Date de publication sur legifrance: 09/01/2018

**Commission Nationale de l'Informatique et des Libertés**

**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 X**

**Délibération de la formation restreinte n° SAN-2018-001 du 08/01/2018 prononçant une sanction pécuniaire à l'encontre de la société X**

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, 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° 2017-068C du 1er mars 2017 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 accessibles à partir de l'URL […] ;

Vu la décision de la Présidente de la Commission portant désignation d'un rapporteur devant la formation restreinte, en date du 1er juin 2017 ;

Vu le rapport de Monsieur François PELLEGRINI, commissaire rapporteur, notifié à la société X le 17 juillet 2017 ;

Vu la demande de huis clos présentée par la société X le 7 septembre 2017 à laquelle il a été fait droit par courrier du 18 septembre 2017 ;

Vu les observations écrites de la société X reçues le 7 septembre 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 21 septembre 2017 :

- M. François PELLEGRINI, Commissaire, en son rapport ;
- Maître X, […] ;
- Mme Y, […] ;
- M. Z, […] ;
- M. XY, […] ;
- M. YZ, […] ;

M. Michel TEIXEIRA, Commissaire du Gouvernement adjoint, n'ayant pas formulé d'observations ;

Le conseil de la société X ayant pris la parole en dernier ;

A adopté la décision suivante :

- Faits et procédure

La société X (ci-après la société ) a pour activité le commerce de détail d'appareils électroménagers en magasin spécialisé. Son siège social est situé […].Elle emploie environ 4400 salariés et son chiffre d'affaires pour l'année 2016 s'élevait à environ 2,4 milliards d'euros. La société fait partie du groupe Y depuis juillet 2016.

Le 27 février 2017, l'éditeur d'un site internet spécialisé dans la sécurité des systèmes d'information a informé les services de la Commission nationale de l'informatique et des libertés (ci-après la CNIL ou la Commission) d'une violation de données à caractère personnel à partir de l'URL […]. L'éditeur indiquait que cette violation aurait permis d'accéder à plusieurs milliers de données de clients de la société.

En application de la décision n° 2017-068C de la Présidente de la Commission du 1er mars 2017 une délégation de la Commission a procédé à des missions de contrôle en ligne et sur place au sein des locaux de la société les 2 et 15 mars 2017. Les procès-verbaux de constats n° 2017-068 et n°2017-068/2, dressés à l'issue de ces missions, ont été notifiés à la société respectivement les 10 et 20 mars suivants.

Lors du contrôle en ligne du 2 mars 2017, la délégation a constaté que l'URL […] renvoyait vers un formulaire permettant aux clients de la société de déposer une demande de service après-vente. Une fois le formulaire obligatoirement renseigné d'une adresse électronique et d'un mot de passe, un lien hypertexte correspondant au numéro d'enregistrement de la demande permettait d'accéder à son suivi. La délégation a constaté que cet identifiant (un numéro de ticket ) est contenu dans l'adresse URL construite de la façon suivante : […] . Elle a relevé qu'en modifiant le numéro d'identifiant dans cette adresse URL, les fiches de demande de service après-vente remplies par d'autres clients de la société étaient accessibles.

La délégation a ainsi pu relever que 912 938 fiches étaient potentiellement accessibles et a procédé au téléchargement, par échantillonnage, de 7 417 d'entre elles. Il a été constaté que des données à caractère personnel de clients étaient accessibles sur des fiches, telles que leur nom, prénom, adresse postale, adresse de messagerie électronique ainsi que leurs commandes.

A l'issue du contrôle, la délégation a pris contact avec la société pour l'informer de

l'existence de cette violation de données à caractère personnel.

Lors du contrôle sur place effectué au sein des locaux de la société le 15 mars 2017, ayant pour objet de vérifier les mesures correctrices prises à la suite de la révélation de la violation de données, la délégation a été informée du fait que la société utilise pour la gestion des demandes de service après-vente de ses clients un outil fourni par son sous-traitant, la société Z.

