**Délibération de la formation restreinte n° 2015-454 du 21 décembre 2015 prononçant un avertissement public à l'encontre de la société PROFILS SENIORS**

La Commission nationale de l'informatique et des libertés, réunie en sa formation restreinte composée de M. Jean-François CARREZ, Président, M. Alexandre LINDEN, Vice-président, M. Philippe GOSSELIN 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 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 saisine n° 13025004 reçue le 13 août 2013 ;

Vu la décision de la Présidente de la Commission nationale de l'informatique et des libertés portant désignation d'un rapporteur, en date du 7 août 2015 ;

Vu le rapport de M. François PELLEGRINI, commissaire rapporteur, adressé à la société PROFILS SENIORS le 14 septembre 2015 par courrier recommandé avec avis de réception, distribué le 15 septembre 2015 ;

Vu les observations écrites versées par la société PROFILS SENIORS le 15 octobre 2015, ainsi que les observations orales formulées lors de la séance de la formation restreinte ;

Vu les autres pièces du dossier.

Ayant entendu, lors de la séance de la formation restreinte du 22 octobre 2015,

- M. François PELLEGRINI, commissaire, en son rapport ;
- Mme Catherine POZZO DI BORGO, Commissaire du Gouvernement adjoint, n'ayant pas formulé d'observation ;
- Monsieur [redacted] de la Société PROFILS SENIORS ;
- Maître [redacted], Avocat associé [redacted] ;
- Monsieur [redacted], Juriste [redacted].

La société PROFILS SENIORS ayant pris la parole en dernier ;

A adopté la décision suivante :

## I. Faits et procédure

La société PROFILS SENIORS (ci-après « la société ») a pour activité principale la constitution d'une base de données relative aux « seniors » français.

Cette base de données, qui compte les données à caractère personnel de plus d'un million de personnes, est destinée à la location à des tiers, en particulier à des fins de prospection commerciale. La société édite par ailleurs le site web « profils-seniors.com » qui propose notamment des sondages en ligne.

La Commission nationale de l'informatique et des libertés (ci-après « la CNIL » ou « la Commission ») a été saisie par un plaignant le 13 août 2013 qui dénonçait l'absence de réponse de la société PROFILS SENIORS à sa demande d'accès aux informations le concernant, ainsi qu'à ses demandes d'opposition tant à la communication de ses données à des tiers qu'à la prospection directe téléphonique. Après que la société a répondu de manière satisfaisante au plaignant, la CNIL a procédé à la clôture de sa plainte le 22 octobre 2013.

Le 26 mars 2015, en application de la décision n° 2015-087C du 18 mars 2015 de la Présidente de la CNIL, la CNIL a procédé à une mission de contrôle dans les locaux de la société PROFILS SENIORS, afin notamment de vérifier le respect par la société des dispositions de la loi du 6 janvier 1978 modifiée.

A cette occasion, la société PROFILS SENIORS a indiqué avoir recours à plusieurs prestataires de service, dont la société [redacted], située à l'Ile Maurice. Cette société, qui gère un centre d'appel, est en charge de contacter des « seniors », en se présentant comme le « cabinet d'études PROFILS SENIORS », pour les interroger sur leurs habitudes de vie et collecter notamment leurs cordonnées postales, téléphoniques et électroniques. Les données ainsi collectées sont déposées sur une plateforme d'hébergement gérée par la société [redacted]. Celle-ci adresse, aux personnes ayant été contactées par [redacted], un courriel de remerciement en précisant que la société PROFILS SENIORS se permettra d'adresser *« par courrier, téléphone ou email des offres choisies auprès d'un club d'annonceurs partenaires »*.

La société PROFILS SENIORS accède aux données collectées, qui sont hébergées par [redacted], via un espace d'administration dédié accessible depuis le web.

Enfin, la société PROFILS SENIORS a indiqué procéder à la location de sa base de données à des tiers, par l'intermédiaire de courtiers qui y accèdent soit par une extraction qui leur est adressée au format ZIP par courriel, soit en se connectant au répertoire de téléchargement de la base de données mise à leur disposition.

Aux fins d'instruction de ces éléments, la Présidente de la Commission a désigné M. François PELLEGRINI en qualité de rapporteur, le 7 août 2015, sur le fondement de l'article 46 de la loi du 6 janvier 1978 modifiée.

