Commission nationale de l'informatique et des libertés

Délibération nº 2012-209 du 21 juin 2012 portant création d'une norme simplifiée concernant les traitements automatisés de données à caractère personnel relatifs à la gestion de clients et de prospects (norme simplifiée nº 48)

NOR : *CNIA1200016X*

La Commission nationale de l'informatique et des libertés,

Vu la convention nº 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 nº 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 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 la loi nº 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés, notamment son article 24 ;

Vu la loi nº 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique ;

Vu l'ordonnance nº 2011-1012 du 24 août 2011 relative aux communications électroniques ;

Vu le décret nº 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 délibération nº 2005-112 du 7 juin 2005 portant création d'une norme simplifiée concernant les traitements automatisés de données à caractère personnel relatifs à la gestion des fichiers de clients et de prospects et portant abrogation des normes simplifiées 11, 17 et 25 ;

Après avoir entendu M. Bernard Peyrat, commissaire, en son rapport, et Mme Elisabeth Rolin, 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 de clients et de prospects sont de ceux qui peuvent, sous certaines conditions, relever de cette définition.

Cette norme permet aux responsables de traitement d'effectuer une déclaration simplifiée, dans les conditions qu'elle précise, pour les traitements relatifs à la gestion de clients et de prospects, à l'exclusion de ceux mis en œuvre par les établissements bancaires ou assimilés, les entreprises d'assurances, de santé et d'éducation.

La norme simplifiée nº 48 en vigueur a été adoptée le 7 juin 2005. Compte tenu de l'évolution du commerce et des méthodes de prospection, il est apparu nécessaire de la compléter.

Décide :

Art. 1er. – Peut bénéficier de la procédure de la déclaration simplifiée de conformité à la présente norme tout traitement automatisé relatif à la gestion de clients et de prospects qui répond aux conditions suivantes.

Art. 2. – *Les finalités des traitements.*

Le traitement peut avoir tout ou partie des finalités suivantes :

– effectuer les opérations relatives à la gestion des clients concernant :
  – les contrats ;
  – les commandes ;
  – les livraisons ;
  – les factures ;
  – la comptabilité et en particulier la gestion des comptes clients ;
  – 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, la gestion des réclamations et du service après-vente ;
– 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 et de promotion. Sauf consentement des personnes concernées recueilli dans les conditions prévues à l'article 6, ces opérations ne doivent pas conduire à l'établissement de profils susceptibles de faire apparaître des données sensibles (origines raciales ou ethniques, opinions philosophiques, politiques, syndicales, religieuses, vie sexuelle ou santé des personnes) ;
- la réalisation d'opérations de sollicitations ;

– l'élaboration de statistiques commerciales ;
– la cession, la location ou l'échange de ses fichiers de clients et de ses fichiers de prospects ;
– 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 impayés et du contentieux, à condition qu'elle ne porte pas sur des infractions et/ou qu'elle n'entraîne pas une exclusion de la personne du bénéfice d'un droit, d'une prestation ou d'un contrat ;
– la gestion des avis des personnes sur des produits, services ou contenus.

Art. 3. – *Les données traitées.*

Les données susceptibles d'être traitées pour la réalisation des finalités décrites à l'article 2 sont :

a) L'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 (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) Les données relatives aux moyens de paiement : relevé d'identité postale ou bancaire, numéro de chèque, numéro de carte bancaire, date de fin de validité de la carte bancaire ;

c) Les données relatives à la transaction telles que le numéro de la transaction, le détail de l'achat, de l'abonnement, du bien ou du service souscrit ;

d) La situation familiale, économique et financière : vie maritale, nombre de personnes composant le foyer, nombre et âge du ou des enfant(s) au foyer, profession, domaine d'activité, catégorie socioprofessionnelle, présence d'animaux domestiques ;

e) Les données relatives au suivi de la relation commerciale : demandes de documentation, demandes d'essai, produit acheté, service ou abonnement souscrit, quantité, montant, périodicité, adresse de livraison, historique des achats et des prestations de services, retour des produits, origine de la vente (vendeur, représentant, partenaire, affilié) ou de la commande, correspondances avec le client et service après-vente, échanges et commentaires des clients et prospects, personne(s) en charge de la relation client ;

f) Les données relatives aux règlements des factures : modalités de règlement, remises consenties, reçus, soldes et impayés n'entraînant pas une exclusion de la personne du bénéfice d'un droit, d'une prestation ou d'un contrat soumis à autorisation de la commission telle que prévue par les dispositions de l'article 25-I (4°) de la loi du 6 janvier 1978 modifiée. Les informations relatives aux crédits souscrits (montant et durée, nom de l'organisme prêteur) peuvent également être traitées par le commerçant en cas de financement de la commande par crédit ;

g) Les données relatives à la sélection de personnes pour réaliser des actions de fidélisation, de prospection, de sondage, de test produit et de promotion ;

h) 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 et la nature des lots offerts ;

i) Les données relatives aux contributions des personnes qui déposent des avis sur des produits, services ou contenus, notamment leur pseudonyme.

