Date de publication sur legifrance: 27/07/2017

Commission Nationale de l'Informatique et des Libertés

Délibération n°SAN-2017-010 du 18 juillet 2017
Délibération de la formation restreinte n° SAN-2017-010 du 18 juillet 2017 prononçant une sanction pécuniaire à l'encontre de la société HERTZ FRANCE

La Commission nationale de l'informatique et des libertés, réunie en sa formation restreinte composée de M. Jean-François CARREZ, Président, de M. Alexandre LINDEN, Vice-président, Mme Dominique CASTERA, Mme Marie-Hélène MITJAVILE et M. Maurice RONAI, membres ;

Vu la Convention n° 108 du Conseil de l'Europe du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel ;

Vu la directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données ;

Vu la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés, notamment ses articles 45 et suivants ;

Vu le décret n° 2005-1309 du 20 octobre 2005 modifié pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés ;

Vu la délibération n° 2013-175 du 4 juillet 2013 portant adoption du règlement intérieur de la Commission nationale de l'informatique et des libertés ;

Vu la décision n° 2016-304C du 21 octobre 2016 de la Présidente de la Commission nationale de l'informatique et des libertés de charger le secrétaire général de procéder ou de faire procéder à une mission de vérification de tous traitements relatifs au site CARTEREDUCTION-HERTZ.com ;

Vu la décision de la Présidente de la Commission portant désignation d'un rapporteur devant la formation restreinte, en date du 6 avril 2017 ;

Vu le rapport de Monsieur François PELLEGRINI, commissaire rapporteur, notifié à la société HERTZ FRANCE le 20 avril 2017 ;

Vu les observations écrites de la société HERTZ FRANCE reçues le 17 mai 2017, ainsi que les observations orales formulées lors de la séance de la formation restreinte ;

Vu les autres pièces du dossier ;

Etaient présents, lors de la séance de la formation restreinte du 1er juin 2017 :
M. François PELLEGRINI, Commissaire, en son rapport ;
En qualité de représentante de la société HERTZ FRANCE : Mme X, avocat ;

Mme Nacima BELKACEM, Commissaire du Gouvernement, n'ayant pas formulé d'observations ;

La représentante de la société HERTZ FRANCE ayant pris la parole en dernier ;

A adopté la décision suivante :

Faits et procédure

La société HERTZ FRANCE (ci-après, la société) a été créée en 1950 et a pour activité la location de véhicules aux particuliers et aux professionnels. Son siège social est situé au 1/3, avenue de Westphalie à Montigny-le-Bretonneux (78180). Elle emploie environ 1250 salariés. Son chiffre d'affaires pour l'année 2015 était de 396 233 000 euros. La société est une filiale détenue à 100% par la société THE HERTZ CORPORATION , située aux Etats-Unis.

Dans le cadre de ses activités, la société a créé en 2011 un programme proposant des réductions sur les locations de véhicules pour lequel a été conçu le site web www.cartereduction-hertz.com (ci-après, le site).

Le 15 octobre 2016, l'éditeur du site web www.zataz.com a informé les services de la Commission nationale de l'informatique et des libertés (ci-après la CNIL ou la Commission) que le traitement de données à caractère personnel accessible à partir de l'URL http://www.cartereduction-hertz.com/create_carte_cb.aspx permettrait une violation des données de plus de 40 000 clients de la société HERTZ FRANCE.

En application de la décision n° 2016-304C de la Présidente de la Commission du 21 octobre 2016, une mission de vérification en ligne a été opérée le jour même sur le site cartereduction-hertz.com . La délégation a alors constaté qu'en ajoutant à cette adresse URL la chaîne de caractères cartcb_id= et un numéro correspondant à un identifiant, les pages affichées faisaient apparaitre les données à caractère personnel renseignées par les personnes ayant adhéré au programme de réduction, notamment leurs nom et prénom, date de naissance, adresse postale, adresse de messagerie électronique et numéro de permis de conduire. La délégation a ainsi pu accéder aux données à caractère personnel de 35 327 personnes.

A l'issue du contrôle, la délégation a pris contact avec la société pour l'informer de l'existence d'une violation de données à caractère personnel sur le site.

