Les Données Personnelles révolutionnent les responsabilités et la répartition des risques dans les entreprises, les administrations et les associations : plus que 4 mois pour se mettre en conformité.

Le 25 janvier 2018

Adopté le 14 avril 2016, le Règlement européen sur la protection des données personnelles (RGPD) entre en vigueur en France et dans toute l'Europe le 25 mai 2018 édictant de nouvelles normes de conformité sanctionnées par des amendes pouvant atteindre 4% du chiffre d'affaires mondial consolidé. Les mesures du RGPD s'appliquent à tous types d'organisations y compris les entreprises sans seuil de chiffre d'affaires, les administrations et les associations.

Pour se mettre en conformité les entreprises doivent mettre en place un certain nombre de mesures dont la pierre angulaire est la nomination du *Data Protection Officer* (DPO) ou Délégué à la Protection des Données (DPD) **et** la mise en place d'un **registre des traitements** de données personnelles, tenu, géré et mis à jour par l'entreprise elle-même (**obligatoire pour toute entreprise de plus de 50 salariés**).

Avant de collecter : consentement et transparence

Le RGPD impose aux entreprises de donner une information claire, intelligible et accessible aux personnes concernées par les traitements de leurs données. Les personnes concernées doivent être en mesure de donner leur accord ou de s'opposer à la collecte de manière non ambiguë.

Pendant le traitement : proportionnalité et finalité

Durant le traitement des données personnelles, le responsable de traitement (une entreprise, une administration, une association) doit veiller à ce que le traitement de ces données soit licite.

Le traitement doit être effectué pour les finalités déterminées et acceptées par la personne concernée.

La conservation des données ne doit pas dépasser le temps nécessaire. Le responsable de traitement doit respecter les principes d'intégrité et de confidentialité des données personnelles en garantissant la sécurité des Systèmes d'Information, et des données personnelles, y compris contre la perte, la destruction ou les dégâts d'origine accidentelle, à l'aide de mesures techniques ou organisationnelles appropriées.

Mise en place obligatoire de processus d'alerte : notification des failles de sécurité

Les entreprises et organisations de tout type sont tenues d'informer sans délai, et sous maximum 72 heures, l'autorité de surveillance nationale (CNIL en France) et le cas échéant les personnes concernées en cas de violation grave des données.

La notification des failles de sécurité doit décrire la nature de la violation de données à caractère personnel et le nombre approximatif d'enregistrements de données concernés, communiquer le nom et les coordonnées du délégué à la protection des données au sein de l'entreprise ou de l'organisation, ou d'un autre contact auprès duquel des informations complémentaires peuvent être obtenues, décrire les conséquences probables de la violation de données à caractère personnel et décrire les mesures prises ou que le responsable du traitement propose de prendre pour remédier à la violation.

La responsabilité pénale du chef d'entreprise

Le fait de violer les dispositions relatives au consentement lors de la collecte, de procéder aux traitements du numéro d'inscription des personnes au répertoire national d'identification des personnes physiques, de conserver des données personnelles au-delà des durées autorisées, de détourner ces informations de leur finalité ou encore de divulguer ces informations constituent des délits punis de cinq ans d'emprisonnement et de 300 000 € d'amende (articles 226-16 et suivants du Code pénal).

Sont punis des mêmes peines le fait de collecter des données personnelles par un moyen frauduleux, déloyal ou illicite, de mettre ou de conserver en mémoire informatisée, sans le consentement exprès de l'intéressé.

Le responsable de traitement engage sa responsabilité pénale s'il procède au traitement de données personnelles sans mettre en œuvre les mesures légales prescrites, notamment concernant la sécurité des données traitées. (articles 226-17 du Code pénal).

Le montant des peines encourues est susceptible d'évoluer avant mai 2018 sous l'influence du RGPD.

financières effectives, proportionnées et dissuasives

Le RGPD renforce les mécanismes de sanctions administratives à l'encontre des responsables de traitement et des sous-traitants.

L'autorité pourra prononcer des amendes administratives pouvant s'élever jusqu'à 20 millions d'euros ou, dans le cas d'une entreprise, jusqu'à 4 % du chiffre d'affaires annuel mondial consolidé total de l'exercice précédent, le montant le plus élevé étant retenu.

L'autorité de contrôle pourra également :

- Prononcer un avertissement ;
- Mettre en demeure l'entreprise ou l'organisation ;
- Limiter temporairement ou définitivement un traitement ;
- Suspendre les flux de données ;
- Ordonner de satisfaire aux demandes d'exercice des droits des personnes ;
- Ordonner la rectification, la limitation ou l'effacement des données ;
- Retirer la certification délivrée ou ordonner à l'organisme de certification de retirer la certification.

Tous les contrats avec les sous-traitants qui délégueraient la gestion de données personnelles doivent être remis à jour et doivent sécuriser la chaine de responsabilités entre les parties conformément à l'article 82 du RGPD.

C'est donc la réputation de l'entreprise qui est également en jeu, à l'égard de ses clients, de ses fournisseurs, et de ses sous-traitants.

Au regard de ce texte contraignant, aujourd'hui plus que jamais, les entreprises, les associations et les administrations doivent apprivoiser les nouveaux principes que le règlement impose et les mettre en œuvre sans délai.

Grant Thornton Société d'Avocats et Grant Thornton vous proposent un accompagnement RGPD pluridisciplinaire, innovant, s'appuyant sur l'expertise des risques, l'approche juridique et les risques liés aux systèmes d'information, de manière à offrir une solution globale à la mise en conformité.

Contacts

Nicolas Remy-Neris
Grant Thornton Société d'Avocats
Avocat – Correspondant informatique & Libertés
Directeur Droit Commercial
E: nremyneris@avocats-gt.com
T: +33 (0)1 41 16 27 25

Alexis Grin
Grant Thornton
Associé | IT Risk Services
E: alexis.grin@fr.gt.com
T: +33 (0)1 41 25 91 64

Jean de Laforcade
Grant Thornton
Directeur Associé | Risk Management
E: jean.delaforcade@fr.gt.com
T: +33 (0)1 41 25 86 68

Grant Thornton Société d'Avocats
29, rue du Pont
92200 – Neuilly-sur-Seine
France
www.avocats-gt.com
T : +33 (0)1 41 16 27 27
F : +33 (0)1 41 16 27 28
E : contact@avocats-gt.com

À propos de Grant Thornton Société d'Avocats
Grant Thornton Société d'Avocats accompagne ses clients dans toutes leurs opérations stratégiques, que ce soit dans un contexte national ou international, grâce à une expertise pluridisciplinaire reconnue dans tous les domaines du droit des affaires.
Le cabinet offre à une clientèle nationale et internationale l'ensemble des prestations nécessaires à la gestion juridique et fiscale des entreprises en intervenant sur des problématiques de droit des sociétés, de due diligences juridiques, fiscales, sociales et contractuelles, de fusions et acquisitions, de droit fiscal, de TVA et commerce international, de mobilité internationale, de droit commercial, droit social et enfin de contentieux des affaires.

***Grant Thornton Société d'Avocats est membre de Grant Thornton International Limited**, organisation mondiale d'Audit et de Conseil, présente dans 140 pays avec plus de 42 200 collaborateurs.*

Grant Thornton
Société d'Avocats