CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

NS 48

Fichiers clients-prospects et vente en ligne

Suite à l'entrée en application du RGPD, les normes adoptées par la CNIL n'ont plus de valeur juridique depuis le 25 mai 2018.

Dans l'attente de la production de référentiels RGPD, les responsables de traitement peuvent s'en inspirer pour orienter leurs premières actions de conformité.

La CNIL attire toutefois l'attention sur la nécessité de veiller au respect des nouvelles règles.

Fichiers clients-prospects et vente en ligne

(Déclaration N° 48)

Suite à l'entrée en application du RGPD, les normes simplifiées adoptées par la CNIL n'ont plus de valeur juridique à compter du 25 mai 2018. Dans l'attente de la production de référentiels RGPD, la CNIL a décidé de les maintenir accessibles afin de permettre aux responsables de traitement d'orienter leurs premières actions de mise en conformité.

La norme simplifiée n° NS-048 concerne les traitements automatisés de données à caractère personnel relatifs à la gestion de clients et de prospects. Elle inclut notamment les traitements de données personnelles ayant pour finalités la gestion des clients, la prospection, les opérations de fidélisation, l'élaboration de statistiques commerciales, la cession, la location ou l'échange de fichiers de clients et de prospects, l'organisation de jeux concours, de loteries ou de toute opération promotionnelle, la gestion des demandes de droit d'accès, de rectification et d'opposition, la gestion des impayés et du contentieux, et la gestion des avis des personnes sur des produits, services ou contenus.

La norme simplifiée n° NS-048 a été adoptée en 2005 et modifiée en 2012. Avec la mise en œuvre de la liste d'opposition au démarchage téléphonique, prévue par le code de la consommation, une actualisation de la norme était nécessaire, notamment pour que les professionnels n'aient pas à effectuer de formalité supplémentaire pour envoyer leurs fichiers de prospection à l'organisme en charge de la gestion de la liste d'opposition. La norme simplifiée a ainsi été modifiée en juillet 2016. A cette occasion, d'autres modifications et précisions ont été apportées à la norme, principalement sur les thématiques des cookies, des données bancaires et des durées de conservation des données.
Sont exclus du champ de cette norme les traitements mis en œuvre par les établissements bancaires ou assimilés, les entreprises d'assurances, de santé et d'éducation, les traitements relatifs à l'organisation de jeux d'argent et de hasard en ligne soumis à l'agrément de l'Autorité de Régulation des Jeux en Ligne et les traitements susceptibles d'exclure des personnes au bénéfice d'un droit, d'une prestation ou d'un contrat.

TEXTE OFFICIEL

Délibération n° 2016-264 du 21 juillet 2016 portant modification d'une norme simplifiée concernant les traitements automatisés de données à caractère personnel relatifs à la gestion de clients et de prospects.

Secteurs d'activité exclus du champ de la norme

Établissements bancaires ou assimilés, entreprises d'assurances, établissements de santé, établissements d'éducation.

Responsables de traitement concernés

Organismes publics ou privés.

Objectif(s) poursuivi(s) par le traitement (finalités)

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 ; la sélection de clients pour réaliser des études, sondages et tests produits (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) ;
- **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'actualisation de ses fichiers de prospection par l'organisme en charge de la gestion de la liste d'opposition au démarchage téléphonique,** en application des dispositions du code de la consommation ;
- **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 ;
- l**a 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'entraine 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.**

Utilisation(s) exclue(s) du champ de la norme

- Traitements qui du fait de leur nature, de leur portée ou de leurs finalités, sont susceptibles d'exclure des personnes au bénéfice d'un droit, d'une prestation ou d'un contrat.

Données personnelles concernées

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, cryptogramme visuel (ce dernier ne devant pas être conservé, conformément à l'article 5) ;
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 nécessaires à la réalisation des actions de fidélisation, de prospection, d'étude, de sondage, de test produit et de promotion, la sélection des personnes ne pouvant résulter que de l'analyse des données listées à l'article 3 ;
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 ;
j) les données collectées par le biais des actions visées à l'article 32-II de la loi du 6 janvier 1978 modifiée, dans le respect des recommandations figurant dans la délibération n° 2013-378 du 5 décembre 2013.

Durée de conservation des donnees

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 faire l'objet d'une politique d'archivage intermédiaire pour une durée n'excédant pas la durée nécessaire aux finalités pour lesquelles elles sont conservées, conformément aux dispositions en vigueur (notamment mais non exclusivement celles prévues par le code de commerce, le code civil et le code de la consommation). Il convient de prévoir à cet effet une base de données d'archives dédiée ou une séparation logique dans la base de données active, après avoir opéré un tri des données pertinentes à archiver.

Pour pouvoir conserver, au-delà de la durée de conservation fixée au regard de l'article 6.5° de la loi, des informations relatives à des clients ou des prospects à des fins d'analyses ou d'élaboration de statistiques agrégées, les données doivent être anonymisées de manière irréversible, en procédant à la purge de toutes les données à caractère personnel, y compris les données indirectement identifiantes. A cet égard, le G29 a adopté un avis le 10 avril 2014 sur les techniques d'anonymisation.