Lors d'une seconde mission de contrôle effectuée au sein des locaux de la société HERTZ FRANCE le 28 octobre 2016, la délégation a été informée de ce que le développement du site avait été confié à un sous-traitant. La société a indiqué que dès qu'elle a été prévenue par CNIL de l'existence de la violation de données, elle en a immédiatement alerté son sous-traitant qui a mis en place les correctifs nécessaires. Ce dernier lui a indiqué que la violation de données avait pour origine la suppression involontaire d'une ligne de code lors du remplacement de l'un des serveurs assurant l'interface avec le prestataire en charge des paiements. A l'occasion de ce contrôle, la délégation a pu constater que la violation de données avait cessé.

Par courrier du 10 novembre 2016, la société a adressé le rapport d'incident établi par son sous-traitant. Il faisait notamment état de ce qu'en juin 2016, la société a changé son

infrastructure serveur et a reconfiguré son interface de programmation afin que celle-ci soit compatible avec l'interface de son prestataire de paiement. A cette occasion, une partie de code a été impactée par erreur, ce qui a provoqué l'incident de sécurité.

La société a par ailleurs indiqué qu'elle avait décidé de faire procéder à un audit de sécurité sur les traitements mis en œuvre pour son compte par son sous-traitant.

Le 16 novembre 2016, la délégation a effectué une mission de contrôle dans les locaux du sous-traitant de la société HERTZ FRANCE. Celui-ci a indiqué à la délégation qu'aucun cahier des charges spécifique à la mise en œuvre du site web ne lui avait été imposé par la société.

Le sous-traitant a confirmé à la délégation de contrôle que la violation de données avait pour origine la suppression involontaire d'une ligne de code lors du remplacement de l'un des serveurs, causant le réaffichage du formulaire contenant l'ensemble des données à caractère personnel renseignées par les personnes s'inscrivant au programme de réduction. Le sous-traitant a également précisé qu'il avait procédé à la mise en production des modifications nécessaires quelques heures après avoir été alerté par la société HERTZ FRANCE.

Le sous-traitant a indiqué à la délégation qu'une analyse des journaux d'accès au serveur avait permis de constater qu'aucun téléchargement massif de données n'avait été réalisé sur le serveur de la société.

Le 13 février 2017, la société HERTZ FRANCE a communiqué à la CNIL le rapport issu de l'audit réalisé par une société de conseil et d'expertise. Il ressort que le niveau global de sécurité chez le sous-traitant comportait des insuffisances. La société a enfin indiqué à la délégation que le sous-traitant avait déjà mis en place plusieurs recommandations formulées dans le rapport d'audit.

Aux fins d'instruction de ces éléments, la Présidente de la Commission a désigné M. PELLEGRINI en qualité de rapporteur, le 6 avril 2017, sur le fondement de l'article 46 de la loi du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés.

A l'issue de son instruction, le rapporteur a notifié à la société HERTZ France, le 20 avril 2017, un rapport détaillant les manquements à la loi Informatique et Libertés qu'il estimait constitués en l'espèce. Ce rapport proposait à la formation restreinte de la CNIL de prononcer une sanction pécuniaire rendue publique.

Etait également jointe au rapport une convocation à la séance de la formation restreinte du 1er juin 2017, indiquant à l'organisme qu'il disposait d'un délai d'un mois pour communiquer ses observations écrites.

La société a produit le 16 mai 2017 des observations écrites sur le rapport, réitérées oralement lors de la séance de la formation restreinte du 1er juin 2017.

Motifs de la décision

L'article 34 de la loi n° 78-17 du 6 janvier 1978 modifiée dispose que : Le responsable du traitement est tenu de prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des

données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès .

Il appartient à la formation restreinte de décider si la société HERTZ FRANCE a manqué à l'obligation lui incombant de mettre en œuvre des moyens propres à assurer la sécurité des données à caractère personnel contenues dans son système d'information et, en particulier, celles enregistrées par le biais de son site www.cartereduction-hertz.com , notamment afin que ces données ne soient pas accessibles à des tiers non autorisés.

