Commission européenne

Sept étapes pour aider les entreprises

à se préparer à l'entrée en vigueur du règlement général sur la protection des données

Justice et consommateurs

À qui s'adresse ce guide?

Ce guide a pour objectif d'aider les entreprises dont l'activité principale ne consiste pas à gérer des données à caractère personnel, telles que les PME qui traitent essentiellement les données à caractère personnel de leurs employés ou qui disposent de listes de clients. Il s'agit, par exemple, de négociants ou de magasins, comme une boulangerie ou une boucherie, ou de fournisseurs de services comme des architectes. Ce guide met en avant les quelques étapes à suivre pour se préparer à l'entrée en vigueur du RGPD.

Les données à caractère personnel sont des informations se rapportant à une personne physique (pas à des personnes morales). Elles comprennent, par exemple: le nom, le prénom, l'adresse personnelle, l'adresse e-mail ou des données de localisation extraites de la carte de votre téléphone portable. Généralement, il s'agit des données que vous pourriez détenir au sujet de vos employés, de vos clients ou de vos fournisseurs.

Moins vos activités entraînent de risque à l'encontre des données à caractère personnel, moins vous devrez entreprendre de démarches

Appliquez des principes clés:

- **collectez des données à caractère personnel dans un but clairement défini, et ne les utilisez pas à d'autres fins** (si vous demandez à vos clients de vous communiquer leur adresse e-mail afin de leur envoyer vos nouvelles offres ou promotions, vous ne pouvez pas utiliser cette adresse à une autre fin et vous ne pouvez pas la vendre à une autre entreprise).
- **ne collectez pas plus de données que nécessaire** (si vous effectuez des livraisons à domicile, vous avez besoin, par exemple, d'une adresse, d'un nom sur une sonnette, mais vous ne devez pas savoir si cette personne est mariée ou célibataire) – soyez simplement attentif aux données à caractère personnel que vous détenez.

ÉTAPE 1 — VÉRIFIEZ LES DONNÉES À CARACTÈRE PERSONNEL QUE VOUS COLLECTEZ ET TRAITEZ, LA FINALITÉ DE CE TRAITEMENT ET SA BASE JURIDIQUE

Vous avez des **employés**; vous traitez leurs données à caractère personnel conformément au contrat de travail et à vos obligations légales (par exemple: déclaration aux autorités fiscales / système social).

Vous pouvez gérer une liste de **clients individuels**, par exemple pour leur envoyer des informations sur des offres spéciales/publicités si vous avez obtenu leur consentement.

Le consentement n'est pas toujours requis. Il existe des cas où les personnes s'attendront à ce que vous traitiez leurs données. Par exemple, en tant que vendeur de pizzas, vous pouvez traiter l'adresse de livraison pour faire la promotion de l'un de vos nouveaux produits. Il s'agit d'un intérêt légitime. Vous devez informer les personnes de l'utilisation que vous comptez faire de ces données et cesser de les traiter si elles vous le demandent.

Si vous gérez une liste de **fournisseurs** ou d'**entreprises clientes**, vous devez le faire conformément aux contrats signés avec eux. Les contrats ne se présentent pas nécessairement sous forme écrite.

ÉTAPE 2 — INFORMEZ VOS CLIENTS, EMPLOYÉS ET TOUTE AUTRE PERSONNE QUAND VOUS COLLECTEZ LEURS DONNÉES À CARACTÈRE PERSONNEL

Les personnes doivent savoir que vous traitez leurs données à caractère personnel ainsi que la finalité de ce traitement.

Mais il n'est pas nécessaire de les informer quand elles savent déjà comment vous utiliserez les données, par exemple, lorsqu'un client vous demande de le livrer à domicile.

Vous devez également communiquer aux personnes qui vous le demandent les données à caractère personnel que vous détenez à leur sujet. Vous devez également leur permettre d'y accéder. Gardez de l'ordre dans vos données pour pouvoir, par exemple, répondre facilement à votre employé s'il vous demande le genre de données à caractère personnel que vous détenez.

ÉTAPE 3 — NE CONSERVEZ LES DONNÉES À CARACTÈRE PERSONNEL QUE POUR LA DURÉE NÉCESSAIRE

Les **données sur vos employés**: aussi longtemps que la relation de travail et les obligations légales qui en découlent le nécessitent.

Les **données sur vos clients**: aussi longtemps que la relation de clientèle et les obligations légales qui en découlent durent (par exemple à des fins fiscales).

Supprimez les données lorsqu'elles ne sont plus nécessaires à la finalité pour laquelle elles ont été collectées.

ÉTAPE 4 — SÉCURISEZ LES DONNÉES À CARACTÈRE PERSONNEL QUE VOUS TRAITEZ

Si vous conservez ces données dans un **système informatique**, limitez l'accès aux fichiers qui contiennent les données, par exemple, au moyen d'un mot de passe. Mettez régulièrement à jour les paramètres de sécurité de votre système.

(Remarque: le RGPD ne prescrit pas l'utilisation d'un système informatique particulier)

Si vous conservez des documents physiques reprenant des données à caractère personnel, assurez-vous qu'ils ne sont pas accessibles par des personnes non autorisées; enfermez-les dans un coffre-fort ou une armoire.

ÉTAPE 5 — CONSERVEZ DES DOCUMENTS RELATIFS À VOS ACTIVITÉS DE TRAITEMENT DES DONNÉES

Préparez un document succinct reprenant les données à caractère personnel que vous détenez et les raisons de cette conservation. Vous pourriez devoir communiquer ces documents à votre autorité de protection des données nationale si elle en émet la demande.

