LA GESTION DES DROITS DES PERSONNES CONCERNÉES DANS LES PME

Règlement général sur la protection des données (RGPD)

BOOST: UN GUIDE CONDENSÉ

Projet BOOST - Booster la connaissance et le respect du RGPD chez les PME belges, en se concentrant sur trois thèmes principaux

Autorité de protection des données
Gegevensbeschermingsautoriteit

UNIVERSITÉ DE NAMUR

VUB VRIJE UNIVERSITEIT BRUSSEL

KU LEUVEN

Ce projet est financé par le programme Droits, Egalité et Citoyenneté REC-AG-2019 de l'Union européenne.

LA GESTION DES DROITS DES PERSONNES CONCERNÉES DANS LES PME

1. INTRODUCTION

Si votre entreprise traite des données à caractère personnel de personnes physiques résidant dans l'Union européenne, depuis mai 2018, elle doit tenir compte du **Règlement général sur la protection des données** (RGPD), mieux connu sous le nom de General Data Protection Regulation (GDPR) en anglais. Le RGPD régit la manière de gérer les données à caractère personnel - pensons aux noms, numéros de téléphone, adresses e-mail, coordonnées, etc. - afin qu'elle se fasse consciencieusement.

Les entreprises qui ne respectent pas la réglementation s'exposent à des amendes.

Le RGPD prévoit des **«droits des personnes concernées»**. Les personnes concernées sont les personnes dont vous traitez des données à caractère personnel. Il est important pour votre entreprise d'être informée de ces droits et de savoir quelle attitude adopter si des personnes concernées les invoquent. La présente brochure aide les petites et moyennes entreprises (PME) à agir correctement si cette situation se présente. Après une explication générale des droits des personnes concernées, vous trouverez des informations sur les démarches à entreprendre et quelques exemples concrets.

QUELS SONT LES DROITS DES PERSONNES CONCERNÉES ?

01 - ACCÈS

Les personnes concernées ont le droit de savoir si leurs données à caractère personnel sont collectées et traitées par votre entreprise et si oui, d'accéder à ces données. Elles ont le droit d'obtenir une copie de ces données ainsi que des informations sur le traitement de celles-ci.

02 - LIMITATION DU TRAITEMENT

Une limitation du traitement gèle le traitement de données. Cela signifie que l'entreprise peut encore seulement conserver les données à caractère personnel et doit cesser toutes les autres activités de traitement. Les personnes concernées ont le droit de demander au responsable du traitement une limitation du traitement si une des situations suivantes s'applique : 1/ les données à caractère personnel sont inexactes, la personne concernée l'a signalé et votre entreprise n'a pas encore contrôlé si elles sont correctes, 2/ le traitement est illicite, mais la personne concernée ne veut pas que les données à caractère personnel soient supprimées, 3/ les données à caractère personnel ne sont plus nécessaires pour les finalités visées, mais la personne concernée a besoin des données pour une action en justice (par ex. une procédure juridique), et/ou 4/ la personne concernée s'est opposée au traitement mais votre entreprise souhaite quand même le poursuivre en raison de certains intérêts et on ne sait pas clairement quels intérêts prévalent.

03 - OUBLI

Les personnes concernées ont le droit de demander au responsable du traitement de supprimer des données à caractère personnel lorsque 1/ les données à caractère personnel ne sont plus nécessaires pour les finalités du traitement, 2/ le consentement a été retiré (pas d'autre base juridique pour le traitement), 3/ la personne concernée s'oppose au traitement, 4/ les données à caractère personnel ont été traitées de manière illicite, 5/ le délai de conservation légal a expiré et/ou 6/ la personne concernée a moins de 16 ans et les données ont été collectées via une application ou un site Internet.

04 - RECTIFICATION & COMPLÉMENT

Les personnes concernées ont le droit de faire rectifier et/ou de faire compléter des données à caractère personnel inexactes, par ex. si les données à caractère personnel ne sont pas correctes ou pas complètes.

05 - PORTABILITÉ DES DONNÉES

Les personnes concernées ont le droit de recevoir les données à caractère personnel qu'elles ont fournies à votre entreprise et de transmettre ces données à un autre responsable du traitement s'il s'agit 1/ de données à caractère personnel que votre entreprise traite sur la

base du consentement ou si le traitement est nécessaire à l'exécution d'un contrat et 2/ si le traitement est effectué par voie automatisée (ce droit ne s'applique pas aux dossiers papier).

