

Date de publication sur legifrance: 12/09/2013

Commission Nationale de l'Informatique et des Libertés

DELIBERATION n°2013-213 du 11 juillet 2013

Délibération n° 2013-213 du 11 juillet 2013 portant création d'une norme simplifiée concernant les traitements automatisés de données à caractère personnel relatifs à la gestion commerciale de clients et de prospects mis en œuvre par les organismes d'assurance, de capitalisation, de réassurance, d'assistance et par les intermédiaires d'assurance (norme simplifiée n° 56).

La Commission nationale de l'informatique et des libertés,

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 n° 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 son article 24 ;

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

Vu la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique ;

Vu l'ordonnance n° 2011-1012 du 24 août 2011 relative aux communications électroniques ;

Vu le code de la consommation, et notamment ses articles L. 121-20-5 et L. 134-2 ;

Vu le code des postes et des communications électroniques, et notamment son article L. 34-5 ;

Vu le code rural ;

Après avoir entendu Monsieur Jean-Paul AMOUDRY commissaire, en son rapport, et Monsieur Jean-Alexandre SILVY commissaire du Gouvernement, en ses observations,

Formule les observations suivantes :

En vertu de l'article 24 de la loi du 6 janvier 1978 modifiée, la Commission nationale de l'informatique et des libertés est habilitée à établir des normes destinées à simplifier l'obligation de déclaration des traitements les plus courants et dont la mise en œuvre n'est pas susceptible de porter atteinte à la vie privée ou aux libertés.

Les traitements informatisés relatifs à la gestion commerciale de clients et de prospects sont de ceux qui peuvent, à condition de respecter les garanties mentionnées ci après, relever de cette définition.

Cette norme permet aux responsables des traitements mis en œuvre par les organismes d'assurance, de capitalisation, de réassurance, d'assistance et par les intermédiaires d'assurances d'effectuer une déclaration simplifiée, dans les conditions qu'elle précise, pour les traitements relatifs à la gestion commerciale de clients et de prospects.

La norme simplifiée n° 56 a été adoptée le 11 juillet 2013.

Décide :

Article 1

Peuvent bénéficier de la procédure de déclaration simplifiée de conformité à la présente norme tout traitement automatisé relatif à la gestion commerciale de clients et de prospects mis en œuvre par les organismes d'assurance, de capitalisation, de réassurance, d'assistance et par les intermédiaires d'assurance et qui répond aux conditions suivantes.

Article 2 Finalités des traitements.

Le traitement peut avoir tout ou partie des finalités suivantes :

- effectuer les opérations relatives à la gestion des clients concernant :
 - un programme de fidélité au sein d'une entité ou plusieurs entités juridiques ;
 - le suivi de la relation client tel que la réalisation d'enquêtes de satisfaction, ou le regroupement des contrats pour un même client au sein de l'entreprise ou du groupe auquel appartient l'entreprise.
- effectuer des opérations relatives à la prospection :
 - la gestion d'opérations techniques de prospection (ce qui inclut notamment les opérations techniques comme la normalisation, l'enrichissement et la déduplication) ;
 - la sélection de personnes pour réaliser des actions de fidélisation, de prospection, de sondage, de test produit ou services et de promotion. Ces opérations ne doivent pas conduire à l'établissement de profils susceptibles de faire apparaître des données sensibles;
 - la réalisation d'opérations de sollicitations.
- l'élaboration de statistiques commerciales ;
- la cession, la location ou l'échange des données relatives à l'identification des clients ou prospects pour améliorer le service au client en proposant des produits ou services permettant de réduire la sinistralité ou d'offrir un contrat ou une prestation complémentaire;
- l'organisation de jeux-concours, de loteries ou de toute opération promotionnelle à l'exclusion des jeux d'argent et de hasard en ligne soumis à l'agrément de l'Autorité de régulation des jeux en ligne ;
- la gestion des demandes de droit d'accès, de rectification et d'opposition ;
- la gestion des avis des personnes sur des produits, services ou contenus.

