



La protection des données personnelles : un enjeu essentiel pour la confiance des consommateurs et la compétitivité des entreprises

Consommation



MEDEF

→→ EDITO

La satisfaction des consommateurs est une des conditions essentielles de la pérennité des entreprises. Qui pourrait imaginer en effet une entreprise sans clients ? C'est pourquoi les entreprises s'engagent au quotidien pour assurer et développer la satisfaction des consommateurs, laquelle repose sur :

- la qualité de l'offre de produits et services qui est la base de la satisfaction des consommateurs, source de valeur ajoutée et justification du prix ;
- la qualité de la relation individuelle avec les consommateurs, qu'il s'agisse de communication, de fidélisation, de gestion de leurs données personnelles, de réponse à leurs questions ou de traitement amiable des différends ;
- la qualité du dialogue avec les parties prenantes de la consommation, associations de consommateurs en premier lieu, institutions françaises et européennes, médias...

La bonne gestion des données personnelles des consommateurs est à la fois un enjeu de confiance et de compétitivité. Elle constitue également le carburant nécessaire au bon fonctionnement de l'économie numérique. L'information des consommateurs, tout comme l'exécution du contrat, font de plus en plus appel aux données communiquées par ceux-ci. Elles permettent d'établir, puis d'entretenir, le lien qui relie le client à l'entreprise. Elles offrent de plus la possibilité de renforcer la qualité de ce lien, en permettant une plus grande personnalisation de la relation client, et donc une meilleure prise en compte des attentes des consommateurs.

Si ces données sont devenues indispensables pour de nombreuses entreprises, leur transmission suppose que le consommateur ait confiance dans l'utilisation qui en sera faite, qu'il ait le sentiment qu'elles ne seront ni détournées de leur finalité ni exploitées de manière illicite ou abusive.

La très grande majorité des entreprises sont bien conscientes de leur responsabilité à l'égard des données qui leur sont confiées. D'une manière générale, le sentiment de confiance se généralise aujourd'hui chez les consommateurs comme en témoigne par exemple le développement croissant des ventes de produits et services sur internet. Pour autant, le développement des usages internet, et plus généralement celui des technologies de l'information et de la communication, multiplie les occasions de transmission de données susceptibles de susciter certaines craintes chez les consommateurs.

A ce titre, le Medef s'investit dans les travaux du Conseil National de la Consommation (CNC) sur la protection des données personnelles des consommateurs, aux côtés des pouvoirs publics et des associations de consommateurs. L'avis du CNC sur la protection des données personnelles, adopté à l'unanimité des collèges professionnels et consommateurs, témoigne de la volonté de trouver des solutions réalistes et équilibrées permettant de renforcer la confiance des consommateurs, en dehors de toute surenchère réglementaire.

Si la recommandation phare de l'avis est la mise en œuvre d'actions d'éducation, de sensibilisation et d'information des consommateurs dans le domaine de la protection des données personnelles, en particulier sur le thème essentiel de leurs droits, le pendant est la sensibilisation des entreprises. Pour répondre à cette dernière demande des parties prenantes, le MEDEF propose par ce guide pratique destiné aux organisations professionnelles et aux entreprises de toute taille et de tout secteur une grille de lecture afin d'améliorer leur information et connaissance de l'environnement législatif et des bonnes pratiques dans ce domaine.

Marc Lolivier
Président du
Groupe de projet Protection
des données personnelles des
consommateurs

Loïc Armand
Président de la
Commission Consommation

→→ SOMMAIRE

Introduction	5
La protection des données personnelles des consommateurs : quels enjeux ?	5
Quels sont les intérêts de la protection des données personnelles des consommateurs pour les entreprises ?	6
Dans quels cas les règles de protection sont-elles applicables ?	8
Les règles actuelles : les étapes à suivre pour utiliser des données personnelles de consommateurs en conformité avec la loi	10
• Etape 1 : formalités préalables auprès de la CNIL	10
• Etape 2 : les règles à suivre au moment de la collecte des données personnelles	16
• Etape 3 : quels sont les droits des consommateurs ?	23
• Etape 4 : Les règles à respecter dans le cadre de l'exploitation des données personnelles	27
Les évolutions à venir	33
Foire aux questions	36
A quelles occasions un professionnel est-il amené à collecter des données personnelles de consommateurs ?	36
Quand dois-je déclarer un fichier à la CNIL ?	36
Qu'est-ce qu'un cookie ?	37
Comment transmettre les informations requises au consommateur ?	37
Que recouvrent les droits d'accès et de rectification du consommateur ?	38
Quelles informations dois-je fournir au consommateur en cas de transfert de données personnelles hors de l'Union Européenne ?	38
Quelles sont, en synthèse, les obligations qui incombent à un professionnel en application de la loi « informatique et libertés » ?	39
Annexes	40
ANNEXE I : les principaux textes de référence	40
I.1 Textes législatifs et réglementaires	40
I.2 Travaux du Conseil National de la Consommation	41
I.3 Documents et travaux réalisés par la Commission européenne	41
ANNEXE II : les exemples de bonnes pratiques	41
ANNEXE III : les outils mis à disposition par la CNIL	42
Remerciements	43

→ → INTRODUCTION

La protection des données personnelles des consommateurs : quels enjeux ?

La protection des données personnelles constitue aujourd'hui un sujet important dans le domaine de la consommation. En effet, avec la mondialisation des échanges et l'évolution des pratiques commerciales, les enjeux liés à la protection des données personnelles des consommateurs sont devenus incontestables.

Ainsi, du fait de l'accroissement des échanges entre professionnels et consommateurs, la collecte et l'exploitation de données personnelles par les professionnels constitue pour eux un élément d'appréciation d'une grande utilité, voire une nécessité ou une obligation réglementaire dans certains cas, permettant notamment de mieux appréhender les besoins des clients et d'améliorer leurs offres (exemple : développement du service après-vente).

Par ailleurs, le développement des nouvelles technologies de l'information et de la communication (internet en particulier) a rendu plus facile la transmission des données personnelles des consommateurs, notamment dans le cadre du fort développement du commerce électronique, qui rend inévitable la transmission de telles données. De plus, les progrès techniques sur le plan du stockage ont abouti à des possibilités de rassemblement très importantes de données par les professionnels. Cependant, certains consommateurs n'ont pas forcément conscience des conséquences que peut avoir la communication de leurs données personnelles à des professionnels, du fait du détournement d'utilisation qui pourrait en être fait.

Si d'une manière générale, l'utilisation des données personnelles des consommateurs contribue au progrès économique, elle peut également amener les entreprises à s'interroger sur les modalités de cette utilisation en particulier au regard des règles de protection de la vie privée des consommateurs et de leurs données personnelles. Ce vademecum a pour objectif de répondre à ces interrogations.

Qu'est-ce qu'une donnée personnelle ?

Selon l'article 2 de la loi 78-17 modifiée du 6 janvier 1978, constitue une donnée à caractère personnel toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres. Il peut s'agir d'un nom, prénom, date de naissance, adresse postale, adresse e-mail, numéro de téléphone, numéro de carte de paiement, empreinte digitale, photo, numéro de sécurité sociale...

En outre, les données à caractère personnel qui font 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 santé ou à la vie sexuelle de celles-ci sont considérées comme des données sensibles dont la collecte est soit interdite soit soumise à des exigences particulières.

Quels sont les intérêts de la protection des données personnelles des consommateurs pour les entreprises ?

Si les règles de protection des données personnelles ont ainsi un intérêt évident pour les consommateurs, leur respect constitue également un élément important pour les entreprises dans leur relation avec les clients.

La diffusion de données personnelles peut exposer les consommateurs à des risques. Or, les comportements abusifs de certaines entreprises ont des répercussions néfastes sur l'ensemble des professionnels ayant recours à des technologies modernes, en entraînant la méfiance des consommateurs. Par conséquent, pour renforcer la confiance des consommateurs, les entreprises ont tout intérêt à mettre en œuvre des bonnes pratiques dans ce domaine, ce qui contribue à améliorer leur image. Cela permettra notamment de s'assurer que la gestion des données personnelles ne devienne pas un frein au développement de l'activité commerciale des entreprises, notamment du commerce électronique, qui est aujourd'hui un canal de vente performant pour de nombreuses entreprises.

De plus, la mise en œuvre de bonnes pratiques peut permettre aux professionnels d'améliorer la qualité de leur relation client. Par exemple, concernant l'utilisation des données personnelles des consommateurs à des fins de prospection commerciale, il pourrait être tentant pour les entreprises d'utiliser tous les nouveaux



moyens à leur disposition pour assurer le plus largement possible la connaissance de leurs produits, et d'exploiter pour cela toutes les données dont ils peuvent disposer sur les consommateurs. Cependant, ces stratégies commerciales parfois ciblées et répétitives sont souvent vécues comme une intrusion par les consommateurs, provoquant des réactions négatives de lassitude et un sentiment d'insécurité face à ces sollicitations non souhaitées, ce qui n'est pas bénéfique pour les entreprises à long terme.