06 - OPPOSITION AU TRAITEMENT

Les personnes concernées ont toujours le droit de s'opposer au traitement de leurs propres données à caractère personnel dans 2 situations :

- Les données à caractère personnel sont utilisées à des fins de marketing direct *(par ex. la personne concernée achète en ligne un ticket pour un spectacle mais reçoit par la suite des publicités pour d'autres concerts qu'elle ne souhaite pas recevoir)*
- La personne concernée s'oppose en raison de sa situation particulière *(par ex. des circonstances personnelles) (par ex. une compagnie d'assurance utilise des données afin de lutter contre les pratiques de blanchiment et peut dès lors refuser de donner suite à une opposition étant donné que la législation anti-blanchiment l'oblige à conserver les données).*

07 - LIMITATION DE LA PRISE DE DÉCISION AUTOMATISÉE & DU PROFILAGE

Une personne concernée ne peut pas faire l'objet d'une décision entièrement automatique - sans intervention humaine - qui l'affecte de manière significative ou qui a des effets juridiques.

La personne concernée a toujours le droit de s'y opposer sauf si la décision est nécessaire à la conclusion ou à l'exécution d'un contrat, est fondée sur le consentement de la personne concernée ou est autorisée par le droit de l'Union ou le droit d'un État membre.

08 - INFORMATIONS CLAIRES CONCERNANT LE TRAITEMENT DE DONNÉES

Les personnes concernées ont le droit de recevoir des informations concises, transparentes, compréhensibles et aisément accessibles sur le traitement de données à caractère personnel.

Les informations peuvent être communiquées par écrit, par voie électronique ou oralement (à la demande).

QUE DOIT FAIRE VOTRE ENTREPRISE ?

DEMANDE DE LA PERSONNE CONCERNÉE

Comme cela a été précisé, les personnes concernées peuvent invoquer divers droits en ce qui concerne le traitement de leurs données à caractère personnel. Quelles démarches votre entreprise doit-elle mettre en place afin d'accéder à une demande ? Cela dépend évidemment du droit invoqué par la personne concernée. Les pages ci-après abordent brièvement ces aspects.

Toutefois, de manière générale, votre entreprise doit être attentive à plusieurs éléments.

POINTS D'ACTION GÉNÉRAUX

1. Veillez à ce que vos **systèmes, vos processus et votre organisation interne** soient conçus en tenant compte des droits des personnes concernées *(par ex. prendre des mesures organisationnelles et techniques, veiller à ce que l'infrastructure IT y soit adaptée, mettre en place des procédures pour assurer une approche aisée, etc.)*

2. Tenez-vous informé des processus de traitement et des flux de données dans votre entreprise (quelles données à caractère personnel sont traitées, où sont-elles conservées, qui y a accès, etc.) Créez un registre des activités de traitement

3. Contrôlez **l'identité** de la personne concernée afin d'éviter de donner accès à des données à caractère personnel de quelqu'un d'autre. On ne peut pas exercer un droit sur les données à caractère personnel d'une autre personne. Réclamer la carte d'identité n'est possible qu'en cas de doute ou lorsque d'autres manières de vérifier l'identité *(par ex. l'accès via un portail en ligne)* ne suffisent pas

4. Vous êtes obligé **d'informer** les personnes concernées de manière claire et transparente sur le traitement de données à caractère personnel. Rédigez à cet effet une déclaration de confidentialité et publiez-la sur votre site Internet

5. Veillez à ce que les personnes concernées puissent exercer leurs droits

6. **Répondez** toujours (gratuitement) à la demande dans un délai d'un mois. La personne concernée doit savoir si sa demande est acceptée et dans le cas contraire, pour quels motifs

7. Examinez **lequel de vos travailleurs** est le plus à même d'assurer le suivi de l'exercice des droits et d'y répondre

8. **Conscientisez les travailleurs** à ce qu'est une demande d'une personne concernée et à la manière dont ils peuvent la reconnaître

ACCÈS

LA PERSONNE CONCERNÉE DEMANDE UN ACCÈS OU UNE COPIE À/DE SES DONNÉES À CARACTÈRE PERSONNEL, QUE FAIRE ?

