|  |
| --- |
| **Le RGPD en 10 étapes**Étape 3 – Inventoriez vos mesures de sécurité  |

## **Le RGPD en 10 étapes**

## **Étape 3 – Inventoriez vos mesures de sécurité**

### Introduction

Lors des 2 étapes précédentes, vous avez identifié les données que vous traitez et la manière dont vous les traitez. L’étape 3 consiste à examiner de plus près la manière dont vous sécurisez les données que vous traitez. Il convient en effet de protéger les données à caractère personnel contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d’origine accidentelle.

Le RGPD impose au responsable du traitement et au sous-traitant de « **mettre en œuvre des mesures techniques et organisationnelles appropriées** ». Lors de l’évaluation du niveau de sécurité approprié, il est tenu compte des risques que présente le traitement, résultant notamment de la destruction, de la perte, de l’altération, de la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d’une autre manière, ou de l’accès non autorisé à de telles données, de manière accidentelle ou illicite.

**TO DO**

Avant de répondre aux questions ci-dessous, posez-vous les deux questions suivantes :

* Où conservez-vous les données ? Il est possible que vous conserviez certaines données dans un fichier Excel ou Access, mais aussi dans un environnement cloud ou dans un logiciel spécifique (programmes de mailing, de comptabilité, etc.), ou tout simplement sur papier.
* Contrôlez aussi qui a accès à ces données. Si vous conservez des données sur papier ; qui a accès à l’armoire où sont rangés ces documents ? Qui dispose d’un compte pour accéder au programme de comptabilité que vous utilisez ?

### Protection en fonction de...

Les mesures de sécurité précises que vous devez prendre dépendent d’une série de facteurs :

* **Les risques liés au traitement** :

Plus le risque est élevé, plus la sécurité doit être renforcée. Les risques dépendent des circonstances du traitement, à savoir sa nature, sa portée, son contexte et ses finalités.

* Pour citer un exemple, le « contrôle des moyens de communication en ligne des travailleurs » impliquera davantage de risques pour les personnes concernées que la finalité « gestion des clients » et nécessitera dès lors une protection accrue.
* Tenez compte du fait que le traitement de données sensibles impliquera un niveau de protection plus élevé. Le cas échéant, prenez contact avec un fournisseur IT pour connaître les possibilités qui s’offrent à vous.
* La portée du traitement joue également un rôle. Les mesures à prendre seront différentes si les données concernent quelques centaines ou quelques dizaines de milliers de clients.
* **L’état de la technique** :

Pour déterminer les mesures à prévoir pour gérer et maîtriser les risques, il faut tenir compte de l’état de la technique. Cela signifie qu’une mesure de sécurité appropriée aujourd’hui ne le sera peut-être plus demain.

* **Les coûts de mise en œuvre** :

Pour déterminer les mesures à prévoir pour gérer et maîtriser les risques, il peut être tenu compte des coûts de mise en œuvre. Ces coûts dépendent du contexte. Il est évident que les coûts de mise en œuvre des mesures de sécurité d’une PME moyenne seront bien inférieurs à ceux que devra engager un hôpital (de taille moyenne). Cela signifie également qu’il n’est pas toujours nécessaire d’opter pour la solution la plus chère.

#### **Quid des normes de certification, comme ISO 27000 ?**

En matière de sécurité, il est possible de s’appuyer sur certaines normes de certification, comme la norme ISO 27000. Les entreprises certifiées selon cette norme peuvent partir du principe que les mesures de sécurité qu’elles ont mises en place sont appropriées.

Il faut cependant garder à l’esprit que ces normes de certification ciblent (actuellement) principalement les aspects techniques de la sécurité de l’information et ne portent pas vraiment sur le cadre plus large de la protection des données à caractère personnel. Dès lors, elles n’offrent qu’une solution partielle au respect (global) du RGPD.

Pour de plus amples informations sur la cybersécurité, nous vous renvoyons aux brochures disponibles [ici](https://www.ibr-ire.be/fr/actualites/news-detail/pr-ts-pour-le-gdpr-consultez-notre-checklist-sur-mesure-pour-les-professions-conomiques).

