|  |
| --- |
| **Le RGPD en 10 étapes**Etape 2- Identifiez comment vous traitez les données  |

## **Le RGPD en 10 étapes**

## **Etape 2 – Identifiez comment vous traitez les données**

### Introduction

Dans l'étape précédente, vous avez répertorié les différentes données que vous traitez. Au cours de l'étape 2, nous examinons comment vous traitez ces données. Pour le GDPR, il ne suffit pas, en effet, de simplement donner un aperçu des données que vous traitez, vous devez également pouvoir démontrer que vous traitez ces données correctement. Pour savoir comment vous traitez les données et si cela se fait correctement, nous devons répondre aux 7 questions suivantes :

1. Les données que vous traitez sont-elles proportionnelles ?
2. Traitez-vous les données uniquement pour les finalités que vous avez communiquées ?
3. Les données que vous traitez sont-elles exactes ?
4. Quelle est la base juridique du traitement de la donnée ?
5. Demandez-vous le consentement de façon correcte ?
6. Combien de temps conservez-vous les données collectées ?
7. Transmettez-vous des données à des tiers ?

C’est l’étape la plus longue et peut-être aussi la plus difficile de cette feuille de route. Prenez donc tout votre temps pour parcourir cette étape.

Il vous faut également prendre en compte que vous ne pourrez pas vous conformer au GDPR à 100%. Personne ne peut prétendre à cela. En tout état de cause cela ne correspond pas non plus aux attentes du GDPR. Il est en revanche demandé que vous puissiez justifier les choix que vous ferez en répondant aux questions ci-dessous. Réfléchissez bien et veillez à documenter les raisons qui ont orienté vos choix et décisions en la matière.

###

### Avant de commencer : ‘Privacy by design’ et ‘privacy by default’

Voilà deux concepts difficiles pour indiquer que vous devez prendre les mesures qui s’imposent afin de garantir le respect des principes du GDPR tant au moment de la définition de la façon dont vous allez traiter les données et des moyens que vous allez mettre en place à cet effet (« privacy by design ») qu’au moment du traitement en tant que tel (« privacy by default »)

L'un des principes fondamentaux de ces deux concepts est que vous ne pouvez traiter que les données réellement nécessaires pour chaque finalité, et plus spécifiquement en ce qui concerne :

* La quantité de données que vous collectez ;
* Dans quelle mesure les données sont traitées ;
* Le délai de conservation des données ;
* L'accessibilité des données

**Concrètement, qu’est-ce que cela signifie ?**

* Si vous développez des programmes ou des applications dans lesquels des données personnelles sont traitées, assurez-vous que les paramètres par défaut sont définis de manière à ce que les données en question soient protégées au maximum, par exemple :

o Ne pas fournir trop de champs ouverts

o Ne pas travailler avec des cases pré-cochées

o Prévoir l’obligation pour la personne concernée d’indiquer à l’avance qu’elle a bien lu vos clauses d’information.

* Si vous achetez des programmes ou des applications, vous devez demander (et vérifier) ​​si le fournisseur a prévu ces deux principes et, par conséquent, si ses produits sont conformes au GDPR.

###

### 1ere  question : les données que vous traitez sont-elles bien proportionnelles ?

Comme indiqué précédemment, **la finalité pour laquelle vous traitez les données est cruciale pour savoir ce que vous pouvez faire avec les données**. Selon le GDPR, les données traitées doivent être adéquates, pertinentes et non excessives» pour chaque finalité.

L'essentiel est que vous ne pouvez traiter que les données nécessaires et pertinentes par rapport à l'objectif pour lequel elles ont été traitées.

Par exemple: dans le cadre de la finalité « administration du personnel » vous devez bien sûr connaître le nom des membres du personnel et leur numéro de compte bancaire. Le traitement des détails d’une évaluation n’est en revanche pas nécessaire au paiement des salaires. En principe, seul le résultat de l'évaluation est pertinent et donc proportionnel car il conduit (peut-être) à un bonus. Le détail de l'évaluation est uniquement pertinent et donc proportionné dans le cadre du traitement "gestion du personnel" (aspects HR).

**TO DO**

Une donnée qui n'est pas proportionnée à la finalité poursuivie ne peut plus être traitée dans le cadre de cette finalité. Si vous ne pouvez pas justifier la proportionnalité pour une finalité donnée, vous devez vous assurer que vous ne traitez plus ces données dans le cadre de cette finalité.