Enfin, une gestion optimisée des données personnelles des consommateurs prévient des risques judiciaires. En effet, à titre d'illustration, la réforme de la loi « Informatique et Libertés » par la loi du 6 août 2004 a eu pour conséquence d'augmenter le risque de non-conformité lié à la réglementation "informatique et libertés" :

- risque pénal qui pèse sur le responsable du traitement (C. pén., art. 226-16, jusqu'à cinq ans d'emprisonnement et 300 000 euros d'amende) ;
- risque de sanction administrative prononcée directement par la CNIL, à la faveur des nouveaux pouvoirs de contrôle et de sanction qu'elle tient de la réforme du 6 août 2004 (pouvoir de mettre en demeure, d'enjoindre de cesser la mise en œuvre d'un traitement, de prononcer une sanction pécuniaire ou un avertissement). Depuis 2004, la CNIL s'est engagée dans une politique sévère de contrôle et de sanction à l'égard des entreprises ;
- risques d'image et de notoriété, lorsque, par exemple, des clients découvrent dans la presse ou par le biais des actions de communication de la CNIL qu'un responsable de traitement n'a pas respecté certaines règles relatives à la confidentialité ou au respect de la vie privée.

Dans quels cas les règles de protection sont-elles applicables ?

En France, l'utilisation des données personnelles des consommateurs est très encadrée par les textes, à savoir principalement la loi Informatique et Libertés du 6 janvier 1978, modifiée notamment par la loi du 6 août 2004 transposant la directive européenne du 24 octobre 1995 (ci-après Loi « Informatique et Libertés »), et la loi du 21 juin 2004 pour la confiance dans l'économie numérique.

Pourtant, certaines entreprises ont tendance à s'interroger sur les réponses à apporter aux demandes des consommateurs à propos de leurs données personnelles, au regard des nombreuses règles en la matière.

Le premier élément qui peut soulever des interrogations concerne la définition des données personnelles. En effet, il est important de savoir ce que recouvre concrètement cette notion, puisqu'elle subordonne l'application du régime protecteur.

Ainsi, la loi Informatique et Libertés ne s'applique qu'aux traitements de données à caractère personnel, qu'ils soient automatisés ou pas.

Il faut cependant savoir qu'elle ne s'applique pas aux traitements mis en œuvre pour l'exercice d'activités purement et exclusivement personnelles.

Quelles activités peuvent être considérées comme purement et exclusivement personnelles ?

On peut entendre par activités personnelles celles concernant la vie privée ou familiale. Par exemple, la tenue d'un répertoire téléphonique, les correspondances privées, ou encore la création d'un site internet personnel sont des traitements entrant dans cette catégorie. Il convient toutefois d'être vigilant concernant ces sites web : leur accès doit être limité à quelques personnes.

Enfin, la finalité du traitement doit être exclusivement personnelle : le carnet d'adresses professionnel n'entre donc pas dans cette catégorie.

Tout d'abord, une donnée personnelle est une information concernant une personne physique. Les noms des sociétés, établissements publics, marques,... ne sont donc pas protégés par la loi Informatique et Libertés. Cette donnée doit identifier ou permettre d'identifier, **directement ou indirectement**, l'individu en cause.

Concernant les données permettant d'identifier directement une personne, il peut bien sûr s'agir des nom et prénom, ou encore d'une photographie ou d'un enregistrement de conversation téléphonique.

L'identification indirecte d'une personne est celle qui nécessite deux étapes. Par exemple, un numéro de téléphone permet d'identifier indirectement une personne, grâce à un annuaire inversé. En ce sens, constituent également des données à caractère personnel toutes les informations dont le recoupement permet d'identifier une personne précise (exemple : une date de naissance associée à une commune de résidence peut dans certains cas permettre l'identification d'une personne).

Quant au traitement de données, la loi le définit de manière large, comme tout ensemble d'opérations portant sur des données personnelles, quel que soit le procédé utilisé. Il s'agit notamment de la collecte, l'enregistrement, l'organisation, la conservation, la communication de données en France et à l'étranger, etc. Le texte reste muet quant à la technologie utilisée : traitement par ordinateur, par cartes à puces, serveurs Web... Cette précaution est destinée à ne pas exclure des avancées technologiques inconnues à ce jour. On dit de la Loi Informatique et Libertés qu'elle est « technologiquement neutre ».

Le traitement peut être automatisé, c'est à dire effectué au moyen d'un ordinateur entendu au sens large, mais aussi, depuis la réforme d'août 2004, non automatisé, c'est à dire manuel.

Ce traitement manuel n'est cependant concerné par la loi que s'il est organisé en un fichier, c'est-à-dire tout ensemble structuré et stable de données à caractère personnel accessibles selon des critères déterminés.

Exemple : si vous rangez vos comptes-rendus de réunion ou des CV de candidats par ordre alphabétique, par date, par thème...il s'agit d'un fichier.

→ → Les règles actuelles : les étapes à suivre pour utiliser des données personnelles de consommateurs en conformité avec la loi

• Etape 1 : formalités préalables auprès de la CNIL

Qui doit déclarer le traitement à la CNIL ?

Le traitement automatisé de données personnelles doit être déclaré par son responsable, c'est-à-dire en principe la personne, le service ou l'organisme qui détermine ses finalités et ses moyens.

A contrario, un prestataire de services (sous-traitant) agissant pour le compte du responsable de traitement (par exemple prestation d'envoi de mailing reposant sur l'utilisation du fichier clients du responsable de traitement) n'a pas à procéder à la déclaration du fichier clients qui lui est confié.

Quand le responsable du traitement est une personne morale, le déclarant est la personne qui décide de mettre en œuvre le traitement. Il peut s'agir du représentant légal, mais aussi, pour des sociétés de taille importante, d'une personne à la tête d'une direction ou d'une branche de l'entreprise, qui dispose d'une délégation de signature.

A qui dois-je déclarer le traitement ?

La Commission Nationale de l'Informatique et des Libertés (CNIL), créée par la Loi Informatique et Libertés du 6 janvier 1978, a pour mission de veiller à ce que les traitements de données personnelles soient créés et exploités conformément aux dispositions de cette loi.

Selon l'article 22 de cette loi, les traitements automatisés de données doivent faire l'objet de formalités préalables auprès de la CNIL (voir le lien vers le site de la CNIL p. 42). Toutefois, selon le type de traitement concerné, les formalités à effectuer sont différentes.

Quel type de déclaration dois-je faire ?

La déclaration simplifiée :

La CNIL édicte des normes simplifiées visant les traitements de données les plus couramment utilisés, dont la mise en œuvre n'est pas susceptible de porter atteinte à la vie privée ou aux libertés. Il s'agit en fait de documents décrivant les caractéristiques d'un type de traitement de données, et les règles spéciales qui lui sont applicables. Ainsi, si un traitement correspond à l'une de ces normes, il suffit alors d'envoyer à la CNIL une déclaration simplifiée de conformité à celle-ci.

Exemples : Norme simplifiée 48 sur les fichiers clients-prospects et la vente en ligne pour les secteurs de la santé, l'éducation, l'assurance et la banque, Norme simplifiée 39 sur la facturation de la téléphonie à la clientèle.

La déclaration normale :

Si votre traitement n'entre pas dans les catégories visées par une norme simplifiée, une déclaration normale est suffisante.

La déclaration normale comporte l'engagement que le traitement satisfait aux exigences de la loi. La CNIL délivre alors un récépissé, et le responsable du traitement peut le mettre en œuvre dès sa réception. En principe, la CNIL doit fournir ce récépissé sans délai, mais dans la pratique il peut être délivré plusieurs semaines après le dépôt de la déclaration.

Par ailleurs, il est possible de procéder à une déclaration unique pour des traitements appartenant à la même structure et ayant des finalités identiques ou liées entre elles.

Cependant, il faut savoir que la délivrance du récépissé par la CNIL n'exonère pas le demandeur de ses responsabilités. Par conséquent, la responsabilité du titulaire du fichier est toujours susceptible d'être engagée.

Si vous ne savez pas quel type de déclaration vous devez effectuer, le site de la CNIL vous permet de le déterminer en fonction de votre situation :

www.cnil.fr rubrique « Déclarer »

En cas de doute persistant, il est plus sûr d'effectuer une déclaration normale.

La demande d'autorisation :

Certains traitements automatisés doivent faire l'objet d'une autorisation préalable de la CNIL en raison de la nature des données traitées, de la finalité du traitement ou du transfert des données traitées hors de l'Union Européenne.