A l'issue de son instruction, le rapporteur a notifié à la société, le 14 septembre 2015 par courrier recommandé avec avis de réception, distribué le 15 septembre 2015, un rapport détaillant les manquements à la loi qu'il estimait constitués en l'espèce. Ce rapport proposait à la formation restreinte de la CNIL de prononcer un avertissement, dont il sollicitait par ailleurs qu'il soit rendu public. Etait également jointe au rapport une convocation à la séance de la formation restreinte du 22 octobre 2015 indiquant à l'organisme qu'il disposait d'un délai d'un mois pour communiquer ses observations écrites.

Le 15 octobre 2015, la société PROFILS SENIORS a produit par courrier daté du 14 octobre 2015 des observations écrites sur le rapport, réitérées oralement lors de la séance de la formation restreinte du 22 octobre 2015.

## II. Motifs de la décision

### 1. Sur le manquement à l'obligation d'effectuer les formalités préalables à la mise en œuvre d'un traitement

L'article 22-I de la loi du 6 janvier 1978 modifiée dispose que « *A l'exception de ceux qui relèvent des dispositions prévues aux articles 25, 26 et 27 ou qui sont visés au deuxième alinéa de l'article 36, les traitements automatisés de données à caractère personnel font l'objet d'une déclaration auprès de la Commission nationale de l'informatique et des libertés* ».

Il ressort des pièces du contrôle, sans que cela ne soit contesté, que la société procède à la collecte de données à caractère personnel, telles que notamment les nom, prénom, adresse postale, adresse électronique, auprès de « seniors » pour constituer une base de données à des fins de location à des tiers. Il a en outre été relevé que la société PROFILS SENIORS n'a procédé à aucune formalité préalable auprès de la CNIL à cet égard.

En défense, la société reconnaît avoir cru, à tort, pouvoir bénéficier des formalités accomplies antérieurement par la société [redacted] qui lui avait cédé ses actifs. Elle indique avoir procédé auprès de la CNIL, depuis la notification du rapport de sanction, à une déclaration du traitement de données à caractère personnel concerné.

La formation restreinte considère que la société ne peut se prévaloir des formalités effectuées par la société [redacted]. En effet, comme cela avait été précisé par la CNIL dans un courrier en réponse de 2011, le rachat des actifs de cette société ne dispensait pas la société PROFILS SENIORS d'effectuer les formalités préalables, dès lors que cette dernière devenait désormais la responsable du traitement concerné. En outre, elle considère que la circonstance que la société ait procédé à la déclaration de son traitement de données à caractère personnel auprès de la CNIL est sans incidence sur la caractérisation du manquement à l'obligation d'effectuer les formalités, préalablement à la mise en œuvre du traitement.

### 2. Sur le manquement à l'obligation de respecter les dispositions relatives aux transferts de données hors de l'Union européenne

L'article 68 de la loi du 6 janvier 1978 modifiée dispose que « *Le responsable d'un traitement ne peut transférer des données à caractère personnel vers un Etat n'appartenant pas à la Communauté européenne que si cet Etat assure un niveau de protection suffisant de la vie privée et des libertés et droits fondamentaux des personnes à l'égard du traitement dont ces données font l'objet ou peuvent faire l'objet. / Le caractère suffisant du niveau de protection assuré par un Etat s'apprécie en fonction notamment des dispositions en vigueur dans cet Etat, des mesures de sécurité qui y sont appliquées, des caractéristiques propres du traitement, telles que ses fins et sa durée, ainsi que de la nature, de l'origine et de la destination des données traitées* ».

L'article 69 de la loi du 6 janvier 1978 susmentionnée dispose qu'il « *peut également être fait exception à l'interdiction prévue à l'article 68, par décision de la Commission nationale de l'informatique et des libertés (...) lorsque le traitement garantit un niveau de protection suffisant de la vie privée ainsi que des libertés et droits fondamentaux des personnes, notamment en raison des clauses contractuelles ou règles internes dont il fait l'objet* ».

La CNIL a constaté, sans que cela ne soit contesté, que la société recourt aux services de la société [redacted], située à l'Île Maurice, sans avoir conclu un quelconque contrat. Pour autant, cette dernière contacte par téléphone, au nom de la société PROFILS SENIORS, des personnes choisies dans l'annuaire afin de collecter leurs données à caractère personnel, ce qui constitue *de facto* un transfert de données hors de l'Union européenne.