Article 3 Les données traitées.

Les données susceptibles d'être traitées pour la réalisation des finalités décrites à l'article 2 doivent relever seulement des catégories suivantes, pour autant qu'elles soient nécessaires au respect des finalités du traitement et à l'exclusion des données de santé :

- a) Les données relatives à l'identification des personnes : identité : civilité, nom, prénoms, adresse, numéro de téléphone (fixe et/ou mobile), numéro de télécopie, adresses de courrier électronique, date de naissance, code interne de traitement permettant l'identification du client ou du prospect (ce code interne de traitement ne peut être le numéro d'inscription au répertoire national d'identification des personnes physiques (numéro de sécurité sociale), ni le numéro de carte bancaire, ni le numéro d'un titre d'identité). Une copie d'un titre d'identité peut être conservée aux fins de preuve de l'exercice d'un droit d'accès, de rectification ou d'opposition ou pour répondre à une obligation légale ;
- b) La situation familiale, économique, patrimoniale et financière et habitudes de vie en lien avec la relation commerciale : vie maritale, nombre de personnes composant le foyer, nombre et âge du ou des enfant(s) au foyer, profession, domaine d'activité présence d'animaux domestiques, loisirs.
- c) Les données relatives aux activités professionnelles et non professionnelles ayant un lien avec la relation commerciale
- d) Les données relatives au suivi de la relation commerciale : demandes de documentation ou de renseignements, demandes relatives aux produits, services ou abonnements proposés, montants, périodicité, adresses, les données relatives aux produits, contrats et services, origine de la vente (entité ou intermédiaire, vendeur, représentant, partenaire, affilié) ou de la demande, correspondances avec le client et service client, échanges et commentaires des clients et prospects, personne(s) en charge de la relation client, remises consenties ou avantages client.
- e) Les données de localisation et de connexion
- f) Les données relatives à la sélection de personnes pour réaliser des actions de fidélisation, de prospection, de sondage, de test produits et services et de promotion ;
- g) Les données relatives à l'organisation et au traitement des jeux-concours, de loteries et de toute opération promotionnelle telles que la date de participation, les réponses apportées aux jeux-concours, la photographie ou l'image de la personne, et la nature des lots offerts ;
- h) Les données relatives aux contributions des personnes qui déposent des avis sur des produits, services ou contenus, notamment leur pseudonyme.

Article 4 Les destinataires et les personnes habilitées à traiter les données :

Peuvent, dans les limites de leurs attributions respectives, avoir accès aux données à caractère personnel :

- les personnes chargées du service marketing, du service commercial, des services chargés de traiter la relation client, les réclamations, et la prospection, des services administratifs, des services logistiques et informatiques ainsi que leurs responsables hiérarchiques ;
- les services chargés du contrôle (commissaire aux comptes, services chargés des procédures internes du contrôle,...) ;
- les sous-traitants dès lors que le contrat signé entre les sous-traitants et le responsable du

traitement fait mention des obligations incombant aux sous-traitants en matière de protection de la sécurité et de la confidentialité des données (art. 35 de la loi du 6 janvier 1978 modifiée).

Peuvent être destinataires des données :

- les partenaires, les sociétés extérieures ou les entités du groupe de sociétés dans les conditions prévues par l'article 6 de la présente norme ;
- les auxiliaires de justices, les officiers ministériels et organismes publics habilités à les recevoir, les arbitres, les médiateurs.

Article 5 : Durées de conservation.

Concernant les données relatives à la gestion de clients et de prospects :

Les données à caractère personnel relatives aux clients ne peuvent être conservées au-delà de la durée strictement nécessaire à la gestion de la relation commerciale.

Toutefois, les données permettant d'établir la preuve d'un droit ou d'un contrat, ou conservées au titre du respect d'une obligation légale, peuvent être archivées conformément aux dispositions en vigueur (code des assurances, code de la mutualité, code de commerce, code civil, code de la sécurité sociale et code de la consommation).