Cet outil est en principe alimenté par deux sources: le formulaire de demande de service après-vente accessible depuis le site de la société X et les demandes adressées par courrier électronique à une adresse dédiée. Le formulaire accessible depuis l'URL litigieuse […] constitue une troisième source d'alimentation. Ce dernier formulaire, dont la société indique n'avoir pas eu connaissance, correspond au formulaire natif développé et commercialisé par la société Z dans sa solution de gestion des demandes de service après-vente. La société a précisé qu'elle ne l'utilisait pas et qu'il n'aurait pas dû être accessible.

La délégation de la CNIL a, en outre, été informée de ce que l'URL de la forme […] permet d'accéder à l'intégralité des demandes contenues dans l'outil de gestion des demandes de service après-vente, y compris aux demandes formulées *via* le formulaire disponible sur le site […] et par courriers électroniques.

La société lui a également indiqué avoir contacté la société Z dès le 6 mars 2017 afin qu'elle prenne les mesures nécessaires, cette dernière lui ayant précisé que les modifications, non aisées à déployer, n'étaient pas mises en place.
La délégation a alors constaté qu'en modifiant l'identifiant numérique dans l'URL […], 918 721 fiches de demande de service après-vente de clients étaient toujours accessibles, dont 5 783 nouvelles fiches créées depuis le contrôle en ligne.
Par courrier électronique adressé à la CNIL le 16 mars 2017, la société a indiqué avoir mis en place les mesures de sécurisation nécessaires dans la soirée du 15 mars 2017, jour du contrôle sur place.

Aux fins d'instruction de ces éléments, la Présidente de la Commission a désigné M. PELLEGRINI en qualité de rapporteur, le 1er juin 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 (ci-après loi du 6 janvier 1978 modifiée ou loi Informatique et Libertés ).

A l'issue de son instruction, le rapporteur a notifié à la société, le 17 juillet 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 de 200 000 euros, qui serait rendue publique.

Etait également jointe au rapport une convocation à la séance de la formation restreinte du 21 septembre 2017, indiquant à l'organisme qu'il avait jusqu'au 7 septembre 2017 pour communiquer ses observations.

La société a produit le 7 septembre 2017 des observations écrites sur le rapport, réitérées oralement lors de la séance de la formation restreinte du 21 septembre 2017.

· Motifs de la décision

L'article 34 de la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux

fichiers et aux libertés 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 X a manqué à l'obligation lui incombant de mettre en œuvre des moyens propres à assurer la sécurité des données à caractère personnel traitées dans le cadre de la gestion des demandes de service après-vente de ses clients, en particulier d'empêcher que les données ne soient accessibles à des tiers non autorisés.

· **Sur la qualité de responsable de traitement**

Le I de l'article 3 de la loi n° 78-17 du 6 janvier 1978 modifiée dispose que *le responsable d'un traitement de données à caractère personnel est, sauf désignation expresse par les dispositions législatives ou réglementaires relatives à ce traitement, la personne, l'autorité publique, le service ou l'organisme qui détermine ses finalités et ses moyens* .

L'article 35 de la loi précitée dispose que : *Les données à caractère personnel ne peuvent faire l'objet d'une opération de traitement de la part d'un sous-traitant, d'une personne agissant sous l'autorité du responsable du traitement ou de celle du sous-traitant, que sur instruction du responsable du traitement. Toute personne traitant des données à caractère personnel pour le compte du responsable du traitement est considérée comme un sous-traitant au sens de la présente loi. Le sous-traitant doit présenter des garanties suffisantes pour assurer la mise en œuvre des mesures de sécurité et de confidentialité mentionnées à l'article 34. Cette exigence ne décharge pas le responsable du traitement de son obligation de veiller au respect de ces mesures. Le contrat liant le sous-traitant au responsable du traitement comporte l'indication des obligations incombant au sous-traitant en matière de protection de la sécurité et de la confidentialité des données et prévoit que le sous-traitant ne peut agir que sur instruction du responsable du traitement .*

· **Sur la détermination par la société des finalités et des moyens de traitement**

La société soutient qu'elle ne dispose pas de la qualité de responsable de traitement concernant les traitements affectés par la violation de données, c'est-à-dire ceux accessibles à partir de l'URL […]

La société indique n'avoir jamais consulté ou utilisé l'URL litigieuse susvisée, qui appartient à la société Z, pour traiter les demandes de ses clients. Elle dispose de son propre formulaire de collecte disponible sur son site […].