### En pratique – exemples de mesures de sécurité

Nous vous présentons ci-dessous quelques exemples de mesures de sécurité envisageables. Comme nous l’avons déjà dit, il ne suffit pas de reprendre cette liste telle quelle : c’est à vous qu’il appartient de déterminer les mesures appropriées en fonction des données que vous traitez.

#### **Mesures techniques**

* Rendre les données temporairement illisibles au moyen d’un algorithme (« chiffrement »)
* N’autoriser l’accès aux données qu’en présence d’une combinaison de 2 éléments d’authentification personnelle ou plus, comme un identifiant + un mot de passe ou une carte d’identité + un mot de passe, etc. (« double authentification »)
* Prévoir des sauvegardes périodiques
* Tenir un journal (reprenant qui a eu accès à quelles données)
* Installer des pare-feux
* Installer des antivirus
* Installer un logiciel attirant l’attention sur l’échéance imminente d’une durée de conservation.
* ...

En ce qui concerne les catégories particulières de données à caractère personnel, il est certainement recommandé de mettre en œuvre certaines mesures techniques telles que la tenue d’un journal, le chiffrement et la double authentification. Si vous traitez beaucoup de données sensibles, il est préférable que vous demandiez à un fournisseur IT qu’il vous présente les possibilités existantes.

#### **Mesures organisationnelles**

* Fermer à clé les armoires où sont conservés les dossiers papier
* Fermer le local d’archives à clé
* Fermer à clé les bâtiments et/ou les locaux des serveurs
* Mettre en place un système de gestion des utilisateurs et des accès
* Faire signer une déclaration de confidentialité à tous les collaborateurs amenés (autorisés) à traiter des données à caractère personnel
* Sensibiliser les collaborateurs (les conscientiser à la sécurité de l’information) au moyen de directives diverses
	+ Élaborer des directives relatives à l’enregistrement de données à caractère personnel sur des supports d’information portables, comme des clés USB ou des ordinateurs portables
	+ Élaborer une politique d’impression
	+ Élaborer des directives relatives au partage de données avec des tiers
	+ Élaborer des directives relatives à la portée des demandes d’information
	+ Élaborer une politique relative aux mots de passe (suffisamment complexes, changement régulier, etc.)
* Mettre en place des procédures claires pour la gestion rapide et efficace des incidents liés à la sécurité des données
* ...

### Limitation de l’accès interne en tant que mesure de sécurité

Toute entreprise doit veiller à ce que seuls les collaborateurs ayant besoin des données dans l’exercice de leur fonction ou pour les besoins de leur service y aient accès. Il s’agit du principe du « *need to know* ».

Ce principe présente une double portée, à savoir les personnes d’une part, et l’objet d’autre part.

* Il détermine avant tout qui peut accéder aux données.
* Il définit ensuite à quelles données ces personnes peuvent accéder.

Exemple : les collaborateurs du service « administration salariale » ne doivent (peuvent) pas accéder aux données détaillées de l’évaluation ou des absences d’un travailleur. Il suffit qu’ils aient accès au résultat ou au fait pour pouvoir réaliser leurs tâches.

En fonction des données sensibles que vous traitez, nous vous recommandons d’élaborer une politique de protection des données fixant clairement quels collaborateurs ont accès à quelles données. En fonction de la sensibilité des données, il peut être recommandé de prévoir un système de « journal » visant à consigner tous les accès des collaborateurs (autorisés) à des données sensibles.

### Transfert de données à des tiers

La sécurité des données ne consiste pas uniquement à en limiter l’accès en interne (collaborateurs de l’entreprise), mais également à limiter les personnes externes pouvant y avoir accès. Autrement dit, vous devez veiller à ce que les données ne soient divulguées ou transférées qu’à des tiers autorisés.

Si vous mettez des données à la disposition de tiers non autorisés, vous vous rendez ou pouvez-vous rendre responsable d’une violation de la sécurité ou d’une fuite de données.

Le transfert de données à des tiers ne pose pas problème dans les cas suivants :

* Le transfert est prescrit ou imposé par le législateur
* Le destinataire du transfert est un sous-traitant approprié avec lequel vous avez conclu un contrat de sous-traitance
* Le transfert est compatible avec la finalité pour laquelle les données ont été initialement collectées et/ou reçues
* Le transfert s’appuie sur le consentement explicite des personnes concernées.