Sophie a transmis ses nom, adresse, numéro de téléphone et adresse e-mail à votre agence d'intérim afin qu'un contrat puisse être établi. Ces données sont conservées dans une base de données en ligne afin qu'à l'avenir, des contrats puissent être rapidement établis en cas de besoin. Sophie souhaite toutefois savoir après quelques mois ce que votre agence d'intérim fait précisément de ses données et invoque son **droit d'accès**. Pas de panique ! Votre entreprise sait exactement quoi faire, à savoir :

- Fournir une copie des données à caractère personnel *(y compris la correspondance enregistrée telle que des conversations téléphoniques et des e-mails, des commentaires dans la marge d'un dossier ou CRM).*
  Il peut s'agir d'un relevé établi par vos propres soins *(pas de directive légale pour la présentation)* ou d'une copie des documents contenant des données à caractère personnel.
- Fournir des informations sur le traitement : finalités du traitement, catégories concernées de données à caractère personnel, destinataires des données à caractère personnel, délais de conservation, droits en matière de respect de la vie privée des personnes concernées, droit de porter plainte auprès de l'Autorité, logique de la prise de décision automatisée (si d'application), organisation qui a fourni les données à caractère personnel (si d'application).

Cela semble simple ? En réalité, cela peut toutefois être plus complexe.

En outre, votre entreprise doit mettre gratuitement une copie à disposition *(pour d'éventuelles copies suivantes, des frais raisonnables peuvent être réclamés).*

DANS QUELLES SITUATIONS CELA PEUT-IL CONSTITUER UN PROBLÈME ?

Situation 1 : Les données à caractère personnel de Sophie sont conservées dans plusieurs bases de données (par ex. fichiers en ligne, dossiers papier, programmes, boîtes mail) et le système informatique ne permet pas d'obtenir simplement un relevé. Votre entreprise ne sait pas quelles données à caractère personnel de Sophie sont traitées et conservées.

Quelles solutions pourront vous **aider** ??

- Disposer d'un relevé correct des différents flux de données et processus de traitement de votre entreprise (via un **registre des activités de traitement** par ex.)
- Créer une procédure et prendre des mesures techniques afin de donner accès aux personnes concernées. L'entreprise est responsable d'un transfert sûr. Veillez à ce que les données soient séparées des données à caractère personnel de tiers.

Situation 2: Sophie demande à son employeur pour accéder à toutes ses données à caractère personnel (et en demande une copie). Ces données à caractère personnel figurent dans des bases de données en ligne, des dossiers papier et des boîtes mail. La question est toutefois de savoir si Sophie doit uniquement accéder aux données à caractère personnel disponibles au service RH ou à toutes les données à caractère personnel enregistrées quelque part (par ex. des e-mails dans lesquels Sophie est citée). En d'autres termes, à quelles données à caractère personnel votre entreprise doit-elle donner accès ?

Quelles solutions pourront vous **aider** ??

Il est recommandé de demander (par écrit) à la personne concernée à quelles données elle souhaite accéder (et de délimiter ainsi la demande, par ex. en posant des questions supplémentaires).

PORTABILITÉ DES DONNÉES

LA PERSONNE CONCERNÉE VEUT FAIRE TRANSFÉRER SES DONNÉES

Cléo n'est plus satisfaite de son fournisseur d'e-mail et aimerait passer chez un concurrent. Toutefois, il est important que Cléo conserve sa liste de contacts qu'elle a soigneusement constituée. Dans le cadre du droit de Cléo à la portabilité des données, le fournisseur d'e-mail actuel est obligé :

- De mettre à disposition toutes les données à caractère personnel que Cléo a fournies, tant directement (par ex. une adresse e-mail sur un formulaire Internet) qu'indirectement (par ex. des données de localisation). Les données dérivées (par ex. un profil de consommateur) ne doivent pas être fournies.
- De le faire sous une forme structurée, couramment utilisée et lisible par machine *(pas de format spécifique prescrit)* pour un tiers et/ou de manière facile à télécharger pour la personne concernée elle-même.
- Astuce **!** En ce qui concerne le format, il est préférable de vérifier pour quelles raisons la personne concernée a besoin des données. *Par ex. Cléo veut obtenir ses données à caractère personnel pour conserver sa liste de contacts. Une bonne pratique serait d'envoyer les données de la liste de contacts dans un format standardisé.*

Comme nous venons de le voir, il n'est toutefois pas toujours si simple d'avoir une idée de toutes les données à caractère personnel qui sont collectées et traitées par votre entreprise. Cela complique évidemment considérablement le transfert de ces données. Afin de pouvoir répondre à cette demande, votre entreprise doit d'abord **rassembler les données à caractère personnel de la personne concernée** avant de pouvoir les mettre à disposition.

COMMENT VOTRE ENTREPRISE PEUT-ELLE RÉPONDRE À CETTE DEMANDE ? QUELQUES ASTUCES !