Par ailleurs et sous réserve du respect de l'article 6 de la 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 (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 (par exemple, une demande de documentation ou un clic sur un lien hypertexte contenu dans un courriel ; en revanche, l'ouverture d'un courriel ne peut être considérée comme un contact émanant du prospect).

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, qui peut être différé à la réception du bien, augmenté, le cas échéant, du délai de rétractation prévu pour les contrats conclus à distance et hors établissement, conformément à l'article L. 221-18 du code de la consommation.

Dans le cas d'un paiement par carte bancaire, le numéro de la carte et la date de validité de celle-ci peuvent être conservés 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 doivent être utilisées uniquement en cas de contestation de la transaction. Les données conservées à cette fin doivent faire l'objet de mesures de sécurité, telles que décrites à l'article 8 de la présente norme et à l'article 5 de la délibération n° 2013-358 du 14 novembre 2013 susvisée.

Les données relatives aux cartes bancaires peuvent être conservées plus longtemps sous réserve d'obtenir le consentement exprès du client, préalablement informé de l'objectif poursuivi (par exemple, faciliter le paiement des clients réguliers). La durée de conservation ne saurait alors excéder la durée nécessaire à l'accomplissement de la finalité visée par le traitement. Le consentement doit prendre la forme d'un acte de volonté explicite et peut par exemple être recueilli par l'intermédiaire d'une case à cocher, non pré-cochée par défaut. Il ne peut résulter de l'acceptation de conditions générales. La Commission recommande par ailleurs que le responsable de traitement intègre directement sur son site marchand un moyen simple et gratuit de revenir sur le consentement donné pour la conservation des données de la carte, afin de faciliter les achats ultérieurs.

De manière générale, les données relatives au cryptogramme visuel ne doivent pas être conservées au-delà du temps nécessaire à la réalisation de chaque transaction, y compris en cas de paiements successifs ou de conservation du numéro de la carte pour les achats ultérieurs.

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 et seules les données nécessaires à la prise en compte du droit d'opposition doivent être conservées (par exemple, l'adresse électronique).

Concernant les statistiques de mesure d'audience :

Les informations stockées dans le terminal des utilisateurs (ex : cookies), ou tout autre élément utilisé pour identifier les utilisateurs et permettant leur traçabilité, ne doivent pas être conservés au-delà de treize 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 treize mois. Au-delà de ce délai, les données doivent être soit supprimées, soit anonymisées.

Dans la limite de leurs attributions respectives, peuvent avoir accès aux données personnelles :

- le personnel habilité 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 ;
- le personnel habilité des services chargés du contrôle (commissaire aux comptes, services chargés des procédures internes du contrôle...) ;
- le personnel habilité des 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 (article 35 de la loi du 6 janvier 1978 modifiée) et précise notamment les objectifs de sécurité devant être atteints.

Destinataires des données

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 norme ;
- les organismes, les auxiliaires de justice et les officiers ministériels, dans le cadre de leur mission de recouvrement de créances ;
- l'organisme en charge de la gestion de la liste d'opposition au démarchage téléphonique

Information des personnes et respect des droits « informatique et libertés »

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.

Lorsque les données sont recueillies par voie de questionnaires, ceux-ci doivent porter mention des prescriptions figurant aux 1°, 2°, 3° et 6° de l'article 32 de la loi du 6 janvier 1978 modifiée. Cette disposition vise les questionnaires au sens large et, notamment, les formulaires à compléter sur un site web.

Lorsque les données à caractère personnel n'ont pas été recueillies directement auprès des personnes concernées, les modalités d'information des personnes sont prévues par les dispositions de l'article 32.III de la loi.

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 des dispositifs visés par l'article L. 34-5 du code des postes et des communications électroniques (système automatisé de communications électroniques au sens de l'article
- L. 32 du CPCE – SMS, MMS, automate d'appel, Bluetooth, etc. – télécopieur et courrier électronique). Toutefois, dans les conditions visées par l'article L. 34-5 du CPCE, le recueil du consentement n'est pas requis lorsque le courrier électronique concerne des produits ou services analogues ;
- la cession à des partenaires des adresses électroniques ou des numéros de téléphone utilisés à des fins de prospection directe au moyen des dispositifs précités visés par l'article L. 34-5 du CPCE ;
- 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, au moment de la collecte de ses données (article 96 du décret du 20 octobre 2005 modifié), dans les cas suivants :

- la prospection par voie postale ou téléphonique avec intervention humaine ;
- la prospection directe réalisée au moyen d'un courrier électronique pour un produit ou service analogue, conformément aux dispositions de l'article L. 34-5 du CPCE ;
- 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.