Elle souligne que, conformément au cahier des charges annexé au contrat de prestation de services conclu entre elle et la société Z le 18 avril 2012, le formulaire natif de Z n'a jamais été demandé par la société X, ni proposé par la société Z.

La société considère ne pas avoir déterminé tous les moyens mis en œuvre par la société Z, cette dernière ayant développé de sa propre initiative et pour des finalités qui lui sont propres le formulaire de demande de service après-vente accessible *via* l'URL litigieuse.

Elle indique que le contenu, le format, le choix des données collectées, le caractère obligatoire ou facultatif des champs de collecte de ce formulaire sont définis par la société Z et ne sont pas personnalisables.

La formation restreinte rappelle que la notion de responsable de traitement doit être interprétée *in concreto.* A ce titre, le groupe de travail de l'article 29 (dit G29 ) précise dans un avis 1/2010 du 16 février 2010 sur la notion de responsable de traitement et de sous-traitant, qu' : *Être responsable du traitement résulte essentiellement du fait qu'une entité a choisi de traiter des données à caractère personnel pour des finalités qui lui sont propres* .

En l'espèce, la société X a fait appel aux services de la société Z pour la gestion et le traitement des demandes de service après-vente de ses clients.

La formation restreinte relève que ces demandes peuvent résulter du formulaire propre de la société X, d'une demande adressée à une adresse électronique dédiée mais également du formulaire développé par la société Z, accessible *via* l'URL […]. L'ensemble de ces demandes se rattachent à un seul et même traitement, celui des données à caractère personnel des clients de la société X, pour une finalité unique de suivi des demandes de service après-vente adressées à cette société. A cet égard, les demandes formulées *via* l'URL […] sont versées dans l'outil de gestion des demandes de service après-vente et sont bien traitées par les services de la société.

La formation restreinte relève également qu'il ne ressort d'aucune pièce du dossier que la société Z traiterait pour son propre compte et pour des finalités qui seraient différentes de celles de la société X, les données à caractère personnel des clients de cette dernière, renseignées dans le formulaire de demande de service après-vente accessible *via* l'URL […].

A ce titre, la formation restreinte rappelle que le G29 dans son avis susvisé, précise que si, en complément du service rendu au responsable de traitement, un contractant procédait au traitement également *à des fins personnelles, par exemple en utilisant les données à caractère personnel reçues en vue de créer des services à valeur ajoutée, il deviendrait alors responsable du traitement (ou éventuellement coresponsable du traitement)* .

La formation restreinte considère que la seule finalité du traitement des données accessibles *via* l'URL […] est celle poursuivie par la société X, à savoir la gestion des demandes de service après-vente.

La formation restreinte en déduit que la société X détermine la finalité du traitement des données collectées *via* l'URL litigieuse.

Concernant les moyens de traitement, la formation restreinte rappelle que le G29 dans son avis susmentionné précise que: *La détermination des moyens englobe [...] à la fois des questions techniques et d'organisation, auxquelles les sous-traitants peuvent tout aussi bien répondre (par exemple, quel matériel informatique ou logiciel utiliser?), et des aspects essentiels qui sont traditionnellement et intrinsèquement réservés à l'appréciation du responsable du traitement, tels que quelles sont les données à traiter?, pendant combien de temps doivent-elles être traitées?, qui doit y avoir accès, etc.*

En l'espèce, si la société Z a mis à disposition le formulaire accessible *via* l'URL […] sans que la société X n'en ait connaissance, la circonstance qu'elle aurait décidé seule d'ajouter ce moyen de traitement - en plus des autres moyens déterminés dans le cadre du contrat de prestations conclu entre les deux sociétés - ne saurait suffire à la considérer

comme responsable de traitement.