1. Dressez la liste des activités de traitement

   Veillez à connaître les processus de traitement de votre entreprise, via la création d'un **registre des activités de traitement** et examinez si la portabilité des données s'y applique. La portabilité des données s'applique uniquement lorsque des données sont traitées **de manière automatique** sur la base du **consentement ou d'un contrat**. Par ex. l'historique de recherche ou les données de localisation d'un client sur un webshop.

2. Établissez un inventaire des données

   Dressez la liste des **(flux de) données** et des finalités pour lesquelles elles sont conservées et traitées. Examinez quels tiers ont accès et quelles données sont conservées en externe.

3. Prenez des mesures organisationnelles et techniques pour permettre l'exercice du droit

   Rédigez des **procédures** internes afin de pouvoir réagir le plus rapidement possible à la demande de la personne concernée et veillez à ce que votre entreprise soit **techniquement** en mesure de fournir les données et/ou de les transmettre à un tiers.

OPPOSITION

LA PERSONNE CONCERNÉE S'OPPOSE AU TRAITEMENT DE SES DONNÉES À CARACTÈRE PERSONNEL

Éric s'oppose au traitement de ses données à caractère personnel par une entreprise. Il dispose de ce droit d'opposition dans **2 situations** :

1. Les données à caractère personnel sont traitées à des fins de (profilage de) **marketing direct**.

   RÉSULTAT : L'entreprise doit cesser d'envoyer des courriers publicitaires.

2. En raison de la **situation particulière** de la personne concernée. Uniquement possible si l'entreprise traite des données à caractère personnel sur la base d'une mission d'intérêt public ou d'un intérêt légitime *(par ex. Éric a participé à une étude médicale et l'on découvre plus tard qu'une connaissance travaille en tant que chercheur auprès du centre).*

   RÉSULTAT : L'entreprise doit cesser de traiter les données, à moins d'avoir de bonnes raisons pour poursuivre le traitement qui prévalent sur les intérêts de la personne concernée ou qui sont liées à une action en justice. L'entreprise doit bien documenter cet intérêt légitime de manière à pouvoir défendre cette pondération des intérêts de manière étayée par la suite.

LIMITATION DU TRAITEMENT

LA PERSONNE CONCERNÉE SOUHAITE QUE L'UTILISATION DE SES DONNÉES À CARACTÈRE PERSONNEL SOIT LIMITÉE (CE QUI EST POSSIBLE DANS LES SITUATIONS SUIVANTES)

Situation 1 : Valérie constate qu'il est possible que ses **données à caractère personnel** soient **inexactes**. Votre entreprise ne peut pas utiliser ces données tant que vous n'avez pas contrôlé si les données sont bel et bien exactes.

Situation 2: Votre entreprise ne peut pas traiter certaines données à caractère personnel mais Valérie ne veut **pas** que votre entreprise **efface** définitivement ces données (par ex. pour pouvoir à nouveau les demander ultérieurement).

Situation 3 : Votre entreprise n'a plus besoin des données de Valérie pour la finalité initiale du traitement, mais Valérie ne veut pas que votre entreprise efface les données car elles sont nécessaires pour une **action en justice**.

Situation 4 : Valérie s'est **opposée** au traitement de ses données en raison de sa situation particulière. Votre entreprise doit cesser le traitement, sauf si vous avez de bonnes raisons qui prévalent sur les intérêts de la personne concernée. Tant que cela n'est pas clair, votre entreprise ne peut pas utiliser les données.

Votre entreprise doit

- Réagir par écrit dans le délai d'1 mois pour faire savoir si la demande est acceptée, pourquoi (pas) et de quelle manière (si d'application) *(y compris le motif du refus)*
- EN CAS DE LIMITATION : Veiller à ce que les données à caractère personnel puissent encore seulement être conservées dès le moment où la personne concernée invoque ce droit
- Permettre l'exercice du droit, par ex. en créant des procédures internes (actualisées) et des mesures techniques
- Faire savoir à des tiers que le traitement de données est limité et l'indiquer dans les fichiers

OUBLI

LA PERSONNE CONCERNÉE VEUT FAIRE VALOIR SON DROIT À L'OUBLI À L'ÉGARD DE VOTRE ENTREPRISE ET FAIRE SUPPRIMER SES DONNÉES À CARACTÈRE PERSONNEL.

Situation 1 : Les données de localisation et l'historique d'achats de Younes sont utilisés par un webshop pour envoyer de la publicité ciblée par e-mail. Initialement, Younes a donné son consentement à cet effet mais il veut retirer ce consentement et faire supprimer ses données.

