26/12/18 - CNIL – Condamnation de la société Bouygues Telecom : 250K€

Categories : Fil d'actualité RGPD

Date : jeudi 27 décembre 2018

Compte tenu de la date des faits, le RGPD n'était pas encore applicable.

Origine du contrôle : Le 2 mars 2018, la CNIL a reçu un signalement l'informant de l'existence d'un incident de sécurité lié aux données personnelles de clients de la marque B&You, détenues par la société Bouygues Telecom. Le 6 mars 2018, Bouygues Telecom, avisé de la violation de données par un message reçu sur son compte institutionnel Twitter, a notifié la violation de données à la CNIL.

Faits : Une vulnérabilité a été détectée, donnant accès à des contrats et factures de clients B&You (donc aux nom, prénom, date de naissance, adresse e-mail, adresse postale, numéro de téléphone mobile) par la simple modification d'une adresse URL sur le site web de Bouygues Telecom. L'impact a porté sur les données de plus de 2 millions de clients B&You pendant plus de 2 ans et 3 mois. Un contrôle dans les locaux de Bouygues Telecom a été effectué le 9 mars 2018 par la CNIL et Bouygues Telecom a rapidement corrigé la vulnérabilité de sorte que les données personnelles des clients n'étaient déjà plus librement accessibles au moment du contrôle.

Obligation d'assurer la sécurité et la confidentialité : Le défaut de sécurité provenait de l'oubli de réactiver sur le site, après une phase de test à la suite d'une fusion des bases de données et système informatiques correspondant aux marques Bouygues Telecom et B&You, la fonction d'authentification à l'espace client qui avait été désactivée pour les seuls besoins de ces tests. Il s'agit donc visiblement d'une erreur humaine. La CNIL a malgré tout considéré que, compte tenu du choix de Bouygues Telecom de mettre en place une unique mesure de sécurité et aucune mesure complémentaire, il lui appartenait d'être particulièrement vigilante quant à l'effectivité de ce seul mécanisme d'authentification. Elle a également retenu que même si Bouygues Telecom justifiait avoir mis en place des tests d'intrusion réguliers, directement ou par le biais de prestataires, ces tests n'étaient pas adaptés aux spécificités de la base de données et n'étaient donc pas efficaces. Bouygues Telecom aurait donc dû prévoir une revue manuelle du code portant sur l'élément critique constitué par ce mécanisme d'authentification, ce qui était rendu possible par les moyens de la société et nécessaire vu le nombre de personnes concernées par le risque. La CNIL reconnait que Bouygues Telecom ne peut totalement se prémunir d'une erreur humaine mais aurait dû mettre en place des mesures permettant de détecter cette erreur humaine.

Sanction : Une amende de 250K€ : Le rapporteur avait au départ proposé à la CNIL une amende de 500K€ puis ayant pris connaissance des observations de Bouygues Telecom a proposé de la

réduire à 250K€. La gravité de la violation a été prise en compte (nombre de données et de personnes concernées, durée de la faille) ainsi que la grande réactivité de Bouygues Telecom dans la résolution de l'incident de sécurité et des nombreuses mesures mises en place pour limiter les conséquences de la faille (ex. rappel de bonnes pratiques et fiches conseil pour ses clients, lutte contre le phishing, surveillance du dark web, formation des salariés).

Publication de la décision : Au regard du nombre très important de données et de personnes concernées, de la durée de la faille, du contexte de multiplication des incidents de sécurité et de la nécessité de sensibiliser les responsables de traitement et les internautes.

https://www.legifrance.gouv.fr/affichCnil.do?oldAction=rechExpCnil&id=CNILTEXT000037856073&fastReqId=2004200385&fastPos=1