Les données des clients utilisées à des fins de prospection commerciale peuvent être conservées pendant un délai de trois ans à compter de la fin de la relation commerciale (c'est-à-dire par exemple à compter de la date d'expiration d'un contrat, du dernier contact émanant du client).

Les données à caractère personnel relatives à un prospect non client peuvent être conservées pendant un délai de trois ans à compter de leur collecte par le responsable de traitement ou du dernier contact émanant du prospect (demande de renseignements ou de documentation, par exemple).

Au terme de ce délai de trois ans, le responsable de traitement pourra reprendre contact avec la personne concernée afin de savoir si elle souhaite continuer à recevoir des sollicitations commerciales. En l'absence de réponse positive et explicite de la personne, les données devront être supprimées ou archivées conformément aux dispositions en vigueur, et notamment celles prévues par le code de commerce, le code civil et le code de la consommation.

Concernant les pièces d'identité :

En cas d'exercice du droit d'accès ou de rectification, les données relatives aux pièces d'identité peuvent être conservées pendant le délai prévu à l'article 9 du code de procédure pénale (soit un an). En cas d'exercice du droit d'opposition, ces données peuvent être archivées pendant le délai de prescription prévu à l'article 8 du code de procédure pénale (soit trois ans).

Concernant la gestion des listes d'opposition à recevoir de la prospection :

Lorsqu'une personne exerce son droit d'opposition à recevoir de la prospection auprès d'un responsable de traitement, les informations permettant de prendre en compte son droit d'opposition doivent être conservées au minimum trois ans à compter de l'exercice du droit d'opposition. Ces données ne peuvent en aucun cas être utilisées à d'autres fins que la gestion du droit d'opposition.

Concernant les statistiques de mesure d'audience :

Au sujet des statistiques de mesure d'audience, les informations stockées dans le terminal des utilisateurs (exemple : cookies) ou tout autre élément utilisé pour identifier les utilisateurs et permettant la traçabilité des utilisateurs ne doivent pas être conservés au-delà de six mois. Les nouvelles visites ne doivent pas prolonger la durée de vie de ces informations. Les données de fréquentation brutes associant un identifiant ne doivent pas être conservées plus de six mois. Au-delà de ce délai, les données doivent être soit supprimées, soit anonymisées.

Article 6 L'information, le consentement et l'exercice du droit d'opposition des personnes.

Au moment de la collecte des données, la personne concernée est informée de l'identité du responsable du traitement, des finalités du traitement, du caractère obligatoire ou facultatif des réponses à apporter, des conséquences éventuelles, à leur égard, d'un défaut de réponse, des destinataires des données, de l'existence et des modalités d'exercice de ses droits d'accès, de rectification et d'opposition au traitement de ses données.

Il doit également être prévu :

- Le recueil du consentement exprès et spécifique de la personne concernée, dans les cas suivants :
 - la prospection réalisée au moyen d'un mode de communication électronique (courrier électronique, SMS ou MMS) hors produits ou services analogues ;
 - la prospection réalisée au moyen d'automates d'appel ou de télécopieurs ;
 - la mise à disposition ou la cession à des partenaires des adresses électroniques ou des numéros de téléphone utilisés à des fins de prospection par automate d'appel, télécopie ou par envoi de SMS, MMS ;
 - la collecte ou la cession des données susceptibles de faire apparaître directement ou indirectement les origines raciales ou ethniques, les opinions politiques, philosophiques ou religieuses ou l'appartenance syndicale des personnes ;
 - la collecte de la photographie ou de l'image de la personne.
- La possibilité de permettre à la personne concernée de s'opposer de manière simple et dénuée d'ambiguïté, dans les cas suivants :
 - la prospection par voie postale ou téléphonique avec intervention humaine ;
 - la prospection réalisée au moyen d'un mode de communication électronique pour un produit ou service analogue ;
 - la prospection entre professionnels (sauf en cas d'utilisation d'une adresse générique) lorsque l'objet du message est en rapport avec l'activité du professionnel ;
 - la cession d'adresse postale et de numéros de téléphone utilisés à des fins de prospection avec intervention humaine ;
 - la cession à des partenaires de données relatives à l'identité (à l'exclusion du code interne de