RÉSULTAT : Le webshop doit supprimer les données, étant donné que le consentement au traitement a été retiré.

Situation 2 : Une agence d'intérim tombe sur le profil LinkedIn d'Elisabeth et la contacte pour voir si elle est intéressée par une offre d'emploi. Elisabeth demande que ses données à caractère personnel ne soient pas utilisées (et demande à ne pas être contactée). Six mois après la demande, un nouveau collaborateur contacte à nouveau Elisabeth via LinkedIn en raison de son profil intéressant. Elisabeth porte plainte auprès de l'Autorité de protection des données car ses données n'auraient pas été supprimées.

RÉSULTAT : L'agence d'intérim ne peut plus utiliser les données par ex. pour envoyer des offres d'emploi. Une procédure peut contribuer à faire en sorte que les données ne soient pas à nouveau collectées et traitées (par inadvertance).

Situation 3 : Un pharmacien doit collecter et traiter des données de clients pour pouvoir offrir un service. La législation liée au secteur impose toutefois que les données à caractère personnel soient conservées pour une durée déterminée, mais la personne concernée demande à exercer son droit à l'oubli. Que doit faire le pharmacien ?

RÉSULTAT : Le pharmacien doit refuser la demande, étant donné que le traitement est nécessaire pour une mission d'intérêt public relative à la santé publique *(voir les exceptions)*

ATTENTION, LE DROIT À L'OUBLI PEUT ÊTRE REFUSÉ SI

- Le traitement est nécessaire à l'exercice du droit à la liberté d'expression et d'information
- Il existe une obligation légale de traiter les données à caractère personnel
- Les données sont traitées pour exercer l'autorité publique ou une mission d'intérêt public
- L'entreprise traite des données pour une mission d'intérêt public dans le domaine de la santé publique
- L'entreprise doit archiver les données dans l'intérêt public
- Les données sont nécessaires pour une action en justice.

QUE DOIT FAIRE VOTRE ENTREPRISE POUR ACCÉDER À UNE DEMANDE ?

1. Réagir à la demande et déterminer si votre entreprise doit y accéder *(voir les exceptions susmentionnées)*

2. En cas d'accord, accéder à la demande gratuitement dans le délai d'un mois *(exception en cas de demandes complexes)*

3. Informer les sous-traitants

4. Prendre des mesures techniques afin que les données à caractère personnel puissent être supprimées, en supprimant aussi les sauvegardes (par le service IT)

ÊTRE INFORMÉ

Soyez transparents vis-à-vis des personnes concernées en les informant de chaque utilisation et de chaque traitement de leurs données à caractère personnel

De cette manière, elles peuvent elles-mêmes évaluer les risques et prendre des décisions quant à leurs données à caractère personnel

Afin d'être transparente, votre entreprise doit communiquer d'une façon concise, transparente, compréhensible et aisément accessible, en des termes clairs et simples (par écrit ou par voie électronique, ou oralement si la personne concernée le souhaite).

En tant que responsable du traitement, votre entreprise fournit des informations sur :

- L'identité et les coordonnées du responsable du traitement
- Les coordonnées du délégué à la protection des données
- La source des données à caractère personnel si vous les avez obtenues auprès d'un tiers
- Les finalités du traitement
- Les intérêts légitimes poursuivis par le responsable de traitement ou par un tiers
- Les destinataires/catégories de destinataires des données à caractère personnel (si d'application)
- Si le responsable du traitement a l'intention de transférer les données à caractère personnel vers un pays tiers ou à une organisation internationale (si d'application)
- La durée de conservation des données à caractère personnel
- Les droits des personnes concernées
- Le droit d'introduire une plainte auprès de l'Autorité
- La base légale du traitement de données
- L'existence et la logique sous-jacente d'une prise de décision automatisée

ASTUCE : Rédigez une **déclaration de confidentialité**.

Adaptez le langage au groupe cible *(par ex. langage adapté aux enfants).*

L'information des personnes concernées ne doit pas forcément se faire absolument sous la forme d'une déclaration de confidentialité, tant que vous fournissez toutes les informations de la bonne manière. Par ex. un pharmacien qui affiche sur la porte une note informative pour informer ses clients du traitement des données à caractère personnel constitue également une bonne pratique.

Pour de plus amples informations, nous vous renvoyons à la brochure FAQ de BOOST qui contient davantage d'informations sur le principe de transparence