###

### 2e question : traitez-vous les données uniquement pour les finalités que vous communiquez ?

Le GDPR implique non seulement que vous ne pouvez traiter que les données qui sont proportionnées au regard d’une finalité donnée, mais aussi que vous ne pouvez utiliser les données traitées dans le cadre d’une finalité donnée *que pour cette finalité*.

Par exemple: les données que vous collectez pour la gestion des clients ne peuvent pas être utilisées à d'autres fins (telles que le marketing direct), sans en informer la personne concernée au préalable ou sans demander une autorisation.

Autrement dit, vous devez, avant de commencer le traitement d’une donnée à caractère personnel, informer la personne concernée de la (des) finalité(s) pour lesquelles vous traitez la donnée. Vous ne pouvez pas traiter ces données ultérieurement à d’autres fins que celles que vous avez indiquées au préalable, à moins que la personne concernée ne vous ait donné son consentement pour ce faire.

Cela nécessite, comme c'est souvent le cas dans le GDPR, un peu de « bon sens ». Vous devrez estimer quels traitements sont « raisonnablement prévisibles » au sein d’une finalité.

Par exemple :

* Il est logique que vous transmettiez les données salariales de vos employés à l'ONSS et au SPF Finances au sein de la finalité « administration du personnel ». Cela ne doit pas être considéré comme un "objectif" distinct.
* Si, par contre, lorsque vous obtenez des informations de vos clients, vous indiquez simplement que vous avez besoin de ces informations à des fins de "gestion des clients", vous ne pouvez plus vendre ces données à des tiers sans obtenir au préalable l’accord de vos clients pour ce faire, ni leur adresser des offres de marketing direct, car cela doit raisonnablement être considéré comme un autre objectif.

À l'étape 4, nous expliquons comment informer correctement la personne concernée.

### 3e question : les données que vous traitées sont-elles exactes ?

Vérifiez si les données que vous conservez et traitez sont bien exactes. Si vous avez des doutes sur l'exactitude des données que vous conservez, il est préférable de les vérifier auprès de la personne concernée.

Remarque : vous ne devez pas pouvoir garantir que toutes les informations personnelles sont correctes. Vous devez pouvoir démontrer que vous avez pris toutes les mesures raisonnables pour vous assurer que les données sont les plus exactes possibles.

### 4e question : quelle est la base juridique de vos traitements de données ?

Vous aurez déjà remarqué que, lorsque nous parlons du RGPD, le consentement est souvent brandi comme étant la panacée, permettant de traiter toutes les données à caractère personnel.

Or, ce raisonnement n’est pas correct. Ce que le RGPD exige en revanche, c’est que vous disposiez d’une base juridique valide pour chaque traitement de donnée à caractère personnel.

Le consentement ne constitue que l’une de ces bases juridiques. Le RGPD fournit encore cinq autres bases juridique possibles. Vous avez donc le choix entre les 6 bases juridiques suivantes :

1. Le traitement est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie ou dans la phase précontractuelle, à la demande de la personne concernée ;
2. Le traitement est nécessaire au respect d'une obligation légale (incombant au responsable du traitement) (par exemple, l'obligation de facturer ou de payer des salaires au personnel) ;
3. Le traitement est nécessaire dans le cadre des intérêts légitimes du responsable du traitement ou d'un tiers, à condition que les intérêts ou les libertés et droits fondamentaux de la personne concernée ne soient pas lésés ;
4. La personne concernée a donné son consentement au traitement de ses données à caractère personnel à une ou plusieurs fins spécifiques ;
5. Le traitement est nécessaire à la protection des intérêts vitaux de la personne concernée ou d'une autre personne physique ;
6. Le traitement est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement.

Pour vous, ce sont principalement les 4 premières bases juridiques qui seront pertinentes.

Inutile donc de demander le consentement à tout bout de champ. Vous devez simplement veiller à pouvoir invoquer l’un des fondements ci-dessus et être en mesure de justifier votre choix.

Comme vous le constaterez dans l’exemple ci-dessous, vous verrez que vous ne devrez que rarement demander le consentement.