traitement permettant l'identification du client) ainsi que les informations relatives à la situation familiale, économique et financière visées à l'article 3 (d), dès lors que les organismes destinataires s'engagent à ne les exploiter que pour s'adresser directement aux intéressés, pour des finalités exclusivement commerciales.

Le consentement visé au a) est une manifestation de volonté libre, spécifique et informée par laquelle une personne accepte que des données à caractère personnel la concernant soient utilisées pour certaines finalités. L'acceptation des conditions générales d'utilisation n'est donc pas une modalité suffisante du recueil du consentement des personnes.

La participation à un jeu-concours ou une loterie ne peut être conditionnée à la réception de prospection directe au moyen d'un automate d'appel, d'un télécopieur ou d'un courrier électronique de la part du responsable de traitement ou de ses partenaires.

Dans le cas d'une collecte via un formulaire, le droit d'opposition ou le recueil du consentement préalable doit pouvoir s'exprimer par un moyen simple et spécifique, tel qu'une case à cocher. Les mentions d'information et les modes d'expression de l'opposition ou du recueil du consentement doivent être lisibles, en langage clair et figurer sur les formulaires de collecte.

Lorsque la collecte des données intervient par voie orale, l'intéressé est mis en mesure d'exercer son droit d'opposition ou de donner son consentement avant la collecte de ses données.

Après la collecte des données :

- la personne concernée a le droit de s'opposer, sans frais, à ce que ses données soient utilisées à des fins de prospection, notamment commerciale, par le responsable actuel du traitement ou celui d'un traitement ultérieur ;
- les messages adressés à des fins de prospection directe, au moyen d'automates d'appel, télécopieurs et courriers électroniques, doivent mentionner des coordonnées permettant de demander à ne plus recevoir de telles sollicitations.

Le responsable du traitement auprès duquel le droit d'opposition a été exercé informe sans délai de cette opposition tout autre responsable de traitement qu'il a rendu destinataire des données à caractère personnel qui font l'objet de l'opposition.

Article 7 L'utilisation d'un service de communication au public en ligne (site internet).

La présente norme s'applique également dans le cas où le responsable de traitement utilise un service de communication au public en ligne pour réaliser les finalités définies à l'article 2.

Des données de connexion (date, heure, adresse internet, protocole de l'ordinateur du visiteur, page consultée) pourront être exploitées à des fins de mesure d'audience et d'assistance technique. Dans ce cas, le consentement préalable des personnes n'est pas nécessaire, à condition qu'ils disposent d'une information claire et complète délivrée par l'éditeur du site internet, d'un droit d'opposition, d'un droit d'accès aux données collectées et qu'elles ne soient pas recoupées avec d'autres traitements tels que les fichiers clients.

L'information relative à la finalité et aux droits des personnes peut être présente dans les courriers électroniques envoyés, sur la page d'accueil du site, et dans ses conditions générales d'utilisation, par exemple.

Concernant l'exercice du droit d'opposition à l'analyse de sa navigation, l'outil permettant de désactiver la traçabilité mise en œuvre par l'outil d'analyse de fréquentation doit remplir les conditions suivantes :

- un accès et une installation aisés pour tous les internautes sur l'ensemble des terminaux, des systèmes d'exploitation et des navigateurs internet ;
- aucune information relative aux internautes ayant décidé d'exercer leur droit d'opposition ne doit être transmise à l'éditeur de l'outil d'analyse de fréquentation.

