La Cnil inflige une amende de 100 000 euros à Darty

	La Cnil inflige une amende de 100 000 euros à Darty

Le groupe est sanctionné pour ne pas avoir suffisamment sécurisé les données des clients ayant eu recours au service après-vente en ligne.

En février 2017, la CNIL a été informée de l'existence d'un incident de sécurité concernant le traitement des demandes de service après-vente des clients de la société ETABLISSEMENTS DARTY ET FILS.
Lors d'un contrôle en ligne réalisé début mars 2017 les équipes de la CNIL ont pu constater qu'une défaillance de sécurité permettait d'accéder librement à l'ensemble des demandes et des données renseignées par les clients de la société, via un formulaire en ligne de demande de service après-vente. Plusieurs centaines de milliers de demandes ou réclamations contenant des données telles que les nom, prénom, adresse postale, adresse de messagerie électronique ou numéro de téléphone des clients étaient potentiellement accessibles.

Le contrôle sur place réalisé quinze jours plus tard a révélé que le formulaire de demande de service après-vente, à l'origine du défaut de sécurité, avait été développé par un prestataire commercialisant un logiciel de service après-vente « sur étagère ». Lors du contrôle, la société ETABLISSEMENTS DARTY ET FILS a indiqué avoir recours à un autre formulaire distinct et ne pas utiliser celui à l'origine de l'incident.

Les vérifications opérées par la CNIL ont pourtant permis de constater que les fonctionnalités du logiciel rendant accessible le formulaire développé par son prestataire n'avaient pas été désactivées. Elles ont également révélé que le prestataire n'avait pas mis en place de filtrage des adresses URLs, qui aurait permis d'empêcher à des tiers non autorisés d'accéder aux données des clients contenues dans l'outil de gestion des demandes de service après-vente *via* le formulaire défectueux.
Alors même qu'elle avait informé la société de cet incident de sécurité, la CNIL a constaté que les fiches des clients étaient toujours accessibles entre le premier et le second contrôle et que de nouvelles fiches avaient été créées dans ce laps de temps. Le soir même du second contrôle, la société l'informait des mesures prises pour remédier à cet incident.
La Présidente de la CNIL a désigné un rapporteur afin que soit engagée une procédure de sanction à l'encontre de la société ETABLISSEMENTS DARTY ET FILS.

La formation restreinte de la CNIL a prononcé une sanction d'un montant de 100.000 euros, estimant que la société avait manqué à son obligation de sécurité des données personnelles, en méconnaissance de l'article 34 de la loi Informatique et Libertés.

La formation restreinte a considéré que le simple fait que la société fasse appel à un prestataire sous-traitant ne la décharge pas de son obligation de préserver la sécurité des données traitées pour son compte, en sa qualité de responsable du traitement.

La société aurait dû s'assurer préalablement que les règles de paramétrage de l'outil mis en œuvre pour son compte ne permettaient pas à des tiers non autorisés d'accéder aux données des clients. Cette vérification préalable d'absence de vulnérabilité fait partie des tests élémentaires qui doivent être réalisés par une société en matière de sécurité des systèmes d'information.
Par ailleurs, en sa qualité de responsable de traitement, la société aurait dû procéder de façon régulière à la revue des formulaires permettant d'alimenter l'outil de gestion des demandes de service après-vente. A ce titre, la formation restreinte a considéré qu'une bonne pratique en matière de sécurité des systèmes informatiques consiste à désactiver les fonctionnalités ou modules d'un outil qui ne seraient pas utilisés ou pas nécessaires.
La formation restreinte a néanmoins tenu compte notamment de l'initiative du responsable de traitement de diligenter un audit de sécurité après cette atteinte à la sécurité des données ainsi que de sa bonne coopération avec les services de la CNIL.
Pour approfondir
> Délibération n°SAN-2018-001 du 8 janvier 2018 Délibération de la formation restreinte n° SAN-2018-001 du 08/01/2018 prononçant une sanction pécuniaire à l'encontre de la société ETABLISSEMENTS DARTY ET FILS Etat: VIGUEUR

Faille non réparée après un premier contrôle
La Commission révèle en avoir rapidement informé Darty. Pourtant « la Cnil a constaté que les fiches des clients étaient toujours accessibles entre le premier et le second contrôle et que de nouvelles fiches avaient été créées dans ce laps de temps ».
Cette faille provenait en fait d'un logiciel de service après-vente proposé par un sous-traitant. Mais la Cnil a considéré « que le simple fait que la société fasse appel à un prestataire sous-traitant ne la décharge pas de son l'obligation de préserver la sécurité des données traitées pour son compte, en sa qualité de responsable du traitement »…[lire la suite]

Besoin d'un **accompagnement pour vous mettre en conformité avec le RGPD ?** ?
Besoin d'une **formation pour apprendre à vous mettre en conformité avec le RGPD** ?
Contactez-nous

A Lire aussi :
Mise en conformité RGPD : Mode d'emploi
Formation RGPD : L'essentiel sur le règlement Européen pour la Protection des Données Personnelles
Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016
DIRECTIVE (UE) 2016/680 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 27 avril 2016
Le RGPD, règlement européen de protection des données. Comment devenir DPO ?
Comprendre le Règlement Européen sur les données personnelles en 6 étapes
Notre sélection d'articles sur le RGPD (Règlement Européen sur la Protection des données Personnelles) et les DPO (Délégués à la Protection des Données)

Notre métier : Vous accompagner dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.
Par des actions de formation, de sensibilisation ou d'audits dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)
Plus d'informations sur : Formation RGPD : L'essentiel sur le règlement Européen pour la Protection des Données Personnelles

---

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle…) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ; (Autorisation de la DRTEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE Cybersécurité & Conformité

Contactez-nous

Réagissez à cet article

Source : *DARTY : sanction pécuniaire pour une atteinte à la sécurité des données clients*