Ainsi, vous devez procéder à une demande d'autorisation si :

- vous enregistrez des données « sensibles » :
 - Origines raciales ou ethniques, opinions philosophiques, politiques, syndicales, religieuses, vie sexuelle ou santé des personnes ;
 - Données biométriques ;
 - Données génétiques ;
 - N° de sécurité sociale (sauf organismes autorisés) ;
 - Appréciations sur les difficultés sociales des personnes.
- votre traitement poursuit des finalités spécifiques :
 - traitements statistiques de l'INSEE ;
 - traitements susceptibles d'exclure du bénéfice d'un droit, d'une prestation ou d'un contrat ;
 - interconnexion de fichiers ayant des finalités distinctes ou correspondant à des intérêts publics distincts.
- si vous transférez des données en dehors de l'Union Européenne (cf. étape 4).

La CNIL a alors deux mois pour faire connaître sa position (refus, autorisation, demande d'informations supplémentaires). Il convient de noter que son silence équivaut à un refus.

La demande d'avis préalable¹ :

Certains traitements de fichiers portant sur des données spécifiques font l'objet d'une procédure d'autorisation plus complexe. Il s'agit

(1) - Cette procédure ne concerne que le secteur public.

des traitements mis en œuvre pour le compte de l'État et des traitements mis en œuvre pour le compte d'une personne morale de droit public ou d'une personne morale de droit privé gérant un service public (articles 26 et 27 de la loi Informatique et Libertés).

Quels renseignements dois-je fournir lors de ma déclaration ?

Les déclarations et les demandes d'autorisations doivent contenir les informations suivantes :

- l'identité et adresse du responsable des traitements ou de son représentant ;
- la ou les finalités du traitement ;
- le cas échéant les interconnexions ou les rapprochements ou toutes autres formes de mise en relation avec d'autres traitements ;
- les données à caractère personnel traitées, leurs origines et les catégories de personnes concernées par le traitement ;
- la durée de conservation des informations traitées ;
- le ou les services chargés de mettre en œuvre le traitement ;
- les destinataires ou catégories de destinataires ;
- les conditions d'exercice du droit d'accès ;
- les dispositions relatives à la sécurité des traitements ;
- le cas échéant les transferts de données à caractère personnel à destination d'États non membres de la Communauté européenne.

En outre, le responsable d'un traitement déjà autorisé ou déclaré doit informer la CNIL sans délai de tout changement affectant les informations précitées ou de toute suppression du traitement.

Les dispenses :

La CNIL a édicté des dispenses de déclaration. Cependant, ces dispenses ne concernent pas les traitements de données personnelles de consommateurs dans un but commercial : il s'agit de manière générale de traitements de données internes, comme par exemple les traitements de gestion de la paie, ou de fichiers de communication non commerciale.

Afin de vérifier si vous pouvez bénéficier d'une dispense, le site de la CNIL propose un système de vérification à l'adresse suivante :

<http://www.cnil.fr/vos-responsabilites/declarer-a-la-cnil/declarer-un-fichier/dispense/mon-secteur-dactivite/>

Les traitements pour lesquels le responsable a désigné un Correspondant Informatique et Libertés (CIL), sont dispensés de déclaration et de déclaration simplifiée (sauf dans le cas où ils sont soumis à autorisation, ce qui est le cas notamment si un transfert de données à caractère personnel vers un Etat non membre de la communauté européenne est envisagé).

Le Correspondant Informatique et Libertés (CIL)

La loi Informatique et Libertés prévoit la possibilité, de manière optionnelle, de nommer un Correspondant Informatique et Libertés.

Il s'agit d'une personne désignée au sein de la structure, ou en externe pour les petites structures, qui est notamment chargée de tenir un registre des traitements mis en œuvre au sein de l'organisme et de veiller au respect des dispositions de la loi Informatique et Libertés.

Consommation



Comment dois-je effectuer ma déclaration ?

Les formulaires nécessaires à la déclaration, disponibles sur le site de la CNIL, peuvent être envoyés par courrier, mais la déclaration peut également s'effectuer directement en ligne sur ce même site.

Toutefois, pour modifier une déclaration existante, il n'est pas possible de procéder à cette modification par Internet. Il faut notifier la modification en adressant un courrier qui précisera le numéro de la déclaration initiale, les coordonnées précises du responsable du traitement et l'objet de la modification.

Déclaration normale ou demande d'autorisation en ligne :
www.cnil.fr rubrique « Déclarer »

Déclaration simplifiée en ligne :
www.cnil.fr rubrique « Déclarer »

Quels sont les risques encourus si je ne respecte pas mon obligation de déclaration ?

Le défaut de déclaration, y compris par négligence, est tout d'abord passible de sanctions pénales, à savoir cinq ans d'emprisonnement et 300 000 euros d'amende, selon l'article 226-16 du Code pénal.

Le non respect de l'obligation déclarative peut également donner lieu à une sanction civile, c'est-à-dire le paiement de dommages et intérêts.

Enfin, la CNIL peut prononcer des sanctions (notamment des sanctions pécuniaires après mise en demeure restée infructueuse).

Il convient également de garder à l'esprit la sanction en termes d'image que constitue la publication des condamnations par la CNIL sur le site Legifrance notamment.

Par ailleurs, le non respect de la Loi Informatique et Libertés a des conséquences sur l'application d'autres réglementations générales. Elle peut par exemple entraîner l'annulation d'une procédure en droit social pour non respect des formalités préalables.

Les sanctions encourues en cas de violation des obligations légales visent en général le responsable du traitement, à savoir la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui détermine les finalités et les moyens du traitement. Dans la plupart des cas, l'application des règles de responsabilité civile ou pénale permettra de déterminer à qui la responsabilité doit être attribuée, et ainsi d'identifier le responsable du traitement.

Face aux incertitudes pratiques parfois liées à l'identification exacte, dans certaines circonstances, du responsable du traitement ou du sous-traitant, le "groupe de l'article 29", regroupant la CNIL et ses équivalents européens, a adopté le 16 février 2010 un avis 1/2010 sur les notions de « responsable du traitement » et de « sous-traitant ».

• Etape 2 : les règles à suivre au moment de la collecte des données personnelles.

Le principe de loyauté

Avant tout, la collecte de données à caractère personnel est soumise à un principe général de loyauté. En effet, la loi Informatique et Libertés énonce : « les données sont collectées et traitées de manière loyale et licite ».

Selon l'article 226-18 du Code pénal, le fait de collecter des données à caractère personnel par un moyen frauduleux, déloyal ou illicite est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende.

Ce principe général de loyauté donne lieu à plusieurs obligations pour le responsable du traitement de données.

L'obligation de loyauté se traduit par exemple en pratique par l'obligation de collecter des données directement auprès de la personne concernée.

A contrario, la collecte indirecte de données à caractère personnel doit être considérée, par principe, comme prohibée.

La collecte indirecte reste néanmoins possible dès lors qu'une disposition législative ou réglementaire le prévoit (par exemple cas d'une enquête diligentée par l'autorité judiciaire). Au-delà des cas

de collecte indirecte prévus dans la loi, il existe parfois une certaine tolérance sur ces sujets spécifiques, comme par exemple s'agissant des opérations de parrainage (marketing direct). La CNIL a ainsi émis le 30 mars 2005 un avis de conformité à la loi "Informatique et Libertés" concernant le code de conduite sur l'utilisation de coordonnées électroniques à des fins de prospection directe adopté par l'Union française du marketing direct (CNIL, délib. n° 2005-51, 30 mars 2005). Ce code prévoit des dispositions particulières en matière de parrainage.

L'exigence de finalité du traitement

La collecte de données personnelles doit obligatoirement avoir un objectif déterminé et légitime, défini dans la déclaration préalable, et par la suite les données ne pourront être utilisées que dans ce cadre. Il s'agit par exemple de la gestion de la clientèle, de prospection commerciale...

De plus, tout changement de finalité de traitement doit être sans délai porté à la connaissance de la CNIL.

Toutefois, il est possible d'utiliser des données faisant déjà l'objet d'un traitement lorsque cette nouvelle utilisation est faite à des fins statistiques ou de recherche scientifique ou historique, si le responsable du traitement respecte les obligations lui incombant à cet égard. Le fait d'utiliser des données personnelles à d'autres fins que celles déclarées à la CNIL constitue un détournement de finalité.

Exemple de détournement de finalité : un directeur d'établissement qui utilise le fichier de cet établissement afin d'envoyer des publicités étrangères à l'activité définie dans la déclaration préalable.

Le détournement de finalité peut aussi consister en une communication non autorisée à un tiers. En effet, l'article 226-22 du Code pénal sanctionne la divulgation de données personnelles par la personne les ayant recueillies à un tiers qui n'a pas qualité pour les recevoir. Ce comportement est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende.

Il est important d'être particulièrement vigilant, car même lorsqu'elle a été commise par imprudence ou négligence, cette divulgation est punie de trois ans d'emprisonnement et 100 000 euros d'amende.