Par ailleurs, la formation restreinte relève que c'est bien la société X qui a choisi de recourir à la solution de gestion proposée par la société Z pour les demandes de service après-vente de ses clients.

En outre, les données à caractère personnel qui sont contenues dans le formulaire développé par la société Z sont celles des clients de la société X auxquelles seuls les salariés de cette dernière ont, en principe, accès.

La formation restreinte estime que l'ensemble de ces éléments confirment que la société X détermine au moins pour partie les moyens du traitement.

En conséquence, la formation restreinte considère que la société X doit être qualifiée de responsable de traitement en ce qu'elle détermine la finalité et les moyens du traitement des données accessibles à partir de l'URL […].

· **Sur la responsabilité de la société**

La société soutient qu'elle ne peut être tenue personnellement responsable car la société Z n'a pas agi sur ses instructions, en méconnaissance de l'article 35 de la loi du 6 janvier 1978 modifiée.

Elle affirme notamment que la société Z a agi hors du cadre défini par le cahier des charges annexé au contrat de prestations de services conclu entre les deux sociétés le 18 avril 2012. La société indique sur ce point n'avoir ni commandité, ni accepté le formulaire de demande de service après-vente mis en œuvre par la société Z, dont elle n'avait pas connaissance.

La formation restreinte rappelle qu'il résulte de l'article 35 de la loi du 6 janvier 1978 modifiée que la circonstance que des opérations de traitement de données soient confiées à des sous-traitants ne décharge pas le responsable de traitement de la responsabilité qui lui incombe de préserver la sécurité des données traitées pour son compte (CE 11 mars 2015, Sté Total raffinage marketing et société X, n° 368748). Dans ses conclusions, le rapporteur public précise sur ce point : *Elle crée [l'intervention d'un prestataire] plutôt, une responsabilité supplémentaire de contrôle effectif des agissements du prestataire* .

La formation restreinte considère qu'il appartenait à la société, en sa qualité de responsable de traitement, de s'assurer et de vérifier que toutes les composantes et options de l'outil de gestion des demandes de service après-vente développées par la société Z répondaient à l'obligation de confidentialité énoncée à l'article 34 de la loi précitée. Au besoin et en application de règles de bonnes pratiques en matière informatique, il revenait à la société de faire désactiver tous les modules inutilement mis en œuvre par son prestataire.

· **Sur le manquement à l'obligation d'assurer la sécurité des données au titre de l'article 34 de la loi du 6 janvier 1978 modifiée**

En défense, la société explique avoir choisi la société Z en raison des garanties sérieuses qu'elle présentait en matière de sécurité. Elle indique par ailleurs avoir exigé dans le cahier des charges annexé au contrat de prestations de service du 18 avril 2012, que seuls ses salariés, autorisés aient accès aux données des messages électroniques entrants de son service client.

La société affirme également que la violation de données n'a été portée à sa connaissance par les services de la CNIL que le 6 mars 2017 et qu'elle a, le jour même, ouvert un ticket d'incident avec le niveau de criticité le plus élevé chez son prestataire.

Elle indique s'être assurée par la suite du suivi de la résolution complète de la violation de données par son prestataire.

La société […] soutient notamment que le comportement des services de la CNIL ne lui permettait pas de considérer que la violation de données en question présentait un risque important pour la sécurité des données.

La société précise en outre avoir réalisé un audit de sécurité les 23 et 24 août 2017 sur la nouvelle version de l'outil de gestion des demandes de service après-vente de la société Z […]

La société soutient ensuite, s'agissant des 7 417 fiches téléchargées, par les services de la CNIL dont 9 non remplies, qu'un nombre important ne comporte aucune donnée à caractère personnel, qu'elles n'étaient pas destinées à recevoir des données sensibles ou des numéros de cartes bancaires et qu'elles étaient difficilement exploitables à grande échelle.

