« RGPD : prendre toutes les mesures »

Le règlement général sur la protection des données impose une obligation de sécurité aux organisations pour assurer la confidentialité des informations. Comment la Cnil y veille-t-elle ? Réponses de **David Conerardy**, avocat au cabinet Seban et associés.

Quelles sont les obligations des gestionnaires pour éviter toute fuite de données sensibles ?
David Conerardy. Depuis 2018, ils ont une obligation générale de sécurité des données personnelles dont ils assurent le traitement. Le règlement général sur la protection des données (RGPD) exige de prendre toutes les mesures techniques et organisationnelles qui s'imposent. La Commission nationale de l'informatique et des libertés (Cnil) rappelle régulièrement les précautions élémentaires : adoption de procédures internes, protection du réseau, sensibilisation des équipes au maniement des données sensibles, notamment de santé, des publics vulnérables… En cas de violation, accidentelle ou issue d'une manœuvre illicite, une déclaration doit être réalisée dès lors que la structure identifie un risque[1].

Comment sont déterminés les contrôles ?
D. C. Chaque année, la Cnil définit des thématiques et des secteurs. Cette année, ce sont notamment les collectes de données dans le cadre des Jeux olympiques et paralympiques, et les informations de mineurs récupérées en ligne. En parallèle, elle réalise des contrôles de pure opportunité. À ce titre, le secteur peut être visé puisqu'il manipule beaucoup de données sensibles de personnes considérées comme vulnérables. Enfin, une accumulation de plaintes sur une période de quelques mois peut susciter son attention.


© Cabinet Seban et associés

Comment se déroulent-ils ?
D. C. Il existe différentes modalités de contrôles administratifs sur pièces ou en ligne. La Cnil peut convoquer dans ses locaux ou se rendre sur place[2]. Les agents vérifient l'effectivité des mesures prises pour assurer la sécurité et la confidentialité des données, notamment toutes celles inscrites au registre des traitements. Le procès verbal est régulièrement suivi d'un dialogue et d'une nouvelle demande de pièces à l'issue desquelles un premier rapport est établi. Si les manquements sont faibles ou résiduels, la procédure est clôturée. S'ils sont graves, après échange de mémoires, une délibération détermine une sanction. La Cnil dispose d'une large palette, la pire étant l'amende qui peut aller jusqu'à 20 millions d'euros maximum ou 4% du chiffre d'affaires. Elle peut aussi rendre publiques ses décisions. Une punition en soi. Le RGPD est en vigueur depuis plus de six ans. La Cnil n'a donc plus la même tolérance qu'au début. D'autant que, depuis, elle a diffusé des guides : elle a fourni beaucoup de documents de droit souple, de recommandations, de référentiels… pour aider les responsables de traitement dans le secteur. Dernière recommandation en date, celle sur la vidéosurveillance dans les chambres d'Ehpad sortie en mai. Il est, de fait, de plus en plus difficile de justifier une non-conformité.

[1] Lire Direction[s] *n° 224, p. 38*
[2] Lire Direction[s] *n° 227, p. 34*