Le principe de proportionnalité

L'exigence de finalité du traitement va de pair avec le respect du principe de proportionnalité : proportionnalité des données collectées et proportionnalité de la durée de conservation.

Les données traitées doivent être adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et de leurs traitements ultérieurs.

Le principe de proportionnalité implique donc que le traitement doit se limiter aux données pour lesquelles il existe un rapport direct avec la finalité initiale du traitement. De plus, les données doivent être supprimées ou archivées quand elles ne sont plus nécessaires pour la finalité du traitement.

De manière générale, la CNIL prend garde à ce que le degré de confidentialité des données, les moyens techniques mis en œuvre pour assurer cette confidentialité, et leur dangerosité potentielle, soient strictement nécessaires aux finalités poursuivies. Vous devez donc vous assurer de limiter la collecte aux données essentielles, afin de ne pas stocker de données superflues. Ainsi par exemple, il convient de vérifier si la date de naissance de l'individu, donnée considérée comme permettant aisément l'identification d'un individu, est indispensable, ou si la seule mention de l'année pourrait suffire.

Quelles informations dois-je fournir aux consommateurs ?

Les données personnelles ne peuvent pas être collectées à l'insu des personnes concernées. La loi Informatique et Libertés prévoit très précisément le contenu des informations à fournir au consommateur au moment de la collecte des données, sauf si elles l'ont été au préalable :

- 1° L'identité du responsable du traitement et, le cas échéant, de celle de son représentant ;
- 2° La finalité poursuivie par le traitement auquel les données sont destinées ;
- 3° Le caractère obligatoire ou facultatif des réponses ;
- 4° Les conséquences éventuelles, à son égard, d'un défaut de réponse ;
- 5° Les destinataires ou catégories de destinataires des données ;

6° Les droits de la personne concernée à l'égard du traitement de ses données (droits d'accès, d'opposition, de rectification, etc.) ;

7° Les transferts de données personnelles envisagés à destination d'un État non membre de la Communauté européenne.

La loi précise également que lorsque les données sont recueillies par voie de questionnaire, celui-ci doit comporter les mentions suivantes : l'identité du responsable, la finalité du traitement, le caractère obligatoire ou facultatif des réponses et l'ensemble des droits permettant à la personne concernée d'accéder à ses données.

Toute personne utilisatrice des réseaux de communications électroniques doit par ailleurs être informée de manière claire et complète 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 stockées dans son équipement terminal de connexion, ou à inscrire, par la même voie, des informations dans son équipement terminal de connexion ;
- des moyens dont elle dispose pour s'y opposer.

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.



Il est par ailleurs prévu une exception au principe de l'information lorsque les données sont rendues anonymes rapidement, selon un procédé reconnu conforme à la loi par la CNIL : dans ce cas, les informations délivrées par le responsable du traitement à la personne concernée peuvent se limiter à l'identité du responsable des traitements ou de son représentant et à la finalité du traitement.

La loi prévoit également une obligation d'information en matière de collecte indirecte, c'est-à-dire lorsque les données à caractère personnel n'ont pas été recueillies auprès de la personne concernée, mais auprès d'un tiers. C'est le cas lorsqu'il y a une cession de données, ce qui est fréquent dans le domaine du marketing notamment. Par exemple, un consommateur fournit son adresse mail sur un site internet, et celui-ci cède ensuite son fichier de données à un tiers à des fins de prospection.

Dans ce cas, le responsable du traitement doit tout de même fournir à la personne concernée toutes les informations énumérées ci-dessus. Elles doivent être portées à la connaissance de l'intéressé dès l'enregistrement des données ou, si une communication des données à des tiers est envisagée, au plus tard lors de la première communication des données.

La loi prévoit cependant que lorsque les données à caractère personnel ont été initialement recueillies pour un autre objet, l'obligation d'information lors de la collecte indirecte ne s'applique pas si le deuxième traitement concerne la conservation de ces données à des fins historiques, statistiques ou scientifiques, lorsque ce traitement est effectué dans des conditions prévues par la loi. Par exemple, si des données sont acquises dans l'unique but de réaliser une étude statistique répondant aux conditions légales, l'information du consommateur n'est pas nécessaire.

L'obligation d'information ne s'applique pas non plus lorsque la personne concernée est déjà informée ou quand son information se révèle impossible ou exige des efforts disproportionnés par rapport à l'intérêt de la démarche.

Le défaut d'information de la personne concernée est sanctionné par une amende de 1 500 euros.

Retrouvez les modèles des mentions légales pour l'information sur le site de la CNIL ;

<http://www.cnil.fr/vos-responsabilites/mentions-legales/>

Par quels moyens dois-je fournir ces informations ?

Les modalités de communication des informations varient selon le support de la collecte de données utilisé.

Lorsque la collecte est réalisée par écrit, l'information doit figurer sur le support de collecte ou, à défaut, sur un document préalablement porté à la connaissance des personnes concernées, en caractères lisibles. Les coordonnées du service doivent également être communiquées, pour leur permettre d'exercer leurs droits d'opposition, d'accès et de rectification.

Lorsque la collecte des données est faite oralement à distance, ces informations doivent être lues aux personnes concernées, en leur indiquant qu'elles peuvent, sur simple demande même exprimée oralement, les recevoir postérieurement par écrit, ou par voie électronique avec leur accord.

Si ces informations sont portées à la connaissance des personnes par voie d'affichage, il doit être indiqué qu'elles peuvent, sur simple demande orale ou écrite, les recevoir sur un support écrit.

Quelles sont mes obligations concernant le consentement du consommateur ?

La loi Informatique et Libertés prévoit notamment qu'il est nécessaire de disposer du consentement de la personne concernée, si elle est majeure, ou de ses parents si elle est mineure, afin de procéder à un traitement de données à caractère personnel la concernant.

La loi prévoit néanmoins la possibilité de procéder au traitement de données en l'absence du consentement de la personne lorsque l'une des conditions suivantes est remplie :

- Le respect d'une obligation légale incombant au responsable du traitement ;
- La sauvegarde de la vie de la personne concernée ;
- L'exécution d'une mission de service public dont est investi le responsable ou le destinataire du traitement ;
- L'exécution soit d'un contrat auquel la personne concernée est partie, soit de mesures précontractuelles prises à la demande de celle-ci ;
- La réalisation de l'intérêt légitime poursuivi par le responsable du traitement ou par le destinataire, sous réserve de ne pas méconnaître l'intérêt ou les droits et libertés fondamentaux de la personne concernée.



Comment s'effectue le recueil du consentement ?

Aux termes de l'article 2 de la directive européenne du 24 octobre 1995, il convient d'entendre par consentement toute manifestation de volonté, libre, spécifique et informée par laquelle la personne concernée accepte que des données à caractère personnel la concernant fassent l'objet d'un traitement.

Dans la pratique, et au regard des exceptions précitées, le recueil du consentement n'est nécessaire que dans un nombre de cas limités, en particulier dans deux cas énoncés par la loi. Le premier concerne la collecte de données sensibles, pour laquelle le consentement doit être exprès. Le second porte sur la collecte de données personnelles à des fins de prospection commerciale par courrier électronique, automate d'appel, SMS et MMS, où la loi requiert le recueil du consentement préalable, sauf exception. Pour plus de précisions concernant la prospection commerciale par courrier électronique, vous pouvez vous reporter à la Charte de l'Union française du marketing direct sur l'e-mailing, validée par la CNIL, disponible à l'adresse suivante :

http://www.ufmd.org/telechar/code_ufmd_prospection_emailing.pdf

Le cas des données dites sensibles

« Il est interdit de collecter ou de traiter des données à caractère personnel qui font 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 santé ou à la vie sexuelle de celles-ci » (Loi Informatique et Libertés, article 8).

Des exceptions sont cependant prévues par la loi. Dans la mesure où la finalité du traitement l'exige pour certaines catégories de données, ne sont notamment pas soumis à l'interdiction :

- Les traitements pour lesquels la personne concernée a donné son consentement exprès, sauf dans le cas où la loi prévoit que l'interdiction ne peut être levée par le consentement de la personne concernée ;
- Les traitements mis en œuvre par une association ou tout autre organisme à but non lucratif et à caractère religieux, philosophique, politique ou syndical. Les informations traitées ne doivent concerner que leurs seuls membres ou des personnes qui entretiennent des contacts réguliers avec cette association ou organisme, et les données ne doivent pas être transmises à des tiers sauf consentement exprès des intéressés ;
- Les traitements portant sur les données à caractère personnel rendues publiques par la personne concernée.

A ce titre, le NIR (numéro d'inscription au registre national ou numéro de sécurité sociale) est à traiter comme une donnée « sensible » dans la mesure où la collecte et l'utilisation de cette information n'est possible que si un texte législatif ou réglementaire le prévoit spécifiquement.

