18 La Cnil actualise sa norme de déclaration des fichiers de clients et prospects

La Commission nationale de l'informatique et des libertés vient d'actualiser sa norme de déclaration simplifiée des traitements de données personnelles relatives à la gestion des clients et prospects, notamment pour l'adapter au commerce et à la prospection en ligne.

Délibération Cnil 2016-264 du 21-7-2016 : JO du 14-9 texte n° 52

1 Les traitements automatisés de données personnelles relatives à la gestion de clients et prospects peuvent faire l'objet d'une **déclaration simplifiée** à la Commission nationale de l'informatique et des libertés (Cnil), à condition que ces traitements respectent les prescriptions d'une norme établie par elle (Norme simplifiée n° 48 adoptée le 7-6-2005 et modifiée le 21-6-2012 : BRDA 14/12 inf. 27).
La Cnil vient d'actualiser cette norme pour tenir compte de l'évolution du commerce et des méthodes de prospection (développement de la vente en ligne avec paiement par carte bancaire, utilisation des cookies, prospection par courriers électroniques et par automates d'appels téléphoniques, etc.). Nous présentons ci-dessous les principales modifications.

> Comme auparavant, les traitements de données dans les secteurs de la banque, l'assurance, la santé et l'éducation ne peuvent pas bénéficier de la norme simplifiée.

2 Les organismes ayant effectué une déclaration simplifiée en référence à l'ancienne norme n° 48 n'ont pas à refaire de nouvelle déclaration. S'ils ne respectent pas les conditions de la nouvelle norme, ils disposent d'un an à compter du 14 septembre 2016 pour **se mettre en conformité**.

Finalités des traitements

3 A la liste des traitements qui peuvent bénéficier de la procédure de déclaration simplifiée viennent s'ajouter :
– la **sélection de clients** pour réaliser des **études, sondages et tests** produits, ces opérations ne devant toutefois pas conduire à l'établissement de profils pouvant faire apparaître des données sensibles (origines raciales ou ethniques, opinions philosophiques, politiques, syndicales, religieuses, vie sexuelle ou santé des personnes), sauf consentement des personnes concernées ;
– l'actualisation des fichiers de prospection par l'organisme en charge de la gestion de la liste d'**opposition au démarchage téléphonique** (liste Bloctel) ;
– les données collectées grâce aux **cookies et autres traceurs**.

Conservation des données

4 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. 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, pendant treize à quinze mois. Ces données doivent être utilisées uniquement en cas de contestation et faire l'objet de mesures de sécurité.
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. La Commission recommande que soit intégré directement sur le site marchand un moyen simple et gratuit de revenir sur le consentement donné.
Le **cryptogramme visuel** ne doit pas être conservé 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 des achats ultérieurs.

5 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. La norme précise désormais qu'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 normale, 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.

6 Au sujet des statistiques de **mesure d'audience des sites web**, la nouvelle norme précise que les informations stockées dans le terminal des utilisateurs (par exemple, les cookies), ou tout autre élément utilisé pour identifier les utilisateurs et permettant leur traçabilité, ne doivent pas être conservés au-delà de 13 mois, contre 6 mois dans la précédente norme. Le délai de conservation des données de fréquentation brutes associant un identifiant est également porté de 6 à 13 mois.

7 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 en principe être effacées dès que le compte est supprimé. Un délai doit être fixé pour déterminer la durée à partir de laquelle un compte dont l'utilisateur ne se sert plus doit être considéré comme un **compte inactif**. Au terme du délai, les données de ce compte doivent être supprimées. Le responsable de traitement doit avertir l'utilisateur par tous les moyens disponibles avant de supprimer le compte et lui permettre 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. A titre indicatif, une durée de deux ans semble 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 restent traitées indépendamment de la clôture du compte et de la suppression des données de celui-ci.

Consentement des prospects

8 Conformément aux dispositions du Code des postes et des communications électroniques (art. L 34-5), la nouvelle norme exige le consentement exprès des personnes concernées en cas de prospection par système automatisé de **communications électroniques** (SMS, MMS, automates d'appel, télécopieur et courrier électronique, Bluetooth, etc.), sauf lorsque le courrier électronique concerne des produits ou services analogues à ceux déjà fournis à la personne. Une action positive et spécifique de l'utilisateur est requise (par exemple, une case à cocher dédiée, non précochée).
Les cookies de mesure d'audience peuvent être déposés et lus sans le consentement des personnes.

Opposition à l'utilisation des données

9 La nouvelle norme précise que le droit pour une personne de s'opposer à l'utilisation de données la concernant à des fins de prospection doit pouvoir intervenir à tout moment et que l'opposition n'a pas à être motivée.