Le Règlement général sur la protection des données (RGPD)

Le Règlement Général sur la Protection des Données (RGPD) entrera en vigueur en mai 2018. Il a vocation à donner au citoyen plus de transparence sur l'usage qui est fait de ses données personnelles et l'assurance de leur protection. Mais le RGDP est également un gage de prévention contre le risque numérique pour l'entreprise.

En quoi consiste le RGPD ?

Le Règlement Général sur la Protection des Données (RGPD) du 27 avril 2016 sera applicable à compter du 25 mai 2018. Il renforce les droits des citoyens concernant l'usage que toutes les entreprises européennes (ou qui ont une activité en Europe) font de leurs données personnelles :

- **transparence :** droit de savoir à quoi servent ses données. Elles doivent être traitées de manière loyale et licite ;
- **droit à la portabilité :** les personnes peuvent réclamer qu'une entreprise lui restitue toutes les données qu'elle a récupérées sur elle ;
- **droit à l'effacement :** un individu peut exiger qu'une entreprise supprime de ses bases de données tous les fichiers la concernant ;
- **droit à réparation :** tout individu peut exiger réparation des dommages matériels ou moraux causés par une violation du Règlement.

Le renforcement de ces droits accentue par conséquent les obligations de toutes les entreprises qui collectent, traitent et stockent des données personnelles.

Aujourd'hui, de nombreuses sociétés ne protègent pas assez leur réseau informatique, par manque de moyens ou de prise de conscience des risques numériques. Résultat, **onze incidents de cybersécurité seraient comptabilisés chaque jour en milieu professionnel en France,** d'après le cabinet de conseil PwC.

Face aux menaces numériques (phishing, infiltration sur le réseau informatique, virus…) pouvant entraîner une fuite de données - non seulement celles de vos clients, mais aussi celles de votre entreprise - vous devez renforcer votre niveau de sécurité.

Les mesures élémentaires à mettre en place

Pour être en conformité avec le RGPD, différentes mesures doivent être prises :

- la réalisation d'une **cartographie exhaustive des supports internes** (serveurs, disques durs) **et externes** (Cloud, prestataires informatiques…) stockant les données personnelles ;
- la création d'un **registre des activités de traitement de toutes les données personnelles** récoltées. Il doit préciser la ou les finalités pour lesquelles ces informations sont collectées ou gérées : relation commerciale, gestion RH, vidéo surveillance, habitudes de consommation, géolocalisation de véhicules... mais également leur lieu d'hébergement, leur durée de conservation ou encore les mesures de sécurité dont elles font l'objet ;
- la nomination d'un **Délégué à la Protection des données.** C'est le responsable du traitement des données dans une entreprise.

À noter que cette nomination ainsi que la création d'un registre des activités de traitement des données sont deux mesures obligatoires pour les entreprises de plus de 250 salariés et pour toutes celles dont les activités nécessitent de traiter des données relatives à des secteurs sensibles (santé, données en lien avec les infractions et les condamnations pénales…).

- L'établissement d'une **liste exhaustive de tous les sous-traitants** enregistrant des informations à caractère personnel. La CNIL signale qu'ils sont tenus « de respecter des obligations spécifiques en matière de sécurité et de confidentialité (...). Ils ont notamment une obligation de conseil auprès du responsable de traitement pour la conformité à certaines obligations du règlement (failles, sécurité, destruction des données, contribution aux audits). »

- **La conservation des seules données personnelles nécessaires** à l'activité de l'entreprise. C'est le principe dit de « minimisation » du RGPD. Si l'on prend le cas d'une newsletter envoyée à des prospects ou à des clients, une entreprise ne doit garder qu'une seule donnée « nécessaire » : l'adresse e-mail. Éventuellement, un site de e-commerce peut enregistrer les dates de naissance pour tenir compte des anniversaires et proposer des offres spéciales à ses consommateurs. La durée de conservation doit par ailleurs être précisée et justifiée.
- La mise en place **de moyens d'identification et d'authentification des salariés.** Cela implique d'établir une politique de gestion des mots de passe et de limiter les accès aux dossiers sensibles aux seuls collaborateurs vraiment concernés.
- La mise en place d'une **politique de sauvegarde** assurant la restitution intègre des données.

D'un point de vue technique, les entreprises doivent s'appuyer notamment sur :

- des techniques de chiffrement des données personnelles ;
- l'authentification forte (certificat électronique, carte à puce…) afin de tracer les accès ;
- des procédures visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement. Cette mission incombe notamment à des sociétés spécialisées dans la sécurité informatique et qui peuvent être mandatées par votre assureur.

Ces principales mesures doivent être mises en place sous peine de sanctions de la CNIL en cas de contrôle ou après un piratage ayant eu un impact sur la sécurité des données personnelles. Le RGPD prévoit des amendes par paliers selon les fautes commises. Il précise que cette sanction peut atteindre jusqu'à 4 % du chiffre d'affaires annuel.

Ce qu'il ne faut pas faire

Envoyer des mailings sans le consentement explicite des citoyens n'est plus possible. Il faut qu'ils aient manifesté « de façon libre, spécifique, éclairée et univoque » leurs accords.

Par ailleurs, si une personne vous demande des précisions sur le traitement de ses données, il n'est pas possible de pratiquer la politique de l'autruche. Une réponse doit par principe être apportée dans les meilleurs délais et en tout état de cause dans le délai d'un mois à compter de la réception de la demande.

Pour aller plus loin

« Des mécanismes techniques et organisationnels garantissant la confidentialité et l'intégrité des données personnelles doivent être mis en œuvre pour éviter que leur consultation par des tiers non autorisés, des modifications ou encore leur perte porte préjudice aux personnes concernées », explique Sophie Nerbonne, Directrice de la conformité à la CNIL dans une interview publiée dans la Revue des Collectivités Locales (n° 485, en septembre 2017). Parmi ces solutions, il y a notamment un logiciel mis à disposition gratuitement par la CNIL. Il permet de réaliser soit même son analyse d'impact sur la protection des données.

LEXIQUE

Les données personnelles

Il s'agit d'informations permettant d'identifier, directement ou indirectement, une personne : nom, âge, lieu de naissance, numéro de Sécurité sociale… L'arrêt n° 1184 du 3 novembre 2016 de la Cour de cassation précise aussi que « les adresses IP (…) sont des données à caractère personnel, de sorte que leur collecte constitue un traitement de données à caractère personnel ».

Pour vous accompagner dans votre mise en conformité avec le RGPD, découvrez l'offre Generali Protection Numérique

https://www.generali.fr/professionnel/assurance-cyber-risques/

GAMP0002FC2A - Mars 2018