Les traitements de données sensibles bénéficiant d'un procédé d'anonymisation peuvent être autorisés par la CNIL, en fonction de leur finalité.

En outre, selon l'article 226-19 du Code pénal, le non respect de cette interdiction est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende.

Enfin, il convient de noter que les traitements de données à caractère personnel relatives aux infractions, condamnations et mesures de sûreté ne peuvent en aucun cas être mis en œuvre par les entreprises.

• **Etape 3 : quels sont les droits des consommateurs ?**

Pour assurer l'objectif de protection des libertés et de la vie privée des consommateurs, ceux-ci peuvent, selon la Loi Informatique et Libertés, exercer un contrôle sur leurs données personnelles faisant l'objet de traitements.

Il est donc important pour les entreprises de savoir quelles peuvent être les demandes des consommateurs sur ce point, afin de tenir compte de leurs droits.

Le droit à l'information

C'est le premier droit dont dispose toute personne faisant l'objet d'un traitement de données. En effet, les données personnelles des consommateurs ne doivent pas être utilisées à leur insu : ceux-ci doivent être informés au préalable des traitements dont elles vont faire l'objet.

L'information n'est pas mise en œuvre uniquement au moment de la collecte mais également lors de chaque exploitation de données personnelles, notamment par le biais de la mention d'information sur le droit d'accès, de rectification et d'opposition.

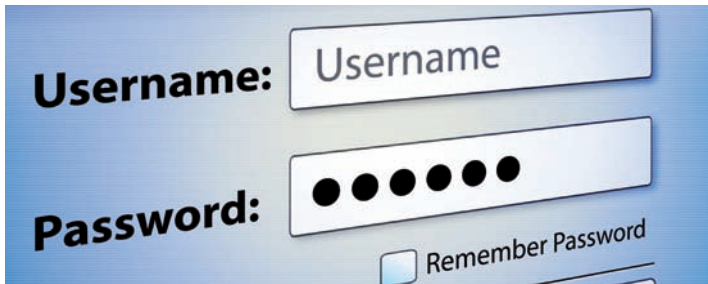
Le droit d'accès

Chacun a un droit d'accès sur les informations le concernant et peut en obtenir une copie, dont le coût ne peut dépasser celui de la reproduction. La communication des données doit être effectuée en termes intelligibles et compréhensibles.

Plus précisément, la loi Informatique et Libertés prévoit que « toute personne physique justifiant de son identité a le droit d'interroger le responsable d'un traitement de données à caractère personnel en vue d'obtenir :

- La confirmation que les données à caractère personnel la concernant font ou ne font pas l'objet d'un traitement ;
- Des informations relatives aux finalités du traitement, aux catégories de données à caractère personnel traitées et aux destinataires auxquels les données sont communiquées ;
- Le cas échéant des informations relatives aux transferts de données à caractère personnel envisagés à destination d'un État membre de la Communauté européenne ;
- La communication sous une forme accessible, des données à caractère personnel qui la concernent ainsi que toute information disponible quant à l'origine de celles-ci ;
- Les informations permettant de connaître et de contester la logique qui sous-tend le traitement automatisé en cas de décision prise sur le fondement de celui-ci et produisant des effets juridiques à l'égard de l'intéressé.

L'exercice du droit d'accès permet de contrôler l'exactitude des données et, au besoin, de les faire rectifier ou effacer (cf. point suivant). Ce droit d'accès appartient aux personnes physiques. Concernant les personnes morales, le droit est attribué aux dirigeants personnes physiques ou à tout autre représentant de la personne morale dont le nom figure dans le fichier.



La communication n'est pas nécessairement écrite. Dans ce cas, selon la CNIL, la durée de la mise à disposition de l'information doit être suffisante pour que le demandeur puisse prendre note commodément et complètement.

Ce droit d'accès connaît toutefois deux limites :

- Si le responsable du traitement estime que les demandes sont manifestement abusives (notamment par leur nombre, leur caractère répétitif ou systématique), il peut refuser d'y donner suite. Cependant, en cas de contestation devant un juge, ce sera à lui de prouver ce caractère manifestement abusif.
- Le droit d'accès ne s'applique pas lorsque les données à caractère personnel sont conservées sous une forme excluant manifestement tout risque d'atteinte à la vie privée des personnes concernées et pendant une durée n'excédant pas celle nécessaire aux seules finalités d'établissement de statistiques ou de recherche scientifique ou historique. Par conséquent, le responsable de traitement doit être en mesure de justifier que les moyens de conservation employés sont de nature à exclure manifestement tout risque d'atteinte à la vie privée des personnes concernées. La CNIL recommande d'utiliser, en particulier en cas de données sensibles, des procédés d'anonymisation. En outre, si les données ne sont conservées que pendant un court délai puis détruites, l'accès est alors impossible.

Enfin, tout refus à une demande d'accès est sanctionné d'une amende de 1 500 euros par infraction constatée.

Retrouvez le guide pratique de la CNIL relatif au droit d'accès sous le lien suivant :

http://www.cnil.fr/fileadmin/documents/Guides_pratiques/CNIL_Droit_d_acces.pdf

Le droit de rectification

Selon la loi Informatique et Libertés, « toute personne physique justifiant de son identité peut exiger du responsable d'un traitement que soient, selon les cas, rectifiées, complétées, mises à jour, verrouillées ou effacées les données à caractère personnel la concernant, qui sont inexactes, incomplètes, équivoques, périmées, ou dont la collecte, l'utilisation, la communication ou la conservation est interdite ».

En pratique, pour exercer son droit de rectification, le consommateur va donc écrire à l'organisme qui détient les informations.

Pour s'assurer de l'effectivité de sa demande, le consommateur peut demander, sans frais, au responsable du traitement de prouver qu'il a procédé aux rectifications demandées.

Si une donnée a été transmise à un tiers, le responsable du traitement doit lui notifier les modifications effectuées, afin qu'il y procède également.

Le fait de s'opposer à une demande de rectification est puni d'une amende de 1 500 euros par infraction constatée.

Le droit d'opposition

Toute personne a le droit de s'opposer, pour des motifs légitimes, à ce que des données personnelles le concernant fassent l'objet d'un traitement. L'exercice de ce droit ne devrait pas empêcher la fourniture du service demandé par le consommateur (exemple : les données personnelles demandées au consommateur pour la gestion de son contrat).



De plus, toute personne peut refuser, à tout moment, sans avoir à le justifier et sans frais, que les données la concernant soient utilisées à des fins de prospection commerciale, (téléphoniques avec intervention humaine ou postales) par le responsable actuel du traitement ou celui d'un traitement ultérieur.

Dans tous les cas, le consommateur doit être informé au moment de la collecte de la possibilité d'exercer librement son opposition et, doit être mis en mesure de l'exercer lors de chaque message adressé.

Pour mémoire, lorsqu'il s'agit de sollicitations commerciales par courrier électronique, automate d'appel, SMS et MMS, le professionnel doit recueillir le consentement préalable du consommateur.

Comment s'exerce le droit d'opposition ?

En pratique, le droit d'opposition s'exerce soit au moment de la collecte d'informations soit plus tard, en s'adressant au responsable du fichier. Ce droit d'opposition peut donc s'exprimer de différentes manières :

- par le refus de répondre lors d'une collecte non obligatoire de données ;
- par le refus de donner l'accord écrit obligatoire pour le traitement de données sensibles ;
- par la possibilité de demander la suppression des données contenues dans les fichiers commerciaux ;
- par la possibilité d'exiger la non-cession ou la non-commercialisation d'informations.

• Etape 4 : Les règles à respecter dans le cadre de l'exploitation des données personnelles

Combien de temps puis-je conserver des données personnelles ?

Les données ne peuvent être conservées au-delà de la durée nécessaire à la réalisation des finalités pour lesquelles elles ont été collectées. Les données pourront être conservées plus longtemps si elles sont destinées à des fins historiques, statistiques ou scientifiques.

La loi "Informatique et Libertés" ne définit spécifiquement aucune durée de conservation précise des données collectées. Elle se limite à poser un principe général aux termes duquel la durée de conservation doit être proportionnée à la "finalité" du traitement. Ce principe laisse donc une certaine souplesse à chaque responsable de traitement pour définir les durées de conservation qui lui apparaissent les plus pertinentes, étant entendu que la CNIL est fondée à exercer un contrôle de proportionnalité sur la durée définie par le responsable du traitement.

Le responsable du fichier doit donc fixer une durée de conservation raisonnable en fonction de l'objectif du fichier, et indiquer cette durée lors de la mise en œuvre des formalités préalables.

En cas de non-respect de cette durée, l'article 226-20 du Code pénal prévoit des sanctions de cinq ans de prison et 300 000 euros d'amende.

Quelles sont mes obligations concernant la conservation des données personnelles ?