En défense, la société rappelle que la violation de données a été portée à sa connaissance par la CNIL le 21 octobre 2016 à 18 h, qu'elle en a immédiatement informé son sous-traitant et que ce dernier a mis en œuvre les correctifs adéquats moins de quatre heures après le signalement de l'incident par les services de la Commission. Elle explique qu'elle a spontanément décidé de faire procéder à un audit de sécurité de son prestataire, qu'elle l'a communiqué à la CNIL et qu'à l'issue de cet audit, son sous-traitant a déjà déployé plusieurs recommandations préconisées par le rapport.

La société soutient ensuite que si les données à caractère personnel d'environ 35 000 personnes ont été concernées par la violation de données, aucune extraction massive de données n'a été effectuée à partir de ses serveurs. En outre, elle fait valoir qu'aucun titulaire de carte de réduction ne lui a rapporté que ses données avaient étés divulguées.

Enfin, la société indique que le contrat conclu avec son sous-traitant contient une clause spécifique à la protection des données à caractère personnel et que la survenance de la violation de données est la conséquence d'une erreur commise par celui-ci.

La formation restreinte relève que la société ne conteste pas la survenance d'un incident de sécurité sur le site www.cartereduction-hertz.com. ayant entrainé une violation de données à caractère personnel. Elle rappelle que cette violation de données a rendu accessibles les données identifiantes de 35 327 personnes telles que leur nom, prénom, date de naissance, adresse postale, adresse de messagerie électronique et numéro de permis de conduire.

La formation restreinte considère que la violation de données résulte d'une négligence de la société dans la surveillance des actions de son sous-traitant. Elle note tout d'abord que la société n'a imposé aucun cahier des charges à son prestataire s'agissant du développement du site. La formation restreinte relève ensuite que l'opération de changement de serveur, à l'origine de la violation de données, concernait les serveurs permettant de communiquer avec le prestataire de paiement et constituait donc une opération délicate requérant une attention particulière. Selon la formation restreinte, la société aurait dû s'assurer, à la suite de cette opération, que la mise en production du site avait été précédée d'un protocole complet de test afin de garantir l'absence de toute vulnérabilité.

Compte tenu de ces éléments, la formation restreinte considère que la société n'a pas pris toutes les précautions utiles afin d'empêcher que des tiers non autorisés aient accès aux données traitées.

La formation restreinte note, toutefois, que la société a réagi rapidement dès qu'elle a eu connaissance de la violation de données en alertant son sous-traitant et qu'il a été mis fin à la violation de données dans un délai très bref. Elle prend également acte de ce que l'incident de sécurité est la conséquence d'une erreur humaine qui ne semble pas avoir

donné lieu à une extraction massive de données par des tiers non autorisés. Enfin, la formation restreinte relève que la société a pris l'initiative de faire procéder à un audit de sécurité de son sous-traitant quelques semaines seulement après la survenance de la violation de données.

Sur la sanction et la publicité
Au regard des éléments développés ci-dessus, les faits constatés constituent un manquement aux dispositions de l'article 34 de la loi du 6 janvier 1978 modifiée.

La formation restreinte relève que la société a fait preuve de négligence dans le suivi des actions de son sous-traitant, ce qui a permis l'accessibilité de données à caractère personnel variées et directement identifiantes se rapportant à un volume important de clients, en l'occurrence 35 327 personnes. La formation restreinte note, en revanche, la grande réactivité de la société dans la résolution de la violation de données, les initiatives prises en termes d'audits de sécurité et sa bonne coopération avec la Commission.

Au regard de ces éléments, une sanction d'un montant de 40.000 euros apparait justifiée.

La formation restreinte considère qu'au regard du contexte actuel dans lequel se multiplient les incidents de sécurité, il y a lieu de rendre publique sa décision.

PAR CES MOTIFS

La formation restreinte de la CNIL, après en avoir délibéré, décide de :

prononcer une sanction pécuniaire à l'encontre de la société HERTZ France d'un montant de 40.000 euros ;
rendre publique sa délibération, qui sera anonymisée à l'expiration d'un délai de deux ans à compter de sa publication.

Le Président

Jean-François CARREZ

Cette décision est susceptible de faire l'objet d'un recours devant le Conseil d'Etat dans un délai de deux mois à compter de sa notification.

Nature de la délibération: SANCTION