En défense, la société reconnaît que son prestataire est situé dans un Etat qui n'est pas considéré par la Commission européenne comme un pays assurant un niveau de protection adéquat et qu'elle ne l'a pas soumis à des clauses contractuelles types, telles que celles proposées par la Commission Européenne. Toutefois, la société précise l'avoir fait, depuis la notification du rapport de sanction, et avoir sollicité l'autorisation de la CNIL sur ce transfert à l'occasion de la déclaration de son traitement effectuée le 14 octobre 2015.

La formation restreinte rappelle que le principe d'interdiction de transférer des données vers un Etat n'appartenant pas à l'Union européenne et n'assurant pas un niveau de protection suffisant de la vie privée, tel qu'en l'espèce, ne peut être levé qu'après une décision de la CNIL. En effet, celle-ci doit apprécier si le traitement garantit un niveau de protection suffisant, notamment en raison des clauses contractuelles ou règles internes dont il fait l'objet. Par conséquent, sans décision préalable de la CNIL, le traitement de flux ne saurait en aucune manière être mis en œuvre. La formation restreinte considère par ailleurs que la circonstance que la société ait conclu un contrat avec son prestataire sur la base de clauses contractuelles type de la Commission européenne par la suite et ait sollicité l'autorisation de la CNIL à cet égard est sans incidence sur la caractérisation du manquement.

### 3. Sur le manquement à l'obligation d'effectuer une collecte loyale des données

L'article 6-1° de la loi n° 78-17 du 6 janvier 1978 dispose que *« les données à caractère personnel sont collectées et traitées de manière loyale et licite »*.

La Commission a constaté que le script d'appel, fourni par la société PROFILS SENIORS à son prestataire [redacted], ne permet pas d'informer correctement les personnes de la finalité de la collecte de leurs données. En effet, il est indiqué aux personnes appelées que la société PROFILS SENIORS *« réalis[e] des enquêtes sur la consommation des ménages en France, en collaboration avec des partenaires qui pourront [les] solliciter pour leurs propres besoins »*. Cette information est de nature à induire en erreur les personnes sollicitées, ces dernières pensant participer à une étude alors que la finalité de la collecte de leurs données est de constituer un fichier destiné à la location à des tiers opérant un démarchage commercial.

En défense, la société estime que le script d'appel délivre les mentions d'information relatives à l'article 32 de la loi du 6 janvier 1978 modifiée même si elle reconnaît que la finalité de la collecte des données aux fins de prospection n'est pas suffisamment mise en avant. Elle indique en tout état de cause avoir procédé à la modification du script d'appel et l'avoir notifié à la société [redacted].

La formation restreinte considère que le message délivré à l'occasion de l'appel ne permet pas aux personnes concernées de comprendre la finalité réelle de la collecte de leurs données. En effet, il ressort des éléments du dossier que les personnes appelées pensent participer à une enquête sur la consommation des ménages français, alors que la finalité réelle est de constituer une base de données de seniors qui feront l'objet de prospection commerciale électronique par des tiers, partenaires de la société PROFILS SENIORS. Le caractère particulièrement vague de l'information conduit ainsi les personnes à délivrer un nombre

important d'informations les concernant, en conséquence de quoi la formation restreinte considère que la collecte des données à caractère personnel auprès des personnes appelées est déloyale. Elle considère en outre que les correctifs apportés au script d'appel, qui par ailleurs ne précisent toujours pas la finalité de prospection commerciale électronique, sont sans incidence sur la caractérisation du manquement.

### 4. Sur le manquement à l'obligation de recueillir le consentement des personnes au traitement de leurs données par des tiers

L'article L. 34-5 du code des postes et des communications électroniques dispose qu'« *Est interdite la prospection directe au moyen de système automatisé de communications électroniques au sens du 6° de l'article L. 32, d'un télécopieur ou de courriers électroniques utilisant les coordonnées d'une personne physique, abonné ou utilisateur, qui n'a pas exprimé préalablement son consentement à recevoir des prospections directes par ce moyen. / Pour l'application du présent article, on entend par consentement toute manifestation de volonté libre, spécifique et informée par laquelle une personne accepte que des données à caractère personnel la concernant soient utilisées à fin de prospection directe. / Constitue une prospection directe l'envoi de tout message destiné à promouvoir, directement ou indirectement, des biens, des services ou l'image d'une personne vendant des biens ou fournissant des services. Pour l'application du présent article, les appels et messages ayant pour objet d'inciter l'utilisateur ou l'abonné à appeler un numéro surtaxé ou à envoyer un message textuel surtaxé relèvent également de la prospection directe. [...]* ».