« 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 » (Loi Informatique et Libertés, article 34).

Cet article impose donc une obligation de sécurité et une obligation de confidentialité des données.

Concernant l'obligation de sécurité, le responsable doit adopter des mesures de sécurité physiques (sécurité des locaux), logiques (sécurité des systèmes d'information), adaptées à la nature des données et aux risques présentés par le traitement et qui, a minima, ne doivent pas être inférieures à l'état de l'art.

Le non-respect de l'obligation de sécurité est sanctionné de 5 ans d'emprisonnement et de 300 000 € d'amende (article 226-17 du Code pénal).

Concernant l'obligation de confidentialité, seules les personnes autorisées peuvent accéder aux données personnelles contenues dans un fichier. Il s'agit des destinataires explicitement désignés pour en prendre connaissance et de certains « tiers autorisés » qui peuvent les recevoir de façon ponctuelle et motivée (exemples : la police, le fisc).

Il faut également être vigilant en cas de recours à des sous-traitants ayant accès dans le cadre de leur mission aux données personnelles recueillies. En effet, la loi Informatique et Libertés prévoit que tout sous-traitant ou toute personne agissant sous l'autorité du responsable du traitement ne peut procéder au traitement des données



personnelles que sur instruction du responsable du traitement. Le sous-traitant doit présenter des garanties suffisantes pour assurer la mise en œuvre des mesures de sécurité et de confidentialité, sans que cela ne décharge le responsable du traitement de son obligation de veiller au respect de ces mesures.

En outre, le contrat liant le sous-traitant au responsable doit comporter l'indication des obligations incombant au sous-traitant en matière de protection de la sécurité et de confidentialité des données, et prévoir que le sous-traitant ne peut agir que sur instruction du responsable.

La communication d'informations à des personnes non-autorisées est punie de 5 ans d'emprisonnement et de 300 000 euros d'amende. Dans le cas où la divulgation intervient par imprudence ou négligence, elle est punie de 3 ans d'emprisonnement et de 100 000 euros d'amende (article 226-22 du Code pénal).

Dans quelles conditions puis-je céder mes fichiers de données personnelles ?

Par cession, on entend ici vendre mais aussi prêter ou louer un fichier contenant des données à caractère personnel.

De telles cessions sont licites, sous réserve que plusieurs conditions soient respectées.

Tout d'abord, il faut que la cession soit prévue dans la déclaration initiale faite à la CNIL par l'entreprise cédante. Si ce n'est pas le cas, l'entreprise désirant céder ces données à caractère personnel à des tiers doit obligatoirement porter ces modifications à la connaissance de la CNIL. À défaut, elle risque la sanction prévue en cas de détournement de finalité (article 226-21 du Code pénal : cinq ans d'emprisonnement et 300 000 euros d'amende).

De plus, il faut qu'il y ait soit absence d'opposition soit consentement de la personne concernée, selon les cas.

En effet, toute personne a le droit de s'opposer à l'insertion des données à caractère personnel la concernant dans un fichier destiné à être commercialisé. Il convient donc d'informer le consommateur de la possibilité d'une cession (notamment à ses partenaires), et de lui donner la possibilité de s'y opposer.

Toutefois, concernant la cession de données sensibles ou de coordonnées électroniques, le recueil du consentement de la personne est exigé (Cf. encadré « Comment s'effectue le recueil du consentement » page 22).

Est-il possible de transférer des données personnelles à l'étranger ?

Il y a transfert de données personnelles vers l'étranger lorsque les données sont transférées depuis le territoire européen vers un Etat non membre de l'Union européenne. Le transfert peut s'effectuer par copie, par déplacement de données, par l'intermédiaire d'un réseau ou d'un support à un autre.

En principe, de tels transferts sont interdits (article 68 de la Loi Informatique et Libertés).

En effet, les lois des Etats membres garantissent la protection de la vie privée à l'égard des traitements de données à caractère personnel. Mais lorsque de telles données sont transmises hors de l'Union, il faut s'assurer que les citoyens ne subissent pas de désavantage parce que leurs droits seraient moins bien protégés.

Il est cependant fait exception à ce principe si le pays du destinataire a été reconnu comme assurant une protection adéquate, c'est-à-dire équivalente à celle dont bénéficie le citoyen européen. Cette protection adéquate peut être réalisée de plusieurs manières :

- Légalement : si le pays non membre de l'Union a été reconnu comme disposant d'une législation assurant une protection suffisante des données personnelles. C'est le cas de la Suisse, des îles Guernesey et de Jersey, de l'Isle de Man, du Canada et de l'Argentine.
- De manière contractuelle : par la signature, entre l'exportateur de données et l'importateur, de clauses contractuelles types approuvées par la Commission européenne. Pour établir ces clauses, on distingue les transferts de responsable de traitement à responsable de traitement et les transferts de responsable de traitement à sous-traitant.

Des modèles de clauses contractuelles types sont disponibles à cette adresse :

<http://www.cnil.fr/vos-responsabilites/transferer-des-donnees-a-letranger/contrats-types-de-la-commission-europeenne/>

Il est également possible d'adopter des Règles internes d'entreprise (BCR ou Binding Corporate Rules) qui constituent le code de conduite d'un groupe dans ce domaine. Les BCR concernent les multinationales qui exportent des données depuis leurs filiales situées au sein de l'Union européenne vers des pays tiers n'assurant pas un niveau de protection équivalent à celui de l'Union européenne. L'adoption de BCR permet d'éviter de conclure autant de contrats qu'il y a de transferts au sein du groupe.

Une trame pour aider les entreprises à la rédaction des BCR est disponible à cette adresse :

http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2008/wp154_fr.pdf

- Aux Etats-Unis, seules les entreprises qui ont volontairement adhéré aux accords dits de Safe Harbor² peuvent librement recevoir des données personnelles d'Europe.

Il existe enfin des exceptions au principe d'interdiction de transferts qui permettent d'exporter des données en dehors de l'UE sans restriction particulière. Ces exceptions sont prévues par la directive

(2) - Les Etats Unis proposent un système de protection des données, qualifié habituellement de Safe Harbor Principles. L'objectif est de satisfaire aux dispositions de la directive vie privée et des lois de transposition, qui interdisent les flux transfrontières vers des pays hors-Union Européenne qui n'ont pas un niveau de sécurité "adéquat".

95/46/CE du 24 octobre 1995, et à l'article 69 de la loi du 6 janvier 1978. Elles concernent par exemple le cas où la personne concernée a consenti expressément au transfert de ses données personnelles ou bien encore l'hypothèse de l'exécution d'un contrat entre le responsable du traitement et l'intéressé. Ces exceptions, qui ont pour conséquence de permettre à un responsable de traitement de pouvoir exporter des données sans encadrement juridique particulier, sont interprétées de façon restrictive par la CNIL qui considère que leur utilisation doit être limitée à des cas ponctuels et exceptionnels. La CNIL estime en particulier que les transferts répétitifs, massifs ou structurels de données personnelles doivent faire l'objet d'un encadrement juridique spécifique et ne peuvent donc pas reposer sur ces exceptions.

Les personnes dont les données sont susceptibles d'être transférées hors de l'Union européenne doivent être informées de l'existence de ce transfert, et ce dernier ne doit pas poursuivre une finalité différente de celle pour laquelle les données ont été initialement collectées.

Dans le cas où le traitement dont sont issues les données transférées entre dans le champ d'application d'une norme simplifiée prévoyant expressément une dispense de demande d'autorisation, il convient de s'y référer.

En cas de non respect des règles en matière de transfert de données, il est prévu des sanctions pénales de 300 000 euros d'amende et de cinq ans d'emprisonnement (articles 226-16, 226-16-1-A et 226-22-1 du Code pénal).



→ → Les évolutions à venir

Le présent document est le reflet des règles de protection des données personnelles des consommateurs existantes. Celles-ci vont probablement évoluer dans les années à venir compte tenu des débats en cours en France et dans l'Union européenne (procédure de révision de la directive cadre du 24 octobre 1995 sur la protection des données actuellement en cours).

Parallèlement à ces évolutions de l'encadrement législatif, l'avis du Conseil National de la Consommation sur la protection des données personnelles des consommateurs a ouvert la voie à des modalités de régulation plus souples et évolutives qui pourront compléter le dispositif législatif et réglementaire classique par une politique de mobilisation volontaire des entreprises et des parties prenantes de la consommation.

Le CNC formule 27 propositions relatives aux actions de sensibilisation et d'information tant des consommateurs que des entreprises, aux acteurs de la protection des données personnelles et au cadre juridique de la protection des données personnelles. Il recommande que les entreprises et les sites Internet prennent des dispositions pour rendre facilement accessibles et repérables leurs règles propres de protection de la vie privée.

