CONFÉDÉRATION DES PME

Août 2017

DONNEES PERSONNELLES : PREPAREZ L'APPLICATION DU RGPD POUR MAI 2018 !

Attention, les règles sur les données personnelles changent : à partir du 25 mai 2018, les entreprises qui collectent, stockent ou utilisent des données personnelles devront respecter les nouvelles obligations issues du Règlement général sur la protection des données, dit « RGPD ». Les sanctions encourues sont sévères.
Voici les principaux éléments à connaitre pour être conforme à la règlementation.

C'EST QUOI UNE DONNEE PERSONNELLE ?

Une donnée personnelle est toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres[1].
Concrètement, ce sont : un nom, une adresse, des données de localisation, un identifiant en ligne, un ou plusieurs éléments spécifiques propres à l'identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale d'une personne[2].

QUELLES EVOLUTIONS NOTABLES PAR RAPPORT A LA LOI INFORMATIQUE ET LIBERTES ?

La première évolution apportée par le RGPD est un allègement des formalités à effectuer pour celui qui recueille, collecte ou traite des données personnelles.
En parallèle, ce Règlement accroît les droits des personnes : l'objectif affiché du texte est de renforcer le contrôle des citoyens européens sur l'utilisation de leurs données personnelles.
Enfin, ce Règlement prévoit des sanctions financières en cas de non-respect des droits accordés aux personnes transmettant leurs données.

QUE RESTE-T-IL DES REGLES ISSUES DE LA LOI INFORMATIQUE ET LIBERTES ?

Il convient de rappeler que les principes de proportionnalité des données collectées par rapport à la finalité du traitement, de loyauté de la collecte, de droit d'opposition des personnes concernées et d'interdiction de principe de la collecte de données sensibles sont toujours applicables.

POURQUOI AVOIR DES REGLES UNIFORMES EN EUROPE ?

Ce nouveau système a pour finalité de limiter les coûts liés aux divers systèmes de protection des données personnelles existant en Europe et aider ainsi les entreprises à se développer à l'international.

---

[1] Définition issue de l'article 2 de la loi 78-17 relative à l'informatique, aux fichiers et aux libertés

[2] Illustrations données sur le site de la Commission européenne, page dédiée à la protection des données

COMMENT VOUS CONFORMER A VOS OBLIGATIONS ?

- Pour le recueil de la donnée personnelle : un consentement clair

Obtenez un consentement clair des personnes concernées pour traiter leurs données. En effet, vous n'avez désormais plus de formalités déclaratives à effectuer auprès de la CNIL mais pour autant, la règle est qu'il vous faut toujours être en mesure de prouver que la personne a donné son consentement.
Nota : le consentement recueilli dans le cadre d'une déclaration écrite relative à d'autres questions doit l'être sous une forme compréhensible et aisément accessible et formulée en des termes clairs et simples.

- Des garanties complémentaires pour le recueil de la donnée sensible

Mettez en place des garanties supplémentaires pour la protection des informations relatives à la santé, à la race, à l'orientation sexuelle, à la religion et aux opinions politiques. Et n'oubliez pas que, par principe, il est interdit de réaliser un traitement de ces données sensibles. Les exceptions à cette interdiction sont limitées, le RGPD en prévoit 10 dont, notamment : lorsque la personne concernée a donné son consentement explicite au traitement de ces données à caractère personnel pour une ou plusieurs finalités spécifiques ; lorsque le traitement porte sur des données à caractère personnel qui sont manifestement rendues publiques par la personne concernée ou encore lorsque le traitement est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée.

- Donner impérativement l'accès à la donnée et permettre sa portabilité

Vous devez donner aux personnes concernées les moyens d'accéder à leurs données et de les transmettre à d'autres entreprises, voire les transmettre vous-même, lorsque cela est techniquement possible.

- Permettre à tout moment l'opposition à la prospection

Octroyez aux personnes concernées le droit de s'opposer à tout moment au traitement de leurs données pour les sollicitations directes (dit aussi « marketing direct », c'est-à-dire : appels, SMS, mails, courriers, etc.).