Ces documents devraient reprendre les informations ci-dessous.

INFORMATIONS	EXEMPLES
La finalité du traitement des données	Informer les clients sur des offres spéciales / fournir des livraisons à domicile; payer des fournisseurs; salaire et couverture sociale pour les employés
Les types de données à caractère personnel	Coordonnées des clients; coordonnées des fournisseurs; données des employés
Les catégories de personnes concernées	Employés; clients; fournisseurs
Les catégories de destinataires	Autorités du travail; autorités fiscales
Les périodes de conservation	Les données à caractère personnel des employés: jusqu'à la fin du contrat de travail (et des obligations légales qui en découlent); les données à caractère personnel des clients: jusqu'à la fin de la relation contractuelle avec le client
Les mesures techniques et organisationnelles de sécurité pour protéger les données à caractère personnel	Un système informatique régulièrement mis à jour; une armoire fermée à clé/un coffre-fort
Peu importe si les données à caractère personnel sont transférées ou non à des destinataires situés en dehors de l'UE	Utilisation d'un processeur situé en dehors de l'UE (par exemple: pour le stockage dans le cloud)

ÉTAPE 6 — ASSUREZ-VOUS QUE VOTRE SOUS-TRAITANT RESPECTE LES RÈGLES

Si vous confiez le traitement des données à caractère personnel à une autre entreprise, ne recourez qu'à un fournisseur de services qui vous garantit que le traitement respecte les exigences du RGPD (par exemple, les mesures de sécurité). Avant de signer un contrat avec un sous-traitant, vérifiez s'il a déjà changé les règles et s'il s'est adapté au RGPD. Inscrivez-le dans le contrat.

ÉTAPE 7 — VÉRIFIEZ SI VOUS ÊTES CONCERNÉ PAR LES DISPOSITIONS CI-DESSOUS

> Afin de mieux protéger les données à caractère personnel, les organisations pourraient devoir nommer un délégué à la protection des données (DPD). **Toutefois, vous ne devez pas désigner de délégué à la protection des données** si le traitement des données à caractère personnel n'est pas une activité principale de votre entreprise, s'il n'est pas risqué, et si votre activité ne se déroule pas à grande échelle.

Par exemple, si votre entreprise collecte des données sur vos clients uniquement dans le but de les livrer à domicile, vous ne devez pas nommer de DPD.

Même si vous devez recourir à un DPD, il peut s'agir d'un employé de votre entreprise chargé de remplir cette fonction en plus de ses autres tâches. Ou il pourrait s'agir d'un consultant externe; à la manière dont de nombreuses organisations recourent à des comptables externes.

> **Vous ne devez normalement pas effectuer une analyse d'impact relative à la protection des données**

Une telle analyse d'impact est réservée aux entreprises dont le traitement entraîne un plus grand risque pour les données à caractère personnel, par exemple si elles effectuent une surveillance à grande échelle d'une zone accessible au public (p. ex.: surveillance vidéo).

Si vous dirigez une petite entreprise qui gère les salaires des employés et une liste de clients, vous ne devez pas effectuer une analyse d'impact relative à la protection des données pour ces opérations de traitement.

Amendes

Les autorités de contrôle de la protection des données sont habilitées à sanctionner les violations des règles relatives à la protection des données. Elles peuvent adopter des mesures correctives (telles qu'une ordonnance ou une suspension temporaire du traitement) et/ou imposer une amende.

Leur décision d'imposer une amende doit être proportionnée et reposer sur une évaluation de toutes les circonstances du cas individuel.

Si elles décident d'imposer une amende, son montant dépendra également des circonstances du cas, y compris de la gravité de la violation ou si la violation a été commise délibérément ou par négligence. Elles prendront également votre attitude et vos intentions en considération.

Si vous souhaitez en savoir plus:

1. **Consultez le document d'orientation en ligne de la Commission européenne sur la réforme en matière de protection des données – disponible dans toutes les langues de l'UE:**

   https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_fr

2. **Consultez votre autorité de protection des données nationale:**

   http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612080

AVIS IMPORTANT

Les informations contenues dans ce guide ont pour objectif de contribuer à une meilleure compréhension des règles de l'UE en matière de protection des données.

Elles servent d'orientation – seul le texte du règlement général sur la protection des données (RGPD) a une valeur juridique. Il en résulte que seul le RGPD est susceptible de créer des droits et obligations pour les personnes. Ces orientations ne créent aucun droit susceptible d'être invoqué ni aucune attente.

L'interprétation contraignante de la législation de l'UE relève de la compétence exclusive de la Cour de justice de l'Union européenne. Les vues exprimées dans ces orientations ne préjugent pas de la position que la Commission pourrait adopter devant la Cour de justice.

Ni la Commission européenne ni aucune personne agissant en son nom ne saurait être tenue responsable de l'utilisation qui pourrait être faite des informations contenues dans ce guide.

Ce document reflétant la situation au moment de sa rédaction, il doit être considéré comme un «outil vivant» susceptible d'être amélioré, et son contenu peut faire l'objet de modifications sans préavis.

Office des publications

Luxembourg: Office des publications de l'Union européenne, 2018

Print	PDF
ISBN 978-92-79-85389-0	ISBN 978-92-79-85384-5
doi:10.2838/247785	doi:10.2838/190551
DS-02-18-544-FR-C	DS-02-18-544-FR-N