Considérant que la sensibilisation des entreprises à la protection de la vie privée sous tous ses aspects implique la formation du personnel, le CNC recommande que les plans de formation déjà existants dans les entreprises soient complétés par des modules spécifiques pour les salariés qui ont accès aux données personnelles des consommateurs, ou qui sont chargés de la mise en œuvre des traitements, ou qui participent à la conception et à la définition des services rendus à la clientèle ou des modalités de démarchage de nouveaux clients.

Prenant acte de l'engagement du MEDEF de réaliser un guide pratique destiné aux organisations professionnelles et aux entreprises de toute taille et de tout secteur afin d'améliorer l'information et la connaissance sur l'environnement législatif et réglementaire et de

présenter des exemples de bonnes pratiques, le CNC préconise que sur cette base, des actions d'information soient réalisées par les organisations professionnelles sectorielles et territoriales à destination de leurs adhérents entreprises. Il recommande en outre le développement de démarches volontaires des entreprises pour la protection des données personnelles des consommateurs, notamment sous la forme de l'élaboration de codes sectoriels de bonne conduite assortis de dispositifs permettant de mesurer l'effectivité des engagements pris et d'en contrôler la bonne application.

Le CNC considère également qu'il n'y aurait que des avantages à ce que plus d'entreprises aient recours à des CIL, notamment en fonction de la sensibilité et du volume des données traitées. Pour les entreprises qui n'ont pas de CIL, le CNC préconise l'identification d'un point de contact pour assurer l'information et l'exercice des droits des consommateurs sur leurs données personnelles. Ce point de contact doit être facilement accessible pour les consommateurs.

Par ailleurs, il recommande à une entreprise qui sollicite le consentement d'un consommateur pour l'envoi d'offres commerciales par voie électronique, tel que prévu par la loi, de dissocier le consentement à recevoir des offres de l'entreprise elle-même et le consentement à recevoir des offres émanant de partenaires de cette entreprise afin d'éviter toute confusion dans l'esprit du consommateur sur la portée de son consentement. En relation avec la CNIL, le CNC dressera, au 1er semestre 2012, un bilan de la mise en œuvre de cet avis.

Enfin, Frédéric LEFEBVRE, secrétaire d'État chargé du commerce de l'artisanat, des PME, du tourisme, des services, des professions libérales et de la Consommation, Alex TÜRK, Président de la CNIL et Nathalie HOMOBONO, Directrice Générale de la DGCCRF ont signé, le jeudi 6 janvier 2011, un protocole de coopération destiné à renforcer la protection des données personnelles des consommateurs. Le nouveau dispositif permettra l'échange d'informations entre les deux autorités afin de renforcer leurs actions de contrôle. Ainsi, la CNIL se verra communiquer les manquements à la loi « Informatique et Libertés » constatés par les enquêteurs du Service national d'enquête (SNE) de la DGCCRF lors de leurs contrôles. Sur la base de ces informations, la CNIL pourra alors user de ses pouvoirs de contrôle et de sanction.



Au titre des évolutions en cours, il convient enfin de souligner l'« accountability » qui fait en pratique référence à l'ensemble des mesures internes prises par un responsable de traitement afin d'attester de son niveau de conformité à la réglementation applicable. Ces mesures internes peuvent par exemple concerner la mise en place d'une procédure de gestion des plaintes, la réalisation d'audits internes ou externes, la réalisation de « privacy impact assessments » (PIA), la désignation d'un correspondant à la protection des données ou encore l'adoption de « binding corporate rules » (BCRs) visant à encadrer les transferts de données en dehors de l'Espace Economique Européen (EEE).

Le concept « d'accountability » valorise une démarche de co-régulation au travers de laquelle l'entreprise est invitée à se responsabiliser et à définir, par elle-même, les mesures de mise en conformité qu'elle estime les plus adaptées à sa situation et sur la base desquelles elle est tenue de rendre compte, tant auprès des autorités de contrôle que des personnes fichées, de son niveau exact de conformité à la réglementation applicable. Ce concept introduit donc à la fois un haut niveau de confort pour l'entreprise qui bénéficie d'une certaine souplesse dans la définition de son programme de conformité, et, dans le même temps, n'abaisse pas le niveau de contrôle susceptible d'être opéré par les autorités publiques.

→ → Foire aux questions

A quelles occasions un professionnel est-il amené à collecter des données personnelles de consommateurs ?

Les situations dans lesquelles un professionnel est amené à collecter des données personnelles de consommateurs sont de plus en plus nombreuses. Les utilisations possibles de ces données sont en effet très variées : elles peuvent servir dans le cadre de la gestion des clients (contrats, commandes, factures, gestion de programme fidélité, gestion des impayés...) ou encore pour la prospection (constitution et gestion d'un fichier de prospects, sélection de clients pour réaliser des actions de prospection et de promotion, élaboration de statistiques commerciales...). De la même façon, les moyens pouvant être utilisés pour procéder à cette collecte sont très nombreux : une entreprise peut ainsi recueillir des informations lors de l'envoi d'une documentation, grâce à un questionnaire, lors de jeux-concours...

Quand dois-je déclarer un fichier à la CNIL ?

En principe, lorsqu'un traitement automatisé comporte des données qui permettent d'identifier directement ou indirectement des personnes physiques, celui-ci doit être déclaré préalablement à sa mise en œuvre.

Il faut toutefois vérifier que le traitement de données concerné n'est pas exonéré de déclaration par la CNIL. Notamment, si vous avez désigné un correspondant Informatique et Libertés (CIL), vous êtes dispensé de déclarer un grand nombre de fichiers.

Comment déterminer la règle applicable à mon traitement de données (déclaration, dispense, autorisation) ?

Il convient tout d'abord de vérifier que votre traitement ne fait pas l'objet d'une dispense : celles-ci sont consultables sur le site de la CNIL. Si tel n'est pas le cas, vous devez consulter les normes simplifiées édictées par la CNIL : si votre fichier correspond à l'une

d'entres elles, vous pourrez faire une déclaration simplifiée. S'il ne répond à aucune norme simplifiée, il vous faut effectuer une déclaration normale. Toutefois, pour certains traitements spécifiques (en raison de la nature des données traitées, de la finalité du traitement ou du transfert des données traitées hors de l'Union Européenne), il est nécessaire de procéder à une demande d'autorisation préalable.

Des aides sont disponibles sur le site de la CNIL pour vous permettre de déterminer la procédure à suivre.

Qu'est-ce qu'un cookie ?

Les cookies sont des fichiers enregistrés sur l'ordinateur d'un utilisateur lors de sa visite sur un site web, permettant de retracer son parcours sur le web, et qui facilitent ainsi sa navigation (mémoire de mots de passe, conservation du contenu de son panier sur des sites commerciaux...). Il s'agit donc de « témoins de connexion ». Si ces fichiers sont parfois utilisés dans une démarche marketing ils font cependant l'objet de règles limitant leur utilisation afin notamment de protéger la vie privée des utilisateurs, leur utilisation est nécessaire pour assurer le fonctionnement de certains services.

Comment transmettre les informations requises au consommateur ? (clause type)

Lorsque la collecte des données est réalisée par écrit, l'information du consommateur doit également se faire par écrit.

Exemple de clause à adapter selon vos besoins (CNIL) :

..... (Veuillez indiquer l'identité du responsable du traitement)

Les informations recueillies font l'objet d'un traitement informatique destiné à ...

(Veuillez préciser la finalité). Les destinataires des données sont : (Précisez).

Conformément à la loi « Informatique et Libertés » du 6 janvier 1978 modifiée en 2004, vous bénéficiez d'un droit d'accès et de rectification aux informations qui vous concernent, que vous pouvez exercer

en vous adressant à (Veuillez préciser le service et l'adresse).

Vous pouvez également, pour des motifs légitimes, vous opposer au traitement des données vous concernant.

Voir aussi concernant l'e-mailing, la charte UFMD³ :

http://www.ufmd.org/telechar/code_ufmd_prospection_emailing.pdf

(3) - UFMD : Union française du marketing direct.

Que recouvrent les droits d'accès et de rectification du consommateur ?

Toute personne dispose du droit de demander au détenteur d'un fichier de lui communiquer toutes les informations la concernant, afin de vérifier les informations enregistrées et, le cas échéant, de les faire rectifier.

Quelles informations dois-je fournir au consommateur en cas de transfert de données personnelles hors de l'Union Européenne (clause type) ?

Le consommateur doit être informé si le transfert de ses données en dehors de l'Union européenne est envisagé. Pour cela, la CNIL propose ce modèle de clause, à adapter selon vos besoins :

..... (Identité du responsable du traitement) dispose(nt) de moyens informatiques destinés à gérer (Veuillez indiquer la finalité du traitement, par exemple la gestion des ressources humaines, la gestion de la paie, la maintenance informatique, etc....).

Les informations enregistrées sont réservées à l'usage du (ou des) service(s) concerné(s) et ne peuvent être communiquées qu'aux destinataires suivants : ... (Veuillez préciser les destinataires).

