout cela, vous êtes prêt pour l'étape 2.

**Checklist**

|  |
| --- |
| * **J’ai un aperçu des missions pour lesquelles j’agis en tant que responsable de traitement et de celles pour lesquelles je suis le sous-traitant.** * **J’'ai une vue d'ensemble des finalités pour lesquelles je traite des données.** * **Pour chaque finalité, j'ai un aperçu des catégories de données à caractère personnel que je traite et des catégories de personnes auxquelles ces données se rapportent.** * **J'ai vérifié si je traitais des données sensibles ou des catégories spéciales de données personnelles.** * **J'ai vérifié comment je collecte ces données.** |