**Exemple**

Si nous appliquons cela aux finalités citées dans la première étape, cela donne ceci :

1. Gestion des relations avec les clients
	* Nécessaire à l’exécution d’un contrat
	* Dans certains cas, obligation légale (par exemple application des lois AML)
2. Gestion des prospects (ou le Direct Marketing)
	* Collecte de données concernant des prospects : intérêt légitime (liberté d’entreprendre))
	* Direct marketing vers les clients et les adresses mails impersonnelles : intérêt légitime (liberté d’entreprendre)
	* Direct marketing vers les prospects : consentement
3. Gestion des relations avec les fournisseurs
	* Nécessaire à l’exécution d’un contrat
4. Comptabilité
	* Nécessaire à l’exécution d’un contrat
	* Obligation légale
5. Communication/Public Relations
	* Intérêt légitime (liberté d’entreprendre)
6. Administration du personnel
	* Nécessaire à l’exécution d’un contrat de travail
	* Obligation légale (tout ce qui concerne le paiement des salaires et des données qui doivent être transmises à l’ONSS et au SPF Finances)
	* Intérêt légitime (par exemple si vous effectuez un contrôle sur les moyens de communication en ligne de votre personnel)
7. Caméra de surveillance
	* Intérêt légitime (controle de la sécurité)

**Attention toutefois :** certaines catégories particulières de données à caractère personnel, comme les données sur la santé, la race, … ne peuvent être traitées, sauf dans des cas exceptionnels.

Si vous traitez de telles données, vous ne le faites en principe que :

* Si vous avez le consentement explicite de la personne concernée pour ce faire
* Pour satisfaire à une obligation légale
* Pour protéger des intérêts vitaux[[1]](#footnote-1).

Concrètement, il est possible qu’en tant que professionnel du chiffre vous preniez connaissance de données sensibles : vous faites par exemple la déclaration fiscale de quelqu’un qui est membre d’un syndicat ou qui est membre d’un parti politique ou d’un couple homosexuel.

Vous êtes responsable de la comptabilité d’un parti politique local. Vous conservez une copie des cartes d’identité électronique ou de passeports sur lesquels figurent des données biométriques. Vous traitez la comptabilité d’un médecin et avez une vue sur sa patientèle.

Contrôlez la situation pour votre cabinet et complétez le cas échéant :

 [ ]  Je traite des données sensibles :

 Je tombe sous l’une des exceptions mentionnées de type

[ ] Obligation légale : AML/ CIR (déclaration fiscale)

#### Ai-je besoin du consentement pour envoyer une newsletter ?

En principe oui, mais pas sur la base du RGPD. Pour faire barrage au spamming, la directive e-Privacy impose d’obtenir le consentement *préalable, libre, spécifique et informé* des personnes physiques pour l’envoi d’e-mails publicitaires (*opt-in*). Cette règle connaît toutefois deux exceptions en ce qui concerne :

* Les personnes physiques qui sont déjà clientes chez vous, pour autant que
* vous ayez reçu les données en direct du client ;
* que les données ne soient utilisées que pour des produits/services similaires ;
* et que le client puisse se désinscrire gratuitement.
* Les mailings vers des adresses impersonnelles du type « info@... » sont autorisés sans consentement préalable. Il doit également être possible de se désinscrire gratuitement.

La question consiste dès lors à savoir durant combien de temps une personne peut être considérée comme « cliente » ? Il vous revient de déterminer vous-même un délai durant lequel vous la considérez en qualité de cliente. Une distinction peut par exemple être faite entre les clients réguliers et les clients ponctuels que vous devrez plus rapidement considérer en qualité de « prospects ».

#### Qu’en est-il en ce qui concerne la publicité par courrier postal ou par téléphone ?

La publicité par courrier postal peut en principe continuer à être envoyée sur base de l’intérêt légitime de la liberté d’entreprendre (pour autant que la personne concernée ait la possibilité de s’y opposer).

En ce qui concerne la publicité par téléphone, la liste « Ne m’appelez plus » doit être consultée. Tant les personnes physiques que les personnes morales ont le droit d’enregistrer leur numéro de téléphone sur cette liste, après quoi vous ne pouvez plus les contacter par téléphone en vue de leur faire part d’un message commercial. L’accès à la liste est payant. Si vous faites de la prospection par téléphone, consultez le site https://www.dncm.be/fr/.

### 5e question : sollicitez-vous le consentement de manière correcte ?

Selon le RGPD, le consentement doit être *libre, spécifique, éclairé et univoque*. En outre, le consentement doit toujours être un acte positif clair. N’utilisez donc pas de cases pré-cochées !

**Vérifiez ce qu’il en est dans votre cabinet et si vous suivez bien les principes suivants lorsque vous demandez le consentement :**

* Je prévois pour le consentement un choix libre : la personne concernée peut donner son consentement de manière explicite (« opt-in »).
* J’explique clairement à la personne concernée à quelles fins elle donne son consentement (cf. *droit à l’information*).
* Je ne déduis pas le consentement d’un silence, d’une case cochée par défaut ou d’une absence d’action.
* Je prévois la possibilité pour la personne concernée de retirer à tout moment son consentement. Retirez son consentement est aussi simple que de le donner; les modalités de retrait sont clairement indiquées.