Le contrôle a permis de constater que la société ne recueille pas le consentement des personnes préalablement à l'envoi par des tiers de courriels de prospection commerciale. En effet, il a été constaté que les personnes appelées sont uniquement informées que la société PROFILS SENIORS réalise *« des enquêtes sur la consommation des ménages en France, en collaboration avec des partenaires qui pourront [les] solliciter pour leurs propres besoins »*. Le courriel qui leur est envoyé ensuite indique qu'elles se verront *« adresser par courrier, téléphone et email, des offres choisies auprès d'un club d'annonceurs partenaires »* et qu'elles peuvent s'y opposer. Les personnes sont invitées à placer l'adresse électronique de la société dans la liste de leurs contacts afin d'éviter un classement erroné en spam des courriels de la société.

En défense, la société fait valoir que le consentement non équivoque des personnes à recevoir de la prospection est recueilli, d'une part, à l'oral suivant le processus décrit dans le script d'appel et, d'autre part, lorsque la personne place l'adresse électronique de la société PROFILS SENIORS dans sa liste de contacts, comme elle y est invitée par courriel. En tout état de cause, elle précise avoir pris des mesures correctives en renforçant l'information délivrée aux personnes appelées, ainsi que dans le courriel adressé postérieurement.

La formation restreinte considère que les personnes concernées ne sont pas en mesure d'exprimer leur consentement à recevoir de la prospection commerciale par voie électronique au sens des dispositions de l'article L. 34-5 du CPCE. En effet, l'information prévue dans le script d'appel n'est pas suffisamment claire, précise et adéquate pour permettre aux personnes concernées de comprendre, sans ambiguïté, que la collecte de leurs données vise principalement à constituer une base de données à destination de tiers qui effectueront à leur égard de la prospection commerciale par voie électronique. Par ailleurs, le courriel de remerciement qui leur est adressé à l'issu de l'appel n'est pas non plus satisfaisant. En effet, ce courriel n'offre que la possibilité de s'opposer à la réception de la prospection commerciale

par voie électronique (« opt-out ») alors qu'en l'espèce le consentement doit être recueilli préalablement (« opt-in partenaires »).

### 5. Sur le manquement à l'obligation d'assurer la sécurité des données

L'article 34 de la loi 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 a manqué à l'obligation lui incombant de mettre en œuvre des moyens propres à assurer la sécurité des données des personnes concernées par le traitement et notamment des mesures adaptées pour que ces données ne soient pas communiquées à des tiers non autorisés.

Le contrôle a permis de constater que la société [redacted], prestataire de la société PROFILS SENIORS, transfère les données collectées à la société [redacted] qui les héberge. Il a été relevé que ce transfert s'opère via une connexion FTP, laquelle ne permet pas d'assurer la sécurité et la confidentialité des données, l'hôte ne pouvant être authentifié et le canal de communication n'étant pas chiffré.

Il a également été constaté que l'accès de la société PROFILS SENIORS à l'espace d'administration de sa base de données, hébergée par [redacted], s'effectue par le renseignement d'un identifiant personnel et d'un mot de passe [redacted], robustesse insuffisante pour sécuriser la base des données de plus d'un million de personnes. En outre, il a été constaté que trois utilisateurs bénéficiaient d'un compte leur permettant de se connecter à la base de données depuis Internet alors que deux d'entre eux avaient quitté la société, démontrant ainsi l'absence de gestion des habilitations délivrées. En outre, il a été constaté que la connexion à cette interface web utilise le protocole « http » non sécurisé, ce qui ne permet pas d'assurer le chiffrement du canal de communication ni d'authentifier le site distant.

Enfin, la délégation a constaté que la société PROFILS SENIORS loue sa base des données à des courtiers, soit en leur adressant par courriel une extraction de cette base au format zip et en leur adressant le mot de passe y afférent par le même canal de communication, soit en leur permettant d'accéder à une copie de la base de données via une connexion FTP non sécurisée.

