PAR
JEAN-MARC GOETZ
DIRECTEUR ASSOCIÉ,
PARKER WILLIBORG
BY JULHIET STERWEN

Le Règlement Général sur la Protection des Données personnelles (RGPD) vise à encadrer les données personnelles des clients et des collaborateurs. Il s'applique à tous, des grandes entreprises aux TPE/PME. Sa date d'entrée en vigueur, fixée au 25 mai 2018, approche à grands pas. Comment faire pour être le plus conforme possible à cette date ?

Le RGPD, c'est le 25 mai pour tous
Et vous ? Êtes-vous prêt ?

Tout d'abord, quelques précisions :

- La réglementation installe un principe de documentation en lieu et place de déclarations auprès de la CNIL. Il appartient à l'entreprise de produire cette documentation. La mise en conformité sera évaluée sur la présentation de ces preuves, comme dans la plupart des contrôles.
- Le RGPD place la maîtrise de toutes les données personnelles sous la responsabilité de l'entreprise. Les données personnelles dites « sensibles » sont particulièrement encadrées. Parmi celles-ci, notons : les données relatives à la santé ou les condamnations pénales. Sont également très suivies les collectes de données en grand volume, permettant d'établir un profilage des personnes.
- L'entreprise est garante de la mise en conformité des partenaires et sous-traitants impliqués dans les traitements de données personnelles. Il lui appartient de s'assurer de leur engagement dans cette démarche.

Le champ d'application est large. En revanche, les actions à mener prioritairement sont les mêmes pour tous. Et elles ne nécessitent pas forcément un investissement important :

> ***Que vous avanciez seul ou accompagné, la mise en conformité ne s'arrêtera pas au 25 mai 2018.***

1. Désigner un référent à la protection des données personnelles

Souvent désigné comme DPO (Data Protection Officer), il ne présente pas un caractère obligatoire pour les sociétés de moins de 250 salariés. Sa désignation est cependant recommandée. Il pilotera le projet de mise en conformité et se présentera comme le point de contact auprès de l'autorité de contrôle. Il n'y a pas de profil type pour le poste : il peut être technique (DSI), juridique, Correspondant informatique et Libertés ou rattaché à la direction ; il peut être également externe à l'entreprise.

2. Établir un plan d'action pour la mise en conformité

Il constitue une première preuve sans avoir à suivre un format imposé. Sa structure est simple et construite autour de la nature des mesures à mettre en œuvre (organisation, documentation, alignement des traitements, formation/communication), son responsable, sa date de mise en service, la preuve associée (par exemple : un compte rendu ou une nouvelle version de logiciel). Ce plan peut être rapidement établi en quelques jours à l'aide des métiers, des responsables d'application régulièrement exposés aux données personnelles : la DSI, les métiers en relation avec les clients, la DRH.

3. Produire/actualiser le registre des traitements des données personnelles

Sensiblement différent de celui utilisé pour les déclarations CNIL, ce registre constitue le document de référence pour les traitements. Il permet de décrire leur finalité, les utilisateurs, le responsable, la nature des données personnelles embarquées, les durées de rétention. Il existe plusieurs modèles dont celui publié par la CNIL[1]. Mais quel est le niveau de détail à appliquer pour la définition du traitement ? Il est d'usage d'y associer une application informatique ou une phase de traitement (collecte/saisie des données personnelles pour une demande de renseignements, contractualisation, ...) mais un niveau de détail plus précis peut être requis en fonction d'autres critères comme la sensibilité ou le volume de données en jeu.

Pour cette production de registre, il est nécessaire de :

- Cartographier les données pour, *a minima*, identifier la localisation du stockage et les supports, les sous-traitants impliqués,
- Déterminer la durée de conservation des données personnelles. C'est un exercice délicat car la réglementation n'accepte pas de conservation sans limite de durée. Il faut pouvoir l'évaluer sur la base des durées légales[2] et des exigences des métiers, par exemple, la durée requise pour répondre aux contrôles fiscaux.

4. Actualiser ses sites web, ses documents avec

- Les nouvelles mentions légales, les liens vers une notice explicative simple rappelant les fondamentaux de la réglementation ainsi que les moyens d'accès à ses droits à l'information (contact email, rubrique du site internet, ...),
- Une gestion explicite du consentement de la personne (case à cocher, ...) avec le rappel de l'objet du traitement sans oublier l'option d'opposition.

5. Écrire aux sous-traitants et partenaires impactés

Qu'il s'agisse d'éditeurs de progiciels, d'hébergeurs de données ou autres, il est important d'acter la demande sur leur avancement par un courrier. N'oublions pas que les fournisseurs peuvent également demander des comptes ; le plan d'action pourra constituer un élément de réponse.

Alors, serez-vous prêt ? Que vous avanciez seul ou accompagné, la mise en conformité ne s'arrêtera pas au 25 mai 2018. Les données personnelles évoluent en permanence. Elles nécessiteront donc un suivi régulier des mesures et des preuves. ●

RGPD : cinq chantiers prioritaires

1. www.cnil.fr/fr/cartographier-vos-traitements-de-donnees-personnelles

2. www.cnil.fr/fr/limiter-la-conservation-des-donnees