Il est également important que le consentement donné puisse toujours être *contrôlé*. Cela implique que vous devez pouvoir démontrer qui a donné son consentement, quand et comment. Enregistrez de préférence ces informations dans un document, par exemple à l’aide des historiques des connexions au site web ou d’un système de signature électronique.

### ATTENTION : Enfants

Les enfants constituent une catégorie particulière de personnes concernées. Le RGPD prévoit des règles spécifiques en ce qui les concerne :

* Le fondement de l’intérêt légitime ne peut en principe être retenu
* Les informations fournies dans la clause de consentement / clause contractuelle / politique de confidentialité, doivent être particulièrement claires
* Il est recommandé de recueillir le consentement des parents/tuteurs

### Le cas échéant, reprenez la clause suivante dans votre politique de confidentialité :

« Le [RESPONSABLE DU TRAITEMENT] ne traite en principe pas de données à caractère personnel de et concernant des mineurs d’âge. En toute hypothèse, le [RESPONSABLE DE TRAITEMENT] ne traite jamais consciemment des données à caractère personnel de mineurs d’âge sans le consentement de leur représentant légal tel que requis pour utiliser les produits et services du [RESPONSABLE DE TRAITEMENT] et pour pouvoir exercer ensuite les droits concernant les données du mineur d’âge.

Si, des données de mineurs d’âge étaient malgré tout traitées de bonne foi, le [RESPONSABLE DE TRAITEMENT] les effacera le plus rapidement possible après prise de connaissance. »

### 6e question: durant combien de temps conservez-vous les données?

Les données à caractère personnel ne peuvent être conservées indéfiniment.

Le RGPD ne prévoit pas de délais légaux de conservation. C’est donc à vous de les déterminer.

Il ne sera a priori pas possible de prévoir un seul délai de conservation pour toutes vos données.

Vous devrez déterminer durant combien de temps il est justifié, selon vous, de conserver les différentes données en fonction des catégories auxquelles elles appartiennent.

Voici quelques pistes pour ce faire :

**Délais de conservation**

* **Conservation durant le traitement**

Il est clair que vous pouvez conserver les données à caractère personnel tant que vous en avez besoin pour la finalité à laquelle vous l’avez affectée.

Par exemple : Tant qu’une personne est cliente chez vous, vous pouvez garder ses données relatives à la gestion de la clientèle.

* **Conservation après le traitement**

Il arrive que vous soyez obligé légalement de conserver les données après leur traitement.

Nous pensons par exemple au délai légal de conservation durant 7 ans après l’émission d’une facture, et au délai légal de conservation de 5 ans pour les données relatives au personnel.

La législation comptable exige que les données soient conservées pendant 7 ans.

Le réviseur d’entreprises qui a exécuté une mission révisorale conserve le dossier d’audit pendant une durée de cinq ans à dater du rapport qui a été établi sur la base du dossier d’audit.

La loi anti-blanchiment prévoit l’obligation que les données collectées dans ce contexte soient conservées pendant 10 ans après la fin de la relation avec le client.

Indépendamment des obligations légales, vous pouvez avoir intérêt à conserver des données plus longtemps. Ainsi votre responsabilité contractuelle (dans la plupart des cas) peut être engagée durant 10 ans après la fin de la relation contractuelle (délai de prescription pour d’éventuelles demandes en justice formulées par votre cocontractant).

Vous pouvez donc parfaitement justifier que vous devez conserver les données à caractère personnel qui sont nécessaires pour l’exécution d’un contrat durant ce délai de prescription.

* **Délai d’archivage**

Après les délais précités, ce sont les délais d’archivage qui commencent à courir. Le RGPD précise qu’à partir de ce moment-là, ce sont uniquement des données anonymisées qui peuvent être conservées. En outre, chaque personne concernée a le droit de demander l’effacement des données dès qu’elles sont archivées au sens du RGPD.

Ces délais doivent également être portés à la connaissance des personnes concernées parmi les informations qui leur sont données.

