Pour nous contacter

–

Equipe IP/IT & Data Protection

ebarbry@racine.eu | (+33) 6.13.28.91.28

La durée de conservation et sécurité informatique, un risque pour l'entreprise

Après avoir condamné cet été le Groupe Accor à hauteur de 600.000 euros, la CNIL vient de prononcer une sanction de 250 000 euros à l'encontre d'INFOGREFFE pour des manquements à des obligations du RGPD.

Le sujet de la durée de conservation des données ainsi que de la sécurité de celles-ci revient très régulièrement dans les décisions de la CNIL. Le 8 septembre 2022, la société INFOGREFFE s'est vue infligée une amende de 250 000 euros à la suite d'un contrôle CNIL pour avoir manqué à plusieurs obligations du RGPD justement en matière de **durée de conservation et de sécurité des données personnelles**.

Une sanction qui rappelle aux entreprises qu'elles ne peuvent conserver aussi longtemps qu'elles le souhaitent les données de leurs membres ou clients et qu'elles doivent garantir une sécurité de ces données **conforme aux exigences du RGPD**.

INFOGREFFE est une société qui permet à ses clients de consulter des informations légales sur les entreprises et de commander des documents certifiés par les greffes des tribunaux de commerce. La CNIL a été saisie de plusieurs plaintes à l'encontre d'INFOGREFFE ce qui l'a amené à faire un contrôle en ligne du site web de l'organisme et ainsi relever des manquements aux obligations de conservation et de sécurité des données personnelles prévues par le RGPD.

D'abord, dans sa délibération, la CNIL rappelle que l'**article 5 du RGPD** impose aux entreprises de conserver les données pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées.

Dans la **charte de confidentialité** du site d'INFOGREFFE, il est prévu que les données à caractère personnel des membres et des abonnés sont conservées 36 mois à compter de la dernière commande de prestation et/ou documents.

La CNIL relève que de nombreuses données à caractère personnel des membres et des abonnés (plus de 900 000) étaient conservées au-delà de la durée de 36 mois, sans que l'organisme soit en mesure de justifier d'un contact récent avec lesdits membres ou abonnés. Par conséquent, ces données étaient

conservées pour des durées excessives par rapport à leur finalité et à la propre politique fixée par l'organisme.

Pour sa défense, INFOGREFFE invoque des finalités (notamment comptables et fiscales) qui justifieraient la conservation de données au-delà du délai de 36 mois. La CNIL rejette cet argument soulignant que l'organisme n'avait pas identifié ces finalités et les durées correspondantes dans sa charte de confidentialité à la date du contrôle.

Sur ce point, la décision rappelle aux entreprises le plan d'action à suivre pour s'assurer de la conformité du traitement au RGPD concernant la durée de conservation des données personnelles :

1. Identifier et qualifier les données traitées ;
2. En déduire les durées de conservation prévues par les dispositions législatives et réglementaires, par les avis de la CNIL ainsi que par l'usage ;
3. Paramétrer des outils informatiques pour faire respecter automatiquement les délais.

Sur les manquements à l'obligation d'assurer la sécurité des données à caractère personnel (article 32 du RGPD). La CNIL rappelle que **tout responsable de traitement doit prendre des mesures suffisantes pour garantir la sécurité des données à caractère personnel traitées**. Ce que n'a pas fait INFOGREFFE.

Lors du contrôle en ligne du site web d'INFOGREFFE, la CNIL constate d'abord que les mots de passe de connexion des utilisateurs à leurs comptes étaient d'une robustesse insuffisante : aucun critère de complexité n'était exigé et la saisie d'un mot de passe sécurisé était impossible en raison de la limitation de leur taille à 8 caractères maximum.

Egalement, la CNIL relève que l'organisme conserve en clair dans sa base de données, les mots de passe ainsi que les questions et réponses secrètes utilisées lors de la procédure de réinitialisation des mots de passe par les utilisateurs.

Face à ces manquements, la CNIL prononce une amende de 250 000 euros à l'encontre d'INFOGREFFE. Le montant de cette sanction prend en compte le chiffre d'affaires de l'organisme et son importante coopération avec la CNIL.

Enfin, compte tenu de la pluralité des manquements relevés, de leur gravité et du nombre de personnes concernées, la CNIL décide de publier la décision de sanction pour une durée de deux ans.

Auteurs

Eric Barbry
Avocat associé
ebarbry@racine.eu

Robin Genest
Juriste
rgenest@racine.eu