actuEL | Direction Juridique
Un journal en ligne des Éditions Législatives

"Face à un contrôle CNIL, mieux vaut être préparé !", explique A. Bensoussan

07/06/2017

La Commission nationale de l'informatique et des libertés (CNIL) a réalisé l'an dernier 430 contrôles d'organismes exploitant des données personnelles. Inopiné, le contrôle peut entraîner des sanctions financières, alourdies dès l'an prochain par le RGPD. Voici les conseils d'Alain Bensoussan, avocat dirigeant de Lexing Alain Bensoussan Avocats, cabinet spécialiste du numérique et des technologies

avancées.

Un contrôle CNIL : pour qui, pourquoi et comment ? Toute entreprise qui exploite des données personnelles peut faire l'objet, un jour, d'un contrôle de conformité de leur traitement par la CNIL. En pratique, la CNIL prévoit chaque année de se pencher sur des secteurs d'activité déterminés. En 2017, il s'agit de l'assurance via les données de santé et de la télévision connectée (voir le programme de la CNIL). Les entreprises œuvrant dans ces domaines et qui plus est, les leaders, doivent donc redoubler de vigilance. Par ailleurs, il faut savoir que les plaintes sont source de contrôle : si un client ou un ex-salarié fait part de son mécontentement vis-à-vis du traitement de ses informations personnelles, il faut là aussi s'attendre à être potentiellement contrôlé. Enfin, la CNIL peut décider de s'autosaisir, en cas de violations de la part de l'entreprise visée (du droit du travail relevé par l'Inspection du travail, par exemple). Les contrôles CNIL sont inopinés : les agents se présentent dans l'entreprise sans prévenir et passent au minimum une demi-journée, voire 2 à 3 jours entiers à vérifier la conformité des traitements de données à la loi Informatique et libertés. Dès le mois de mai 2018, la vérification portera sur la bonne application du règlement général sur la protection des données (RGPD) (voir notre dossier), avec à la clé, le risque de sanctions plus lourdes en cas de non-respect des obligations : jusqu'à 20 millions d'euros d'amende ou 4 % du chiffre d'affaires mondial d'une société. Enfin, depuis 2014, la CNIL effectue également des contrôles en ligne. Ceux-ci portent notamment sur les sites web d'entreprise et, par exemple, leur politique de cookies ou encore la sécurité du site.

Le jour J : coopérez !

Un contrôle CNIL est un événement majeur pour l'entreprise et ses salariés. Deux agents au minimum se présentent dans les locaux et réclament à voir le responsable des lieux, qui n'est pas nécessairement le chef d'entreprise. Mieux vaut laisser la délégation faire son travail, car en cas d'entrave, l'article 51 de la loi Informatique et libertés prévoit jusqu'à un an d'emprisonnement et 15 000 euros d'amende. La CNIL envoie sa délégation avec une mission précise : il peut s'agir de contrôler le service clients (notamment la base de données clients/prospects), les ressources humaines (les données sur les salariés actuels et anciens), etc. Les agents doivent avoir accès à tous les documents utiles au contrôle : ils apportent donc de quoi copier les informations sur clé USB ou disque dur, peuvent effectuer des copies d'écran, contrôler la conformité du système de vidéosurveillance, etc. La CNIL peut notamment demander à vérifier tous les contrats : sous-traitance informatique, location de fichiers, etc. Dans l'entreprise contrôlée, les interlocuteurs sont généralement le directeur d'établissement, le DSI, le directeur juridique et le directeur opérationnel du service contrôlé ainsi que le Cil quand l'organisme en a désigné un.

Un avocat peut vous aider

La présence d'un avocat peut aider à apaiser l'ambiance lors d'un contrôle CNIL et surtout, à minimiser les conséquences néfastes pour l'entreprise. Comment ? En aidant le client à adopter une « posture Informatique et libertés ». Il s'agit de répondre de façon précise aux questions des agents de la CNIL tout en prenant des engagements clairs d'amélioration, qui vont dans le sens des attentes de la Commission. Par exemple, en proposant un cryptage du traitement de certaines données. Le contrôle donne lieu à la rédaction d'un procès-verbal de fin de mission, signé par l'entreprise, dans lequel sont constatés les éventuels manquements et mentionnés les documents examinés. L'avocat intervient pour aider son client lors de la signature du PV. Il formule également des engagements par écrit dans un courrier adressé a posteriori à la Commission. A l'issue du contrôle, la CNIL peut demander des pièces complémentaires ou décider d'auditionner un membre de l'entreprise en particulier. Quant aux conséquences, elles sont de trois sortes : soit la CNIL demande des améliorations, soit elle prononce une sanction (voir article 45 de la loi Informatique et libertés), soit elle classe sans suite.

Afin de vous préparer : mettez-vous en situation

La meilleure anticipation du contrôle CNIL consiste à préparer la visite éventuelle des agents, en ayant à jour tous les documents et contrats susceptibles d'être vérifiés, mais également en bâtissant une méthodologie et en simulant une visite. La méthodologie devra notamment préciser qui sera présent le jour du contrôle, qui prendra la parole, qui signera le procès-verbal, etc. Il faut également bien connaître l'état de conformité des pièces généralement réclamées par la CNIL, service par service, en insistant sur les données les plus sensibles (à caractère racial, religieux, de santé, les coordonnées bancaires, etc.).

propos recueillis par Olga Stancevic