La formation restreinte rappelle qu'une violation de données est réalisée dès lors que des données à caractère personnel ont été rendues accessibles, volontairement ou non, à des tiers non autorisés. En l'espèce, les enquêteurs de la Commission ont pu accéder aux demandes de service après-vente formulées par les clients de la société, confirmant ainsi le défaut de sécurisation signalé par un tiers.

La formation restreinte note que la violation de données en question trouve son origine dans le système de filtrage des URLs permettant l'accès aux formulaires de demande de service après-vente. Ce filtrage est assuré par Z, le prestataire de la société.

La formation restreinte considère qu'en retenant un logiciel standard dit sur étagère proposé par son prestataire, il incombait à la société de procéder aux vérifications des caractéristiques de ce produit qui auraient permis d'identifier le risque résultant de l'existence d'un accès aux données des clients contenues dans l'outil de gestion des demandes de service après-vente et d'empêcher celui-ci.

La vérification préalable notamment des règles de filtrage des URL fait partie des tests élémentaires qui doivent être réalisés par une société en matière de sécurité des systèmes informatiques.

En outre, la formation restreinte considère qu'il appartenait à la société de procéder de façon régulière à la revue des formulaires de demande de service après-vente accessibles et permettant d'alimenter l'outil de gestion des demandes de service après-vente. A ce titre, elle souligne 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.

De plus, la formation restreinte estime que la société a fait preuve de négligence dans la surveillance des actions de son prestataire dans la résolution de la violation. La formation restreinte relève ainsi que ce n'est qu'après le second contrôle de la CNIL, le 15 mars

2017, que la violation de données a pris fin. A ce titre, elle rappelle que depuis le premier contrôle en ligne le 2 mars 2017, 5 783 nouvelles fiches clients avaient été créées, portant à 918 721 le nombre de fiches accessibles le 15 mars 2017.

La formation restreinte relève également que contrairement aux observations en défense de la société, celle-ci n'établit pas avoir quotidiennement demandé à la société Z des justificatifs sur les mesures correctives mises en place et ce jusqu'à la résolution complète de la violation de données, le 15 mars 2017. Au contraire, à la suite du ticket d'incident ouvert le 6 mars 2017 auprès de Z, il apparaît qu'une seule demande de précisions a été formulée par la société le 9 mars suivant. La formation restreinte en déduit donc que la société n'a pas procédé à un suivi régulier de la résolution de la violation de données auprès de son prestataire.

La formation restreinte note également que cette violation a pu concerner plusieurs centaines de milliers de clients de la société, le nombre de fiches de demandes de service après-vente s'élevant à 918 721 au jour du second contrôle. En outre, des données à caractère personnel telles que leur nom, prénom, adresse postale, adresse de messagerie électronique ainsi que leurs commandes ont été rendues accessibles.

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. Elle a ainsi méconnu les obligations qui lui incombent au titre de l'article 34 de la loi du 6 janvier 1978 modifiée.

· Sur la sanction et la publicité

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 de nombreux clients.

Si la formation restreinte prend acte de l'absence de traitement de données sensibles telles que définies à l'article 8 de la loi du 6 janvier 1978 modifiée ou de données bancaires, pour autant, elle considère que le manquement à la sécurité et à la confidentialité est grave en raison de la multitude de catégories de données traitées qui révèlent des informations sur les personnes et leur vie privée, au travers notamment des commandes passées.

La formation restreinte note, en revanche, que la société a réagi 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 raisonnable. Elle relève également que la société a pris l'initiative, après la survenance de la violation de données, de faire procéder à un audit de sécurité en août 2017 sur la nouvelle version de l'outil de gestion des demandes de service après-vente proposé par son prestataire. Elle note, enfin, sa bonne coopération avec la Commission.

Au regard de ces éléments, une sanction d'un montant de 100.000 (cent mille) euros apparait proportionnée.

La formation restreinte considère qu'au regard des éléments précités, du contexte actuel dans lequel se multiplient les incidents de sécurité et de la nécessité de sensibiliser les internautes de quant au risque pesant sur la sécurité de leurs données, 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 X d'un montant de 100.000 (cent mille) 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.