Art. 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 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) et précise notamment les objectifs de sécurité devant être atteints.

Peuvent être destinataires des données :

– les partenaires, les sociétés extérieures ou les filiales d'un même groupe de sociétés dans les conditions prévues par l'article 6 de la présente norme ;
– les organismes, les auxiliaires de justice et les officiers ministériels, dans le cadre de leur mission de recouvrement de créances.

Art. 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 (notamment celles prévues par le code de commerce, le code civil et le code de la consommation).

Par ailleurs et sous réserve du respect de l'article 6 de la présente norme, 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 d'un achat, de la date d'expiration d'une garantie, du terme d'un contrat de prestations de services ou 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 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 les données relatives aux cartes bancaires :

Les données relatives aux cartes bancaires doivent être supprimées une fois la transaction réalisée, c'est-à-dire dès son paiement effectif. Dans le cas d'un paiement par carte bancaire, elles peuvent être conservées pour une finalité de preuve en cas d'éventuelle contestation de la transaction, en archives intermédiaires, pour la durée prévue par l'article L. 133-24 du code monétaire et financier, en l'occurrence treize mois suivant la date de débit. Ce délai peut être étendu à quinze mois afin de prendre en compte la possibilité d'utilisation de cartes de paiement à débit différé.

Ces données peuvent être conservées plus longtemps sous réserve d'obtenir le consentement exprès du client, préalablement informé de l'objectif poursuivi (faciliter le paiement des clients réguliers, par exemple). Ce consentement peut être recueilli par l'intermédiaire d'une case à cocher (non précochée par défaut), par exemple, et ne peut résulter de l'acceptation de conditions générales.

Les données relatives au cryptogramme visuel ne doivent pas être stockées.

Lorsque la date d'expiration de la carte bancaire est atteinte, les données relatives à celles-ci doivent être supprimées.

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.

Art. 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 :

a) 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 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 ou qui sont relatives à la vie sexuelle de celle-ci (par exemple, eu égard au type de documentation demandé, à la nature du produit acheté, du service ou de l'abonnement souscrit).

b) 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.

Art. 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. 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 abonné ou 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 l'abonné ou 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.

Art. 8. – *Sécurités.*

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.

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.

Les accès aux données relatives aux moyens de paiement doivent faire l'objet de mesures de traçabilité permettant de détecter *a posteriori* tout accès illégitime aux données et de l'imputer à la personne ayant accédé illégitimement à ces données.

Lorsqu'un moyen de paiement à distance est utilisé, le responsable de traitement doit prendre les mesures organisationnelles et techniques appropriées afin de préserver la sécurité, l'intégrité et la confidentialité des numéros de cartes bancaires contre tout accès, utilisation, détournement, communication ou modification non autorisés en recourant à des systèmes de paiement sécurisés conformes à l'état de l'art et à la réglementation applicable. Ces données doivent être notamment chiffrées par l'intermédiaire d'un algorithme réputé « fort ».

Lorsque le responsable de traitement conserve les numéros de carte bancaire pour une finalité de preuve en cas d'éventuelle contestation de la transaction, ces numéros doivent faire l'objet de mesures techniques visant à prévenir toute réutilisation illégitime, ou toute réidentification des personnes concernées. Ces mesures peuvent notamment consister à stocker les numéros de carte bancaire sous forme hachée avec utilisation d'une clé secrète.

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 (apposition d'un marquage spécifique, par exemple).

Art. 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.

Art. 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.

Les traitements susceptibles d'exclure des personnes du bénéfice d'un droit, d'une prestation ou d'un contrat, notamment ceux ayant pour finalité l'évaluation du risque présenté par une commande ou un client, doivent faire l'objet d'une demande d'autorisation auprès de la CNIL.

Les dispositions de la présente norme ne sont pas applicables aux secteurs d'activités suivants : établissements bancaires ou assimilés, entreprises d'assurances, de santé ou d'éducation.

Art. 11. – Les organismes privés et publics ayant effectué une déclaration simplifiée en référence à la norme simplifiée n° 48 et qui ne respectent pas les conditions fixées par la présente norme disposent d'un délai de douze mois à compter de la publication de la présente délibération pour mettre leur traitement en conformité.

La délibération n° 2005-112 du 7 juin 2005 portant création d'une norme simplifiée concernant les traitements automatisés de données à caractère personnel relatifs à la gestion des fichiers de clients et de prospects et portant abrogation des normes simplifiées 11, 17 et 25 est abrogée.

Art. 12. – La présente délibération sera publiée au *Journal officiel* de la République française.

Fait le 21 juin 2012.

La présidente,
I. Falque-Pierrotin