S’il n’est pas possible de communiquer le délai de conservation en tant que tel, il faut au minimum donner les critères sur base desquels ces délais seront déterminés. Dans certaines politiques de confidentialité on voit apparaître le message suivant : « *Nous ne conservons pas vos données au-delà de ce qui est nécessaire par rapport à la finalité du traitement* »

Il est conseillé, lorsque c’est possible, de décrire le délai de conservation de façon un peu plus précise, par exemple : « *Après la fin du contrat, les données seront conservées durant 10 ans (étant donné que les demandes en justice sur base du contrat peuvent être introduites durant ce délai de 10 ans).* »

**TO DO**

Il est possible de prévoir un délai dans une application ou un programme à l’échéance duquel les données sont effacées.

Cela suppose que pour chaque donnée, le début du délai de conservation soit clairement établi.

Cela doit être fait de façon précise car l’effacement de données qui sont encore nécessaires peut être qualifié en tant que violation (fuite) de données.

Une alternative peut être de vérifier de façon périodique si les données en question sont encore nécessaires et les effacer si besoin ou si cela semble conseillé.

En outre vous devez veiller à ce que le délai de conservation soit le plus possible limité à ce qui est nécessaire :

* Il est par exemple parfaitement possible que dans l’hypothèse d’une demande en justice d’une personne concernée, seul un nombre limité de données doit être conservé. Dans ce cas, la conservation des autres données n’est en principe plus nécessaire. En pratique il sera toutefois très difficile d’effectuer le tri des données à conserver ou non.

Il doit alors être possible de conserver *toutes* les données durant le délai de prescription mais nous vous conseillons de limiter le plus possible les accès aux données qui ne sont pas absolument nécessaires.

* Prenez également en compte le fait que les exigences en ce qui concerne le délai de conservation pour les « données sensibles » seront plus élevées. Cela suppose par exemple que ces données soient davantage sécurisées en ne les conservant par exemple pas sur papier mais dans un fichier séparé, si possible à l’aide d’un software IT utilisant le cryptage des données et qui soit par exemple accessible à une seule personne.

### 7e question : transmettez-vous les données à des tiers?

Si vous transmettez des données à des tiers, ceux-ci sont appelés les « destinataires » de vos données.

Intuitivement vous déclarerez sans doute que vous ne transmettez pas de données à des destinataires. Nous attirons votre attention sur le fait que le terme « destinataires » est beaucoup plus large que ce que vous pouvez penser. Il ne s’agit pas seulement de la question de savoir par exemple si vous vendez ou transmettez des données à vos partenaires commerciaux.

Parmi le groupe des « destinataires » il y a également le groupe des « sous-traitants ».

Dans l’étape 1 nous avons vu que le sous-traitant est celui qui traite des données pour votre compte. Les secrétariats sociaux, les software comptables, les fournisseurs IT,… sont tous des « sous-traitants, et donc aussi des « destinataires ». Ce sont tous des tiers qui reçoivent des données de votre part.

**TO DO**

Répertoriez à qui vous transmettez vos données. Utilisez les catégories générales, comme :

* Les partenaires commerciaux
* L’Etat
* Les sous-traitants
* ….

Avez-vous analysé et répondu à toutes ces questions ?

Oui, alors vous êtes prêts pour l’étape 3.

**Checklist**

|  |
| --- |
| * **J’ai vérifié, pour chaque finalité, si les données sont correctes et proportionnelles ; les autres données sont supprimées.**
* **J’ai déterminé une base juridique pour toutes les données que je traite.**
* **Si je dois demander le consentement, j’ai vérifié que j’ai bien demandé le consentement de façon correcte.**
* **J’ai fixé un délai de conservation adéquat pour toutes les données.**
* **J’ai répertorié à qui je transmets des données à caractère personnel.**
 |

1. D’autres justifications possibles sont énumérées à l’article 9 §2 du RGPD : le traitement porte sur des données à caractère personnel qui sont manifestement rendues publiques par la personne concernée ; le traitement est nécessaire à la constatation, à l'exercice ou à la défense d'un droit en justice ou chaque fois que des juridictions agissent dans le cadre de leur fonction juridictionnelle; le traitement est nécessaire pour des motifs d'intérêt public ( la proportionnalité avec l’objectif poursuivi doit être garantie) ; le traitement est nécessaire aux fins de la médecine préventive ou de la médecine du travail, de l'appréciation de la capacité de travail du travailleur, de diagnostics médicaux, de la prise en charge sanitaire ou sociale, ou de la gestion des systèmes et des services de soins de santé ou de protection sociale ; le traitement est nécessaire pour des motifs d'intérêt public dans le domaine de la santé publique ; le traitement est nécessaire à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques. [↑](#footnote-ref-1)