En défense, la société ne conteste pas ces éléments et fait valoir les actions correctives qui ont été mises en place. Elle indique ainsi que son prestataire, la société [redacted], a fait l'acquisition d'un certificat SSL et mis en place le protocole « https » et un serveur « ftps » afin d'assurer le chiffrement des canaux de transmission des données et l'authentification des serveurs distants. Elle ajoute que la politique des mots de passe a également fait l'objet de modifications, des mots de passe [redacted] soumis à renouvellement régulier étant désormais imposés. Elle avance que les courtiers ne peuvent désormais accéder aux bases de données que par la plateforme hébergée par [redacted], par le biais du même protocole sécurisé. Enfin, elle précise que les profils administrateurs des deux anciens salariés de la société ont fait l'objet d'une suppression en présence de la délégation de contrôle.

La formation restreinte prend acte des mesures correctives mais considère que la société n'avait pas mis en œuvre des moyens suffisants pour répondre à l'obligation de sécurité et de confidentialité des données imposée par la loi du 6 janvier 1978 modifiée.

En effet, en utilisant une connexion « ftp », elle n'a pas veillé à ce que les transferts des données collectées par ses prestataires s'opèrent de manière sécurisée, ce qui pourtant relève de mesures élémentaires afin de garantir la sécurité des données et empêcher que des tiers non autorisés y aient accès.

Concernant les mots de passe, la formation restreinte considère que lorsqu'aucune mesure complémentaire n'est mise en œuvre, la sécurité du système d'information repose exclusivement sur la complexité des mots de passe. Or, en l'espèce, le mot de passe choisi pour accéder [redacted] est insuffisamment robuste pour garantir la sécurité du système d'information. Par ailleurs, la société n'a pas veillé à la mise en œuvre d'une gestion des habilitations et des droits d'accès, mesure de sécurité pourtant basique afin de se prémunir contre une intrusion malveillante dans le système d'information. [redacted]

La formation restreinte considère enfin que, si des correctifs ont finalement été mis en place par la société, force est de constater que cette mise en conformité ne découle que de l'initiation d'une procédure de sanction.

### 6. Sur le manquement à l'obligation d'assurer la sécurité et la confidentialité des données gérées par un sous-traitant

L'article 35 de la loi du 6 janvier 1978 modifiée 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. »*

La délégation de contrôle a été informée par la société PROFILS SENIORS qu'elle n'avait conclu aucun contrat avec son sous-traitant, la société [redacted], chargée de collecter des données à caractère personnel en son nom. De plus, il a été constaté que le contrat conclu par la société PROFILS SENIORS avec son sous-traitant, la société [redacted] qui héberge notamment sa base de données, ne comporte aucune clause spécifique dédiée à la sécurité et la confidentialité des données à caractère personnel collectées.

En défense, la société ne conteste pas l'absence de contrat conclu avec la société [redacted]. Concernant le contrat relatif à la société [redacted], elle fait valoir qu'il comporte plusieurs clauses dédiées à la sécurité et que, n'étant pas un professionnel de l'informatique, elle a pu légitimement croire que les données hébergées par son sous-traitant

étaient suffisamment sécurisées. Elle reconnaît toutefois que ces clauses peuvent être considérées comme insuffisantes en matière de sécurité et indique avoir apporté des correctifs depuis.

La formation restreinte constate que le contrat liant la société à son prestataire [redacted] ne comporte aucune indication des obligations incombant au sous-traitant en matière de protection de la sécurité et de la confidentialité des données, ni aucune mention relative au fait que le sous-traitant ne peut agir que sur instruction du responsable du traitement. Elle relève en outre l'absence de contrat avec son prestataire [redacted] prévoyant de telles obligations. La formation restreinte considère donc que la société a manqué à ses obligations résultant de l'article 35 de la loi du 6 janvier 1978 modifiée.

Par ailleurs, la formation restreinte prend acte des actions correctives entreprises par la société pour se conformer aux dispositions de la loi du 6 janvier 1978 modifiée mais considère que cette circonstance est sans incidence sur la caractérisation du manquement. En outre, elle relève que le manquement persiste au jour de l'audience, les contrats et avenants conclus avec les prestataires respectifs de la société n'ayant pas été signés par elle, ce qui ne leur confère aucune existence légale.

### 7. Sur la sanction et la publicité

Les manquements commis par la société PROFILS SENIORS justifient que soit prononcé à son encontre un avertissement.

Compte tenu des circonstances de l'espèce, la formation restreinte décide de rendre publique sa décision.

## PAR CES MOTIFS

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

- **De prononcer un avertissement à l'encontre de la société PROFILS SENIORS ;**
  **De rendre publique sa délibération.**

Le Président

Jean-François CARREZ

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