LexCase FLASH
Lettre d'information de LexCase
PARIS · LYON · MARSEILLE

IP/IT/DATA

Durée de conservation et sécurité des données à caractère personnel : le rappel de la CNIL

La CNIL a relevé plusieurs manquements commis par Infogreffe, concernant la durée de conservation des données à caractère personnel de ses utilisateurs et les mesures de sécurité mises en place pour la protection des mots de passe.



Si vous n'avez que 30 secondes

Le 7 septembre 2022, la CNIL a prononcé une amende administrative d'un montant de 250 000 euros à l'encontre du Groupe d'Intérêt Économique (GIE) Infogreffe, lequel fournit un service de diffusion de l'information légale sur les sociétés via le site Internet « infogreffe.fr ».

En 2021, la CNIL a procédé au contrôle en ligne de son site Internet à la suite d'une plainte déposée par un utilisateur à l'encontre de l'organisme.

D'une part, Infogreffe ne respectait pas la durée de conservation de 36 mois à compter de la dernière commande de prestations et/ou documents, indiquée dans sa charte de confidentialité.

D'autre part, le GIE n'avait pas pris les mesures suffisantes pour garantir la sécurité des données à caractère personnel des utilisateurs sur le site Internet.

Par conséquent, la CNIL a conclu au manquement du GIE aux articles 5.1, e) et 32 du RGPD.

Infogreffe est un GIE qui regroupe les greffes des tribunaux de commerce de France. Cet organisme édite depuis 1996 un service de diffusion de l'information légale sur les entreprises sur le site Internet « infogreffe.fr ».

Le site Internet permet de consulter des informations légales sur les sociétés et autres groupements et de commander des documents certifiés (extraits Kbis, statuts de société, comptes annuels, etc.).

Infogreffe collecte et traite des données à caractère personnel relatives aux utilisateurs de son site Internet:

- Les membres, qui sont des utilisateurs disposant d'un compte leur permettant de commander différents actes sur la plateforme ;
- Les abonnés, qui sont des utilisateurs souscrivant à un abonnement annuel leur permettant d'accéder à des services spécifiques.

En 2020, la CNIL avait été saisie d'une plainte de la part d'un utilisateur, reprochant à Infogreffe de conserver les mots de passe des utilisateurs en clair et de les communiquer sur simple appel au service d'assistance téléphonique sans vérifications complémentaires.

En 2021, la CNIL a procédé au contrôle en ligne du site litigieux, avec pour objectif de vérifier la conformité des traitements de données à caractère personnel mis en œuvre par Infogreffe.

À l'occasion de ce contrôle, la CNIL a constaté que le site Internet ne respectait pas les durées maximales de conservation des données à caractère personnel qui figuraient pourtant dans sa charte de confidentialité.

Dans ces circonstances, la CNIL a sanctionné Infogreffe pour les motifs suivants :

- Le non-respect de l'obligation de conserver les données à caractère personnel pour une durée proportionnée à la finalité du traitement ;
- Le manquement à l'obligation d'assurer la sécurité des données à caractère personnel des utilisateurs.

LexCase FLASH
Lettre d'information de LexCase

1. Le non-respect de la durée de conservation des données à caractère personnel

L'article 5.1, e) du RGPD prévoit que les données à caractère personnel doivent être conservées « *pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées* ».

La charte de confidentialité du site Internet édité par Infogreffe prévoyait que les données à caractère personnel des utilisateurs étaient conservées 36 mois à compter de la dernière commande.

La CNIL a considéré que, si la conservation de certaines données à caractère personnel peut apparaître justifiée, certaines actions doivent être réalisées, notamment :

- L'archivage intermédiaire des données ;
- L'anonymisation des données.

En l'espèce, la CNIL a constaté qu'Infogreffe conservait les données à caractère personnel d'environ 1 million de ses utilisateurs dans un fichier sans limitation de durée. Elle a également constaté que pour 25 % des comptes utilisateurs, les données à caractère personnel n'avaient pas été anonymisées et qu'aucune procédure d'anonymisation automatique n'avait été mise en œuvre.

2. Le non-respect des mesures de sécurité

L'article 32 du RGPD prévoit que le responsable de traitement doit mettre en œuvre « *des mesures techniques et organisationnelles afin de garantir un niveau de sécurité adapté au risque* ».

La CNIL a considéré que les mesures de sécurité déployées par Infogreffe pour garantir la sécurité des données à caractère personnel de ses utilisateurs étaient insuffisantes.

L'autorité de contrôle s'est appuyée notamment sur sa délibération n°2017-012 du 19 janvier 2017 portant adoption d'une recommandation relative aux mots de passe. Cette délibération prescrit un certain nombre de recommandations :

- La communication et la conservation des mots de passe ne doivent jamais être effectuées en clair;
- La taille du mot de passe doit être au minimum de 8 caractères et doit comporter différentes catégories (majuscules, minuscules, chiffres, caractères spéciaux).

En l'espèce, la CNIL a considéré que les mesures de sécurité étaient insuffisantes au regard des risques encourus par les utilisateurs :

- Les mots de passe de connexion des utilisateurs à leurs comptes étaient d'une robustesse insuffisante, sans aucun critère de complexité ;
- Ces mots de passe étaient transmis et conservés en clair dans la base de données d'Infogreffe ;
- Aucune confirmation n'était envoyée à l'utilisateur lors de la modification de son mot de passe.

La CNIL a considéré que la faiblesse de ces mesures comportait des risques importants pour l'utilisateur et notamment des erreurs de manipulation, une divulgation de ses données à caractère personnel ou encore, des tentatives d'usurpation de son compte.

La décision de la CNIL doit inciter les responsables de traitement à la plus grande vigilance s'agissant de la limitation des durées de conservation des données à caractère personnel et de la gestion de la sécurité des mots de passe.

L'ÉQUIPE IP/IT/DATA DE LEXCASE



Iliana BOUBEKEUR
Avocate associée
iboubekeur@lexcase.com



Guillaume BUSSEUIL
Avocat Collaborateur
gbusseuil@lexcase.com



Manon FAUCHER
Avocat Collaborateur
mfaucher@lexcase.com