|  |
| --- |
| **Le RGPD en 10 étapes**  Etape 10- Prévoyez une procédure en cas de fuite de données |

## **Le RGDP en 10 étapes**

## **Etape 10 – Prévoyez une procédure en cas de fuite de données**

### Introduction

Même si vous faites tout ce qu’il faut pour respecter le GDPR, vous pourriez toujours être amené à constater qu’une violation s’est produite. Il est question dans ce cas de fuite de données. Vous devez définir une procédure dans laquelle vous décrivez comment vous procédez en cas de fuite de données.

### Qu’est-ce qu’une fuite de données?

Une fuite de données est à interpréter au sens large. Ce terme est défini par le GDPR comme “une violation de la sécurité des données personnelles qui entraîne par accident ou de manière malintentionnée la destruction, la perte, l’altération, la divulgation ou l’accès non autorisé à des données transmises, stockées ou traitées de quelque manière que ce soit”.

Il s’agit par exemple de:

* l’indisponibilité des données, suite à une action de ransomware (“prendre en otage” des données en échange d’une rançon)
* La violation de l’intégrité, suite à une altération non autorisée des données
* la violation de la confidentialité des données, suite à la communication ou la mise à disposition de données à des personnes qui n’y sont pas habilitées ou autorisées. Ceci peut arriver tant par accident (une mauvaise manipulation des données) que de manière illégale (une conséquence d’un piratage d’ordinateur). Par exemple, un email est envoyé par inadvertance à une mauvaise adresse email.

#### A titre préventif – lignes directrices pour éviter des fuites de données

Chaque responsable du traitement doit faire en sorte que les collaborateurs soient sensibilisés à la question de la fuite des données en vue d’assurer une sécurité suffisante. Ceci implique que des lignes directrices soient établies et rappelées à intervalles réguliers (voir étape 8).

#### Procédure en cas de fuite de données – information en interne

Les collaborateurs doivent savoir comment réagir en cas de fuite de données. Ceci implique notamment qu’il soit indiqué vers qui (quel service ou personne) les collaborateurs peuvent se tourner s’ils perdent des supports de données déterminés, si des systèmes sont ou deviennent indisponibles, etc.

#### Procédure en cas de fuite de données – Equipe de gestion de crise

Il est recommandé dans les entreprises plus grandes de mettre en place une sorte d’’équipe de gestion de crise’. Cette équipe devra juger si la fuite de données comporte un risque et si par conséquent elle ne doit pas être notifiée à l’autorité de contrôle.

Il est recommandé que les personnes suivantes fassent partie de l’équipe de gestion de crise: le chef d’entreprise, le responsable du service informatique ou le partenaire informatique, la personne qui agit comme point de contact pour l’autorité de contrôle.

#### Inventaire des fuites de données

Le RGPD comporte l’obligation de documenter toutes les violations liées aux données personnelles. Ceci implique la rédaction d’un inventaire de toutes les fuites de données, indépendamment du risque y lié. Ainsi, l’autorité de contrôle peut vérifier, lors d’un contrôle ultérieur, si le responsable se conforme à son obligation de notifier ou de communiquer les fuites de données de manière appropriée.

Un tel inventaire doit également mentionner les fuites de données qui ne donnent pas lieu à un risque et qui ne doivent dès lors pas être notifiées à l’Autorité de protection des données ni communiquées à la personne impliquée. Ce qui en fait une obligation lourde, surtout administrative.

### Déclaration à l’Autorité de protection des données et à la personne concernée

A chaque fuite de données, vous devez analyser si la fuite présente un risque pour les droits et les libertés des personnes concernées. Si ce n’est pas le cas, une mention dans l’inventaire interne suffit.

S’il existe bel et bien un risque, vous devez signaler la fuite de données dans les 72 heures à l’Autorité de protection des données via un formulaire spécial que vous trouvez sur leur site internet : <https://www.autoriteprotectiondonnees.be/notification-fuites-de-donnees-general>

Si la fuite de données présente un *risque élevé* pour les droits et libertés des personnes concernées, vous devez également signaler vous-même cette fuite immédiatement aux personnes concernées.