- Supprimer la donnée sur demande

Octroyez aux personnes concernées le « droit à l'oubli » : supprimez leurs données à caractère personnel si elles en font la demande, à moins que cette suppression ne compromette la liberté d'expression ou la possibilité de faire des recherches.

QUELLES SONT LES SANCTIONS ENCOURUES ?

Après rappel à l'ordre et avertissement, les sanctions pour violation de ces nouvelles obligations sont lourdes : suspension du traitement des données et amende qui peut aller jusqu'à 20 millions d'euros ou 4 % du chiffre d'affaires annuel (mondial le cas échéant), la somme retenue étant la plus élevée.

LE DELEGUE A LA PROTECTION DES DONNEES

Nommer un Délégué à la protection des données, nouveauté issue du RGPD, n'est pas toujours obligatoire. Cela dépend du type et de la quantité de données que vous collectez, si le traitement des données est votre principale activité et si vous effectuez ces opérations à grande échelle.
Vous devez impérativement nommer un Délégué à la protection des données dans 2 situations :

- Lorsque vos activités de base vous amènent à réaliser un suivi à grande échelle, régulier et systématique des personnes,

– Lorsque vos activités de base vous amènent à traiter à grande échelle des données dites « sensibles » (orientation sexuelle, convictions religieuses, données biométriques ou génétiques, origine raciale ou ethnique, etc.), ou relatives à des condamnations pénales et infractions.

Nota : la notion de « traitement à grande échelle » n'a pas été définie.

- Seules des illustrations ont été données par le G29 (regroupement de toutes les CNIL européennes) : les transports en commun sont considérés comme des traitements de données à grande échelle ; les traitements de données d'un médecin ou d'un avocat ne sont pas vus comme à grande échelle.
- La CNIL vise aussi les compagnies d'assurance ou les banques pour leurs fichiers clients, les opérateurs téléphoniques ou les fournisseurs d'accès internet.

On ne peut donc savoir de façon certaine quels traitements de données sont à grande échelle et donc les cas où l'entreprise doit obligatoirement nommer le Délégué à la protection des données.

CERTAINES PME DOIVENT TENIR UN REGISTRE DES ACTIVITES DE TRAITEMENT

Les PME doivent tenir, sous forme écrite, un registre des activités de traitement, uniquement dans 3 situations :

- Le traitement n'est pas occasionnel,
- Le traitement représente une menace pour les droits et les libertés des citoyens,
- Le traitement porte sur des données sensibles ou des casiers judiciaires.

→ Que doit mentionner un tel registre ?

– Le nom et les coordonnées de l'entreprise,
– Les raisons du traitement des données,
– La description des catégories de personnes concernées et des données à caractère personnel,
– Les catégories d'organisations recevant les données,
– Le transfert des données vers un autre pays ou à destination d'une autre organisation,
– Les délais de suppression des données, si possible,
– La description des mesures de sécurité utilisées pour le traitement, si possible.

POUR EN SAVOIR PLUS

Pour en savoir plus sur vos nouvelles obligations qui deviendront effectives le 25 mai 2018, vous pouvez consulter :

- Le site de la CNIL dont un onglet en haut de page « Règlement européen » traite du RGPD sous tous ses aspects : www.cnil.fr avec un onglet « se préparer au Règlement européen »
- La page dédiée à la protection des données sur le site de la Commission européenne : http://ec.europa.eu/justice/newsroom/data-protection/infographic/2017/index_fr.htm

Pour ceux qui souhaitent prendre connaissance des textes à l'origine de ces nouvelles mesures :
Règlement 2016/679 du Parlement européen et du Conseil du 27 avril 2016
Directive 2016/680 du Parlement européen et du Conseil du 27 avril 2016

Pour en savoir plus :

Site CNIL : https://www.cnil.fr/fr/se-preparer-au-reglement-europeen

Infographie Commission européenne : http://ec.europa.eu/justice/newsroom/data-protection/infographic/2017/index_fr.htm