Si vous transférez des données à des tiers et que vous ne pouvez pas invoquer l’un de ces motifs, il peut être utile de prévoir une « finalité » distincte pour ce transfert.

Exemple : une entreprise qui souhaite vendre ou louer son fichier de clients à une autre entreprise est tenue d’obtenir le consentement explicite des clients concernés à cette fin.

Attention : le transfert de données à des tiers est en principe interdit dans les cas suivants :

* Le responsable du traitement est soumis au secret professionnel ou à un devoir de confidentialité
* Le transfert est interdit par la législation ou la réglementation
* Le transfert n’est pas compatible avec la finalité pour laquelle les données ont été initialement collectées et/ou reçues et ne peut s’appuyer sur le consentement explicite des personnes concernées.

### Transfert vers des pays tiers

Le RGPD ne s’applique qu’aux pays faisant partie de l’Espace économique européen (EEE)[[1]](#footnote-1). Afin de garantir la sécurité des données à caractère personnel, le RGPD prévoit toutefois la possibilité de transférer des données à caractère personnel vers des pays situés en dehors de l’EEE (« pays tiers »), mais uniquement dans certains cas.

Vous pourriez vous dire que cette situation ne vous concerne pas, parce que vous ne transférez jamais de données vers des pays en dehors de l’EEE, mais cela arrive plus souvent qu’on ne le pense. Si vous avez décidé de conserver certaines données dans un environnement cloud ou dans un logiciel spécifique, il n’est pas garanti que les serveurs de votre fournisseur se situent au sein de l’EEE. Si les serveurs sont en dehors de l’EEE, sachez que vous transférez en réalité des données vers un pays tiers.

Nous vous recommandons dès lors de demander à vos fournisseurs où se situent leurs serveurs. Il est probable que vous n’obteniez pas de réponse des grands acteurs internationaux et que vous deviez trouver la réponse vous-même dans leur politique relative à la protection de la vie privée ou dans leurs conditions générales[[2]](#footnote-2).

Si vous constatez qu’il y a effectivement transfert vers un pays tiers (parce que les serveurs se trouvent en dehors de l’EEE par exemple), vous devez procéder à quelques vérifications :

1. Vous devez vérifier si le pays concerné fait partie des 12 pays dont le niveau de sécurité a été qualifié de suffisamment élevé par l’UE pour que vous puissiez y transférer des données sans demander d’autorisation à l’Autorité de protection des données[[3]](#footnote-3). Vous trouverez la liste de ces pays sur <https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_fr>.
2. En ce qui concerne les États-Unis, vous devez vérifier si votre fournisseur figure sur la [liste Privacy Shield](https://www.privacyshield.gov/list). Si c’est le cas, vous pouvez lui transférer des données sans demander d’autorisation à l’Autorité de protection des données.

Si le pays tiers/l’entreprise concerné(e) ne figure dans aucune de ces deux listes, vous ne pouvez y transférer des données que moyennant la mise en œuvre de mesures spécifiques. Ces mesures sont toutefois particulièrement techniques et complexes. Étant donné qu’elles ne seront nécessaires que dans certaines situations, nous les ajoutons ci-dessous. Si le pays tiers/l’entreprise concerné(e) figure dans l’une des deux listes susmentionnées (liste des 12 pays ou liste Privacy Shield), vous pouvez simplement ignorer les développements ci-dessous et passer directement à l’étape 4.

### Mesures supplémentaires en cas de transfert vers des pays tiers

**Les mesures mentionnées ci-dessous ne s’appliquent que si vous devez transférer des données vers des pays situés en dehors de l’EEE et ne figurant pas dans la liste des 12 pays, ou à une entreprise américaine non reprise dans la liste Privacy Shield !**

Dans ce cas, le responsable du traitement ou le sous-traitant ne peut transférer des données que s’il a prévu des garanties appropriées et à la condition que les personnes concernées disposent de droits opposables et de voies de droit effectives.

Ces garanties appropriées peuvent être fournies au moyen d’instruments élaborés au niveau de l’Union européenne, à savoir :

* Des règles d’entreprise contraignantes (ou Binding Corporate Rules).

Cet instrument permet de transférer des données à caractère personnel entre les membres d’un groupe d’entreprises ou d’un groupe d’entreprises engagées dans une activité économique conjointe.