Certains de ces destinataires sont situés en dehors de l'Union Européenne, et en particulier les destinataires suivants (Veuillez indiquer le nom des entités ou services destinataires ainsi que leur pays d'établissement) Ces destinataires auront communication des données suivantes (à préciser, par exemple nom, prénom, matricule, coordonnées professionnelles, salaire, données de connexion...)

La transmission de ces données aux destinataires situés en dehors de l'Union Européenne est destinée à ... (Veuillez indiquer la finalité du transfert des données).

Les garanties suivantes ont été prises pour s'assurer d'un niveau de protection suffisant des données personnelles :

Le pays du ou des destinataires(s) offre un niveau de protection adéquat par décision de la Commission Européenne : (Précisez laquelle);

Les ou les destinataires (s) adhèrent (s) aux principes du Safe Harbour;

Le transfert de données a été autorisé par la CNIL et est encadré par les clauses contractuelles types établies par la Commission Européenne (préciser le numéro de la délibération autorisant le transfert);

Le transfert de données a été autorisé par la CNIL et est encadré par des règles internes validées par la CNIL;

La société bénéficie d'une des exceptions mentionnées à l'article 69 de la loi du 6 janvier 1978 modifiée en 2004 : (Préciser laquelle).

Consommation

Conformément aux articles 39 et suivants de la loi n° 78-17 du 6 janvier 1978 modifiée en 2004 relatives à l'informatique, aux fichiers et aux libertés, toute personne peut obtenir communication et, le cas échéant, rectification ou suppression des informations la concernant, en s'adressant au service.....
 (Veuillez citer le nom du service auprès duquel il est possible d'exercer son droit d'accès).

Un clausier recensant des modèles de clauses pour un grand nombre de situations est disponible sur le site de la CNIL, à l'adresse suivante : <http://www.cnil.fr/vos-responsabilites/informations-legales/>

Quelles sont, en synthèse, les obligations qui incombent à un professionnel en application de la loi « informatique et libertés » ?

Nature de l'obligation	Fondement juridique	Sanction
Obligation de loyauté	Art. 6-1° de la loi « informatique et libertés »	Article 226-18 du code pénal
Obligation de proportionnalité	Art. 6-2°	Article 226-21 du code pénal
Obligation de définir une durée de conservation des données	Art. 6-5°	Article 226-20 du code pénal
Obligation d'assurer la sécurité et la confidentialité des données collectées	Art. 34	Article 226-17 du code pénal
Obligation de respecter l'exercice des droits que les personnes concernées tiennent de l'application de la loi « Informatique et Libertés »	Art. 32	Articles 226-18-1 et R. 625-10 à 12 du code pénal
Obligation d'encadrer les transferts de données en dehors de l'Union européenne	Art. 68	Article 226-22-1 du code pénal
Interdiction de principe de collecter certaines catégories particulières de données	Art. 8 et 9	Articles 226-16-1 et 226-19 du code pénal
Obligation de déclarer ses fichiers à la CNIL ou de désigner un correspondant à la protection des données	Art. 23 et s.	Article 226-16 du code pénal

→ → Annexes

ANNEXE I : les principaux textes de référence

I.1 Textes législatifs et réglementaires

Au niveau communautaire, la protection des données personnelles est essentiellement régie par la directive 95/46/CE du 24 octobre 1995 du Parlement européen et du Conseil 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.

En France, le texte essentiel est la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée par la loi n°2004-801 du 6 août 2004 transposant la directive précitée.

La loi n°2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique comporte également plusieurs dispositions protectrices des consommateurs. Elle a notamment introduit l'article L34-5 du Code des postes et des communications électroniques, qui exige le consentement préalable du consommateur avant toute prospection commerciale par voie électronique.

Vous pouvez consulter ces textes aux adresses suivantes :

La directive 95/46/CE du 24 octobre 1995 :

http://eurlex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=FR&numdoc=31995L0046&model=guichett

La loi n°78-17 du 6 janvier 1978 dite « informatique et libertés » :

<http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=LEGITEXT000006068624&dateTexte=20101229>

La loi n°2004-801 du 6 août 2004 :

<http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT00000441676>

La loi n°2004-575 du 21 juin 2004 :

<http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT00000801164>

Le décret n°2005-1309 du 20 octobre 2005 pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés :

<http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000241445>

I.2 Travaux du Conseil National de la Consommation

Avis du CNC du 18 mai 2010 sur la protection des données personnelles des consommateurs

http://www.minefi.gouv.fr/conseilnationalconsommation/avis/2010/180510protection_donnees_perso.pdf

I.3 Documents et travaux réalisés par la Commission européenne

http://ec.europa.eu/justice/policies/privacy/index_en.htm

ANNEXE II : les exemples de bonnes pratiques

Charte de l'emailing de l'UFMD – Code relatif à l'utilisation de coordonnées électroniques à des fins de prospection directe – validée par la CNIL

Ce code a pour objet de définir un certain nombre de règles déontologiques en matière de collecte et d'utilisation de coordonnées électroniques à des fins de prospection directe.

Il s'adresse plus particulièrement aux professionnels réalisant des opérations de prospection directe à caractère commercial. Sont donc exclues de son champ d'application les opérations de nature caritative, politique et associative.

Dans un premier temps, ce code vise plus spécifiquement la prospection directe par courrier électronique, étant précisé que les autres formes de coordonnées électroniques pourraient être intégrées dans le code à l'occasion de ses prochaines mises à jour.

Les règles présentées ci-après ont été définies par les organisations professionnelles réunies au sein de l'UFMD. Elles reposent sur des critères de transparence et de respect de la volonté des individus quant à l'utilisation de leurs données à caractère personnel, critères sur lesquels doit reposer toute activité de prospection directe légitime.

L'UFMD entend, à travers ce code, réaffirmer son attachement au respect des principes fondamentaux de la protection des données à caractère personnel, en matière de marketing direct et de prospection directe.

Le texte tient notamment compte de la loi pour la confiance dans l'économie numérique du 21 juin 2004 et de la loi Informatique et Libertés du 6 août 2004. L'UFMD s'engage à diffuser et à encourager le respect de ces règles par le plus grand nombre d'entreprises, notamment avec l'aide des organisations regroupées au sein de l'Union.

Retrouvez la Charte sous le lien suivant :

http://www.ufmd.org/telechar/code_ufmd_prospection_emailing.pdf

ANNEXE III : les outils mis à disposition par la CNIL

La CNIL met à disposition des particuliers et des entreprises des informations et outils sur son site

<http://www.cnil.fr/>

Vous y trouverez notamment :

- un rappel des obligations des entreprises ;
- la procédure et une aide à la déclaration de fichiers ;
- les modèles de mention CNIL ;
- des informations sur le transfert des données à l'étranger.

Y est également disponible une série de guide pour les entreprises (sécurité des données, transferts de données...) :

<http://www.cnil.fr/en-savoir-plus/guides/>

La CNIL met à disposition une permanence téléphonique de renseignement juridique (SORP - service d'orientation et de renseignement du public de la CNIL) disponible tous les jours, de 10h à 12h et de 14h à 16h, en composant le 01.53.73.22.22.

La CNIL propose enfin un outil d'autodiagnostic sécurité accessible depuis son site.

→ → Remerciements

Ce guide s'inscrit dans les travaux de la commission Consommation du MEDEF. Il a été rédigé par :

- Aurélie Bellamy, juriste, PSA PEUGEOT CITROEN
- Laura Boulet, directrice juridique, UDA
- Agnès Chatellier-Chamoulaud, juriste, BNPPARIBAS
- Françoise Costinesco, sous-directeur juridique, FFSA
- Léonard Cox, directeur de mission, MEDEF
- Guillaume Desgens Pasanau, avocat, ERNST & YOUNG
- Anne Fécamp, juriste, GDF SUEZ
- Laureline Frossard, juriste, UDA
- Marianne Kabelis, chargée d'études juridiques, FFSA
- Marc Lolivier, délégué général, FEVAD
- Nelly Mignotte, juriste, CCFA
- Jennifer Spittaël, stagiaire, MEDEF
- Nicolas Stoop, chargé de mission, MEDEF
- Fabienne Villars et Yannick Bailly, juristes, RENAULT
- Vanessa Younès-Fellous, juriste, SFR

Le MEDEF tient à remercier l'ensemble des personnes qui ont contribué à sa réalisation et en particulier les membres du groupe de projet Protection des données personnelles des consommateurs présidé par Marc Lolivier (FEVAD).

Mouvement des Entreprises de France
55 avenue Bosquet, 75330 Paris Cedex 07
www.medef.com

Contact : Nicolas Stoop
consommation@medef.fr
Tel. : + 33 (0)1 53 59 17 11

Dépôt légal : mars 2011

