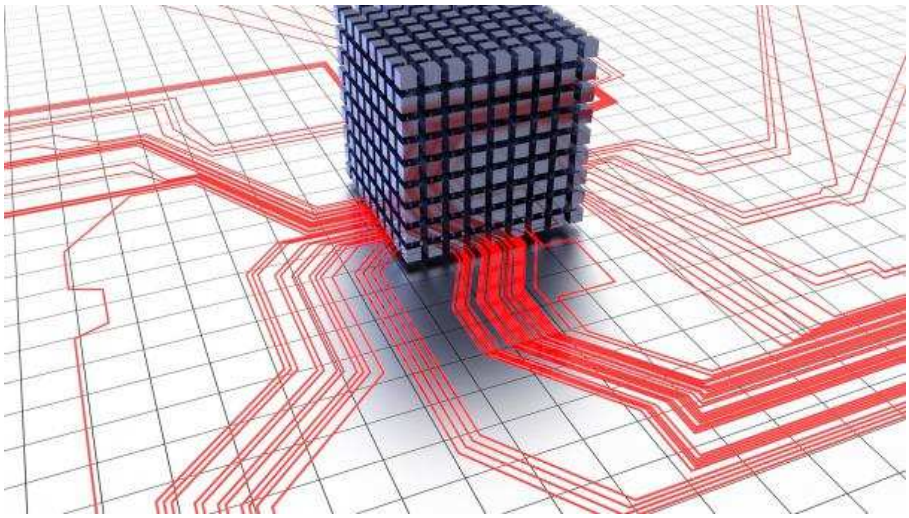
L'AGEFI actifs 07/06/2019

Manquements au RGPD

Sergic : sanction de 400.000 euros pour atteinte à la sécurité des données

La formation restreinte de la Cnil a prononcé une sanction de 400.000 euros à l'encontre de la société Sergic
Il est reproché à la société d'avoir insuffisamment protégé les données des utilisateurs de son site web et d'avoir négligé la conservation de ces données



" Les sanctions de la Cnil pour défaut de sécurisation des systèmes d'information continuent de pleuvoir et se rapprochent à grands pas du secteur des CGP et banques privées " prévient Stéphane Astier, avocat au cabinet Haas Avocats.

En l'espèce, la société Sergic est spécialisée dans la promotion immobilière, l'achat, la vente, la location et la gestion immobilière. Pour les besoins de son activité, elle édite le site web *www.sergic.com*. Ce dernier permet notamment aux candidats à la location de télécharger les pièces justificatives nécessaires à la constitution de leur dossier.

En août 2018, la Cnil a reçu une plainte d'un utilisateur du site indiquant avoir pu accéder, depuis son espace personnel, à des documents enregistrés par d'autres utilisateurs en modifiant légèrement l'URL affichée dans le navigateur.

Un contrôle en ligne réalisé le 7 septembre 2018 a permis de constater que des documents transmis par les candidats à la location étaient librement accessibles, sans authentification préalable. Parmi ces documents figuraient des copies de cartes d'identité, de cartes Vitale, d'avis d'imposition, d'attestations délivrées par la caisse d'allocations familiales, de jugements de divorce, de relevés de compte ou encore d'identité bancaire.

Le jour même de son contrôle, la Cnil a alerté la société de l'existence de ce défaut de sécurité et de la violation de données personnelles consécutive. Quelques jours plus tard, un contrôle sur place a été réalisé dans les locaux de la société. A cette occasion, il est apparu que la Sergic avait connaissance de la vulnérabilité depuis le mois de mars 2018 et que, si elle avait entamé des développements informatiques pour les corriger, ce n'est que le 17 septembre 2018 que la correction totale est devenue effective.

Sur la base de ces investigations menées, la Cnil chargé a constaté deux manquements au règlement général sur la protection des données (RGPD).

1 / Tout d'abord, la formation chargée des sanctions a considéré que la société Sergic a manqué à son obligation de préserver la sécurité des données personnelles des utilisateurs de son site.

En effet, La société n'avait pas mis en place de procédure d'authentification permettant de s'assurer que les personnes accédant aux documents étaient bien celles à l'origine de leur téléchargement, alors qu'il s'agissait d'une mesure élémentaire à prévoir.

Un manquement aggravé d'une part, par la nature des données rendues accessibles, et d'autre part, par le manque particulier de diligence de la société dans sa correction : la vulnérabilité n'a été définitivement corrigée qu'au bout de 6 mois et aucune mesure d'urgence visant à limiter l'impact de la vulnérabilité n'a été prise dans l'attente.

2 / Ensuite, la Cnil a constaté que la société conservait sans limitation de durée en base active l'ensemble des documents transmis par les candidats n'ayant pas accédé à location au-delà de la durée nécessaire à l'attribution de logements.

Or, par principe, la durée de conservation des données personnelles doit être déterminée en fonction de la finalité du traitement. Lorsque cette finalité (par exemple, la gestion des candidatures) est atteinte, et qu'aucune autre finalité ne justifie la conservation des données en base active, les données doivent soit être supprimées, soit faire l'objet d'un archivage intermédiaire si leur conservation est nécessaire pour le respect d'obligations légales ou à des fins précontentieuses ou contentieuses.

Dans ce cas, les données doivent être placées en archivage intermédiaire, par exemple dans une base de données distincte. Là encore, la durée de cet archivage doit être limitée au strict nécessaire.

Dans ces conditions, la formation restreinte a prononcé une amende de 400.000 euros [1].

Un montant jugé à la hauteur de la gravité du manque de diligence de la société dans la correction de la vulnérabilité et du fait que les documents accessibles révélaient des aspects très intimes de la vie des personnes. La Cnil a toutefois pris en compte, également, la taille de la société et sa surface financière.

[1] Délibération de la formation restreinte n° SAN – 2019-005 du 28 mai 2019