* Des clauses types de protection des données fixées par la Commission européenne. Il s’agit notamment du contrat de transfert de responsable du traitement à responsable du traitement (modèle 2004/915/CE) et du contrat de transfert de responsable du traitement à sous-traitant (modèle 2010/87/UE).
* Des clauses types de protection des données adoptées par une autorité de contrôle (nationale) et approuvées par la Commission européenne.
* Le cas échéant, un code de conduite approuvé ou un mécanisme de certification approuvé, assorti de l’engagement contraignant et exécutoire pris par le responsable du traitement ou le sous-traitant dans le pays tiers d’appliquer les garanties appropriées

Il ne sera pas toujours évident pour une PME de négocier un instrument offrant des garanties appropriées avec le destinataire dans un pays tiers. S’il s’avère impossible de mettre un tel instrument en place, le transfert peut avoir lieu selon l’une des deux possibilités suivantes :

#### Possibilité 1 : dérogations pour des situations particulières

Il ne sera pas toujours évident pour une PME de négocier un instrument offrant des garanties appropriées avec le destinataire dans un pays tiers.

S’il est impossible d’appliquer l’étape précédente, le transfert ne peut avoir lieu qu’à l’une des conditions suivantes (ici, nous partons du principe que le transfert n’est pas régulier et systématique, mais plutôt occasionnel et non répétitif) :

* Obtention du consentement explicite de la personne concernée (après communication des risques afférents au transfert)
* Exécution d’un contrat auquel la personne concernée est partie ou de mesures précontractuelles prises à la demande de celle-ci
* Conclusion ou exécution d’un contrat conclu dans l’intérêt de la personne concernée entre le responsable du traitement et une autre personne physique ou morale
* Constatation, exercice ou défense de droits en justice
* Sauvegarde des intérêts vitaux de la personne concernée ou d’autres personnes, lorsque la personne concernée se trouve dans l’incapacité physique ou juridique de donner son consentement

#### Possibilité 2 : intérêts légitimes impérieux

Si et seulement s’il s’avère impossible d’appliquer les étapes précédentes, le transfert peut éventuellement avoir lieu aux fins des intérêts légitimes impérieux poursuivis par le responsable du traitement.

Les conditions sont les suivantes

* Le transfert n’est pas autorisé sur la base des étapes précédentes
* Le transfert n’est pas fondé sur une décision d’adéquation
* Le transfert n’offre pas de garanties appropriées
* Aucune des dérogations pour des situations particulières n’est applicable
* Le transfert ne revêt pas un caractère répétitif
* Le transfert touche un nombre limité de personnes concernées
* Le transfert est nécessaire aux fins des intérêts légitimes impérieux poursuivis par le responsable du traitement, sur lesquels ne prévalent pas les intérêts ou les droits et libertés de la personne concernée
* Le responsable du traitement a évalué toutes les circonstances entourant le transfert de données et a offert, sur la base de cette évaluation, des garanties appropriées

Les mesures supplémentaires applicables sont les suivantes

* Le responsable du traitement est tenu d’informer l’autorité de contrôle
* Le responsable du traitement est tenu d’informer les personnes concernées du transfert et de ses intérêts légitimes impérieux en particulier

Ces conditions et mesures sont telles que l’application de cette possibilité restera plutôt exceptionnelle.

**Check-list**

|  |
| --- |
| * **J’ai vérifié si les mesures de sécurité que j’ai mises en œuvre sont suffisantes, compte tenu du type de données, de leur coût et des éventuels risques.**
* **J’ai prévu des mesures de protection supplémentaires pour les données sensibles.**
* **Je sais quels collaborateurs ont accès à quelles données et je limite cet accès aux collaborateurs qui en ont besoin dans l’exercice de leur fonction.**
* **J’ai vérifié si je transférais des données vers des pays tiers ou, le cas échéant, si j’offrais des garanties appropriées en matière de sécurité.**
 |

1. Il s’agit des États membres de l’UE, ainsi que de l’Islande, de la Norvège et du Liechtenstein. [↑](#footnote-ref-1)
2. Pour Facebook par exemple : <https://www.facebook.com/about/privacyshield> [↑](#footnote-ref-2)
3. Il s’agit du nouveau nom de la « Commission de la protection de la vie privée ». [↑](#footnote-ref-3)