Par ailleurs, tout utilisateur d'un service de communications électroniques doit être informé de manière claire et complète, sauf s'il l'a été au préalable, par le responsable du traitement ou son représentant :

- de la finalité de toute action tendant à accéder, par voie de transmission électronique, à des informations déjà stockées dans son équipement terminal de communications électroniques, ou à inscrire des informations dans cet équipement ;
- des moyens dont il dispose pour s'y opposer.

Ces accès ou inscriptions ne peuvent avoir lieu qu'à condition que la personne utilisatrice ait exprimé, après avoir reçu cette information, son accord qui peut résulter de paramètres appropriés de son dispositif de connexion ou de tout autre dispositif placé sous son contrôle.

Ces dispositions ne sont pas applicables si l'accès aux informations stockées dans l'équipement terminal de l'utilisateur ou l'inscription d'informations dans l'équipement terminal de l'utilisateur :

- soit a pour finalité exclusive de permettre ou faciliter la communication par voie électronique ;
- soit est strictement nécessaire à la fourniture d'un service de communication en ligne à la demande expresse de l'utilisateur.

Article 8 Mesures de sécurité.

Le responsable du traitement prend toutes précautions utiles pour préserver la sécurité des données visées à l'article 3, et notamment empêcher qu'elles soient déformées ou endommagées ou que des tiers non autorisés y aient accès.

En particulier, les accès aux traitements de données doivent nécessiter une authentification des personnes accédant aux données, au moyen par exemple d'un code d'accès et d'un mot de passe individuels, suffisamment robustes et régulièrement renouvelés, ou par tout autre moyen d'authentification.

Les conditions d'administration du système d'information prévoient l'existence de systèmes automatiques de traçabilité (journaux, audits...).

Dans le cas de l'utilisation d'un service de communication au public en ligne, le responsable de traitement prend les mesures nécessaires pour se prémunir contre toute atteinte à la confidentialité des données traitées. Les données transitant sur des canaux de communication non sécurisés doivent notamment faire l'objet de mesures techniques visant à rendre ces données incompréhensibles à toute personne non autorisée.

Concernant les pièces d'identité, celles-ci ne doivent être accessibles qu'à un nombre de personnes restreint et des mesures de sécurité doivent être mises en œuvre afin d'empêcher toute réutilisation détournée de ces données.

Article 9 Transfert de données vers l'étranger.

La présente norme simplifiée couvre les transferts de données mentionnées à l'article 3 et collectées pour les finalités énumérées à l'article 2, lorsqu'une des conditions suivantes est réunie :

- les transferts s'effectuent à destination d'un pays reconnu par la Commission européenne comme assurant un niveau de protection adéquat ou d'une entreprise américaine ayant adhéré au Safe Harbor ;
- ils sont encadrés par les clauses contractuelles types de la Commission européenne ou par des règles internes d'entreprise (BCR - Binding Corporate Rules) dont la CNIL a préalablement reconnu qu'elles garantissent un niveau de protection suffisant de la vie privée et des droits fondamentaux des personnes ;
- ils correspondent à l'une des exceptions prévues à l'article 69 de la loi du 6 janvier 1978 modifiée, dont le champ d'application est limité à des cas de transferts ponctuels et exceptionnels.

Ainsi les transferts répétitifs, massifs ou structurels de données personnelles ne sont pas couverts par la présente norme et ils doivent faire l'objet de formalités préalables auprès de la CNIL dans les conditions prévues par ladite loi.

Seules peuvent être transférées les données pertinentes au regard de la finalité poursuivie par le transfert.

Article 10 Exclusion du bénéfice de la norme simplifiée.

Tout traitement non conforme aux dispositions de la présente délibération devra faire l'objet d'une déclaration normale auprès de la CNIL ou d'une inscription à la liste des traitements établie par le correspondant à la protection des données à caractère personnel.

Article 11.

La présente délibération sera publiée au Journal officiel de la République française.

La Présidente

Isabelle FALQUE-PIERROTIN

Nature de la délibération: Norme simplifiée