Comment mettre ses données en conformité avec le RGPD ?

La conformité impose de respecter certaines bonnes pratiques. À l'occasion de la Maddy Keynote qui s'est tenu le 14 septembre dernier, deux experts se sont réunis pour faire le point : Gilles Garnier, délégué à la Protection des données, et Damien Noworyta, responsable de la Protection des données à la Macif.

Temps de lecture : minute

21 septembre 2021

En 2020, la Cnil a reçu 13 585 plaintes et infligé plus de 138 millions d'euros d'amendes. Loi " Informatique et libertés ", règlement général sur la protection des données (RGPD), directive ePrivacy… La protection des données personnelles n'est aujourd'hui plus une option. Pour la Macif, c'est même un facteur déterminant dans le choix d'une startup. Startups auxquelles le groupe fait de plus en plus souvent appel dans le cadre de sa stratégie de développement. Principal avantage : leur capacité à proposer des services ultra innovants… à condition qu'ils s'inscrivent dans le respect de la réglementation.

1ère étape : recenser les traitements

L'un des premiers points à aborder lorsque l'on se met en conformité est le recensement des traitements. Comment faire ? En identifiant au préalable l'ensemble des traitements réalisés par l'entreprise : gestion des salariés, gestion des clients… ou une prestation en particulier qui

impliquerait le traitement de données personnelles. Une fois l'ensemble des traitements identifiés, il est alors nécessaire de les réunir dans ce qu'on appelle un registre des traitements. Principal intérêt : il permet d'avoir sous la main l'ensemble des traitements réalisés par l'entreprise. Certains champs étant rendus obligatoires par la réglementation européenne, un modèle de registre est disponible sur le site de la Cnil pour aider les entreprises à se mettre en conformité.

2e étape : constituer un registre des traitements

Une fois le registre créé, il importe de s'assurer que les données qui ont été collectées et traitées sont réellement nécessaires, qu'il n'y a pas de traitement des données sensibles, et que les durées de conservation ont été clairement définies et sont respectées. D'où l'intérêt du registre pour faciliter cette tâche parfois chronophage.

L'entreprise respecte l'ensemble des points ci-dessus ? Alors cap sur l'étape suivante. En revanche, si la revue de ce registre met en avant la non-conformité de certains des points précédents, c'est qu'il est alors nécessaire d'améliorer les pratiques en place.

3e étape : respecter les droits des personnes

Cela peut sembler évident, mais il est important de rappeler que lorsqu'une entreprise collecte les données de ses clients, celles-ci ne lui appartiennent pas. Elles restent leur propriété. Les clients doivent donc pouvoir continuer à agir sur leurs données. Résultat, ils doivent être informés des traitements réalisés sur leurs datas, mais aussi avoir la possibilité d'exercer différents droits, comme accéder ou effacer leurs informations.

Ainsi, dans le cas de demandes d'accès, l'entreprise a l'obligation de

fournir au demandeur une copie de l'ensemble des données personnelles dans un délai d'un mois. Au-delà, elle s'expose au risque d'être pénalisée par la Cnil. C'est pourquoi il est indispensable de bien se préparer en amont afin d'être sûr de répondre dans les temps.

4e étape : sécuriser les données

Enfin, dernier point clé (mais avec un niveau de priorité absolue) : la sécurisation des données. La crise sanitaire l'a démontré : les données personnelles ont beaucoup de valeur, notamment pour les cybercriminels. 86 % des entreprises ont ainsi été victimes d'une attaque réussie ces 12 derniers mois selon le rapport annuel Cyberthreat Defense. Et 40 % d'entre elles ont même été ciblées au moins six fois !

Voici pourquoi il est plus que nécessaire de s'assurer que les données d'entreprise sont bien protégées. Comment ? *A minima* en appliquant des mesures de sécurité purement techniques : utilisation d'un antivirus, chiffrement des données, changement régulier des mots de passe… Toutefois, les solutions technologiques seules suffisent rarement à éviter tout risque de vol ou de perte de données. Le plus important dans la sécurisation de vos données reste en effet la sensibilisation des utilisateurs. L'erreur humaine serait ainsi la principale cause de violation de sécurité des données informatiques (pour 62 % des professionnels IT).

En sensibilisant les salariés sur les enjeux de sécurité, en les formant ou en leur donnant quelques conseils quant aux bonnes pratiques à adopter, le risque est moindre de voir les données d'entreprise être la cible d'une tentative de piratage. Parmi les principaux avantages : un collaborateur sensibilisé saura plus facilement identifier une tentative de phishing ou de rançongiciel. Une mesure particulièrement utile lorsque l'on sait que le nombre de ransomwares a augmenté de 64 % entre août 2020 et juillet 2021.

Mettre ses données en conformité au RGDP n’est pas si simple. Le processus implique notamment une connaissance fine des évolutions réglementaires et la prise en compte de nombreux points clés. Pour vous y aider, de nombreuses ressources en ligne sont disponibles sur le site de la Cnil, dont des templates et des fiches pratiques. Vous pouvez également demander directement conseil à la Cnil ou vous faire accompagner par un cabinet spécialisé. Dans tous les cas, n’oubliez pas que le plus important dans le choix d’une startup, comme d’un fournisseur ou d’un partenaire, c’est le respect de la confidentialité des données.

Maddyness, partenaire média de la Macif

Article écrit par Maddyness, avec Macif