Les consommateurs qui ne souhaitent pas faire l'objet de prospection commerciale par voie téléphonique peuvent s'inscrire gratuitement sur la liste d'opposition au démarchage téléphonique prévue par les articles L. 223-1 et suivants du code de la consommation. Il est notamment interdit à un professionnel, directement ou par l'intermédiaire d'un tiers agissant pour son compte, de démarcher téléphoniquement un consommateur inscrit sur la liste d'opposition, sauf en cas de relations contractuelles préexistantes. La location ou la vente de fichiers contenant des données téléphoniques et comportant les coordonnées d'un ou de plusieurs consommateurs inscrits sur la liste est également interdite.

Le contrôle du respect de ces obligations est assuré par les services de la Direction générale de la concurrence, de la consommation et de la répression des fraudes du ministère de l'Économie, de l'Industrie et du Numérique.

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. Une action positive et spécifique de l'utilisateur est requise (par exemple, une case à cocher dédiée, non pré-cochée).

La participation à un jeu-concours ou une loterie ne peut être conditionnée à la réception de prospection directe de la part du responsable de traitement ou de ses partenaires, de même que l'achat d'un bien, le bénéfice d'une réduction ou la fourniture d'un service.

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. Cette opposition peut intervenir à tout moment et n'a pas à être motivée ;
- les messages adressés à des fins de prospection directe, au moyen des dispositifs visés par l'article L. 34-5 du CPCE, 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.

Conformément à l'article 39 de la loi, toute personne peut demander au responsable de traitement la communication, sous une forme accessible, des données à caractère personnel la concernant ainsi que toute information quant à l'origine de celles-ci. Le droit de rectification s'exerce dans les conditions prévues à l'article 40 de la loi.

L'utilisation d'un service de communication au public en ligne (site web) :

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'elles disposent d'une information claire et complète délivrée par l'éditeur du site web, d'un droit d'opposition, d'un droit d'accès aux données collectées. Ces dernières ne doivent pas être 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 web ;
- 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.

Les cookies de mesure d'audience peuvent être déposés et lus sans recueillir le consentement des personnes lorsqu'ils remplissent les conditions visées à l'article 6 de la délibération n° 2013-378 du 5 décembre 2013, portant adoption d'une recommandation relative aux cookies et aux autres traceurs visés par l'article 32-II de la loi du 6 janvier 1978.

De manière générale, pour l'ensemble des traitements mis en œuvre pour les finalités définies à l'article 2 de la présente norme qui utilisent des données collectées par le biais des technologies visées à l'article 32-II de la loi, la présente norme renvoie aux recommandations de la délibération n° 2013-378 du 5 décembre 2013.

Lorsque l'utilisation d'un service de communication au public en ligne donne lieu à la création d'un compte par l'utilisateur, les données doivent être effacées dès que le compte est supprimé, sous réserve des exceptions listées à l'article 5 de la norme.

S'agissant des comptes n'étant plus utilisés depuis un certain laps de temps par l'utilisateur, un délai doit être fixé pour déterminer la durée à partir de laquelle ces comptes doivent être considérés comme des comptes inactifs. Au terme de ce délai, les données relatives au compte inactif doivent être supprimées. Le responsable de traitement doit avertir l'utilisateur par tous les moyens disponibles avant de procéder à cette suppression et lui donner la possibilité de manifester sa volonté contraire. Il est envisageable que la personne concernée donne son consentement spécifique pour que tout ou partie des données soient archivées par le responsable de traitement, pour une durée déterminée et raisonnable, en vue d'une réactivation future du compte.

Le laps de temps au terme duquel un compte doit être considéré comme inactif doit être défini par le responsable de traitement conformément aux dispositions de l'article 6.5° de la loi du 6 janvier 1978 modifiée. A titre indicatif, une durée de deux ans semble par exemple appropriée pour un compte créé sur un site de rencontres.

Dans tous les cas, le responsable de traitement doit ménager la possibilité pour la personne concernée d'exercer ses droits si des données à caractère personnel la concernant restent traitées indépendamment de la clôture du compte et de la suppression des données de celui-ci.

Sécurité et confidentialité

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.

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 mots de passe ne doivent pas être stockés en clair.

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 (par exemple, protocole HTTPS).

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 (notamment le

chiffrement des données 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 mesure technique visant à prévenir toute réutilisation illégitime, ou toute ré-identification des personnes concernées (stockage des numéros de carte bancaire sous forme hachée avec utilisation d'une clé secrète).

De manière générale, s'agissant de mesures de sécurité à mettre en place pour les données relatives aux cartes bancaires, la norme renvoie vers l'article 5 de la délibération n° 2013-358 du 14 novembre 2013.

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, fourniture du seul recto de la pièce d'identité et photocopie en noir et blanc par exemple).

Transferts des donnes hors de l'union européenne

La norme couvre les transferts de données mentionnées à l'article 3, collectées pour les finalités visées 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 en raison de sa législation interne ou de ses engagements internationaux, souscrits notamment à l'issue de négociations avec la Commission européenne, en vue de la protection de la vie privée et des libertés et droits fondamentaux des personnes ;
- ils sont encadrés par les clauses contractuelles types de la Commission européenne ou par des règles internes d'entreprise (BCR - Binding Corporate Rules) ou des clauses contractuelles ad hoc 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.