**Checklist**

|  |
| --- |
| * **J’ai établi une procédure en cas de fuite de données.** * **J’ai informé mes collaborateurs au sujet de cette procédure et des mesures préventives.** * **Je dispose d’un inventaire des éventuelles fuites de données.** |

### Procédure en cas de fuite de données + Modèle de registre des fuites de données

## **Procédure**

**Etape 1:** Analysez si la violation concerne bel et bien des « données personnelles », et si oui, si vous êtes responsable du traitement de ces données personnelles.

**Etape 2:** analysez l’étendue de la fuite de données:

* De combien de données s’agit-il?
* Combien de personnes sont-elles concernées?
* Des données sensibles ont-elles été divulguées?
* Des données concernant des groupes vulnérables ont-elles été divulguées?

**Etape 3:** Analysez si la violation comporte un risque pour les droits et les libertés des personnes physiques concernées par les données.

Par exemple: Si par inadvertance, vous envoyez un email contenant des données personnelles à un collègue, qui ne devait pas recevoir cet email, il s’agit d’une violation d’un point de vue technique. Toutefois, le risque de cette violation pour la personne concernée est toutefois très limité parce qu’il s’agit d’un collègue et que les données personnelles de seulement une personne sont en jeu. Par contre, si vous deviez rendre public par inadvertance une partie de votre fichier clientèle, il s’agirait d’un risque élevé pour les personnes concernées.

**Etape 4:** N’existe-t-il aucun risque pour les droits des personnes concernées?

Dans ce cas, il suffit de reprendre la violation dans le registre des fuites de données ci-dessous. Sur la base de ce registre, vous pouvez alors évaluer à terme si des mesures complémentaires sont nécessaires à tel ou tel endroit.

**Etape 5:** Existe-t-il bien un risque pour les droits des personnes concernées? Dans ce cas, vous devez le signaler à l’Autorité de protection des données (dans les 72 heures) et aux personnes concernées (immédiatement).

* 1. Avec mention de :
     1. La nature de la violation
     2. Des catégories de personnes concernées et des données personnelles, et approximativement le nombre de celles-ci
     3. Nom et données de contact où l’Autorité de protection des données peut vous contacter pour davantage d’informations
     4. Les conséquences probables de la violation
     5. Les mesures que vous proposez ou que vous avez déjà prises pour vous attaquer à la violation et en limiter les conséquences.
  2. La déclaration à l’Autorité de protection des données se fait via un formulaire spécifique que vous trouvez sur leur site internet: <https://www.autoriteprotectiondonnees.be/notification-fuites-de-donnees-general>

## **Registre des fuites de données**

Veuillez remplir ce registre chaque fois que vous constatez une fuite de données, que celle-ci doive ou non être notifiée à l’Autorité de protection des données ou à la personne concernée.

**Responsable du traitement:**

* **Nom: …**
* **Adresse: …**
* **Numéro d’entreprise:…**
* **Date de la fuite de données:** ………………………
* Description de la fuite de données: : ……………………………………………………………………………………………………………………………………………………..………………………………………………………………………………………………………………………………………………………………..
* Mesures en vue d’éviter une fuite de données à l’avenir : ……………………………………………………………………………………………………………………………………………………..………………………………………………………………………………………………………………………………………………………………..
* (si applicable): la fuite de données a été notifiée le [*date]* :

……………………………………………………………………………………………………………………………………………………..……………………………………………………………………………………………………………………………………………………………………..

* **Date de la fuite de données:** ………………………
* Description de la fuite de données: : ……………………………………………………………………………………………………………………………………………………..………………………………………………………………………………………………………………………………………………………………..
* Mesures en vue d’éviter une fuite de données à l’avenir : ……………………………………………………………………………………………………………………………………………………..………………………………………………………………………………………………………………………………………………………………..
* (si applicable): la fuite de données a été notifiée le [*date]* :

……………………………………………………………………………………………………………………………………………………..……………………………………………………………………………………………………………………………………………………………………..

* **Date de la fuite de données:** ………………………
* Description de la fuite de données: : ……………………………………………………………………………………………………………………………………………………..………………………………………………………………………………………………………………………………………………………………..
* Mesures en vue d’éviter une fuite de données à l’avenir : ……………………………………………………………………………………………………………………………………………………..………………………………………………………………………………………………………………………………………………………………..
* (si applicable): la fuite de données a été notifiée le [*date]* :

……………………………………………………………………………………………………………………………………………………..……………………………………………………………………………………………………………………………………………………………………..