

L'utilisation des données à caractère personnel *Use of personal data*

Sommaire

Introduction	4
Définitions	6
Champ d'application de la loi « Informatique et Libertés »	8
Principes relatifs à la qualité des données	8
Règles à respecter dans la collecte des données	10
Information de la personne concernée	12
Licéité des traitements	14
Conservation et mise à jour des données	14
Déclaration et demandes d'autorisation	16
Sous-traitance	16
Agir en tant que sous-traitant	18
Transfert des données à caractère personnel en dehors de l'UE	18
Marketing ciblé	20
Collecte des données de prospects	20
Sites Internet	22
Fichiers de marketing direct	26
Cookies	28
Prospection par automates d'appel	28
Prospection téléphonique (télémarketing)	30
Prospection par courrier électronique	30
Dissimulation d'identité	30
Sites Internet situés en dehors de l'UE	32
Messages électroniques adressés à des employés de sociétés	32
Informations obtenues dans le cadre de relations commerciales	34
Employés du responsable du traitement	34

Table of Contents

<i>Introduction</i>	5
<i>Définitions</i>	7
<i>Scope of the Data Protection and Privacy Act</i>	9
<i>Data Quality Principles</i>	9
<i>Data Collection Rules</i>	11
<i>Informing the data subject</i>	13
<i>Lawfulness of Data Processing</i>	15
<i>Preservation and updating of data</i>	15
<i>Declarations and requests for authorisation</i>	17
<i>Subcontracting</i>	17
<i>Acting as a Subcontractor</i>	19
<i>Transfer of personal data outside the EU</i>	19
<i>Direct marketing</i>	21
<i>Prospect Data Collection</i>	21
<i>Websites</i>	23
<i>Direct marketing files</i>	27
<i>Cookies</i>	29
<i>Prospecting via automated calls</i>	29
<i>Telephone prospecting</i>	31
<i>Email prospecting</i>	31
<i>Identity concealment</i>	31
<i>Websites located outside the EU</i>	33
<i>Emails to company employees</i>	33
<i>Information obtained in the course of commercial relationships</i>	35
<i>Data controller employees</i>	35

Introduction

La loi n°78-17 du 6 janvier 1978 dite loi « Informatique et Libertés » est en France le texte fondamental en matière de protection des données à caractère personnel. Le Décret n° 2005-1309 du 20 octobre 2005 vient compléter le dispositif.

La loi de 1978 a été amendée par la loi n°2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements à caractère personnel venue transposer la directive 95/46/EC du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

La Commission Nationale de l'Informatique et des Libertés (CNIL) est chargée de veiller au respect de la loi « Informatique et Libertés » qui lui confie cinq missions principales :

- informer et conseiller les responsables de traitements et les personnes concernées par les traitements de leurs droits et obligations ;
- garantir le droit d'accès des personnes concernées aux données contenues dans les traitements ;
- recenser les fichiers et accorder des autorisations aux traitements de données « à risque », donner un avis sur les traitements publics utilisant le numéro national d'identification des personnes, et recevoir les déclarations des autres traitements ;
- contrôler les traitements automatisés d'informations nominatives et vérifier leur conformité à la loi « Informatique et Libertés », et sanctionner les manquements ;
- réglementer par l'établissement de normes simplifiées ou de décisions d'autorisation unique permettant aux traitements les plus courants et les moins dangereux de faire l'objet de formalités allégées, ou de dispenses de déclarations dispensant de toute déclaration des catégories de traitement jugées sans risque pour les libertés individuelles.

Introduction

In France, the fundamental legislation for protection of personal data is Act no. 78-17 dated January 6 1978, referred to as the Data Protection and Privacy Act. Decree No. 2005-1309 dated October 20 2005 has since completed the statutory framework.

The 1978 Act was amended by Act No. 2004-801 dated August 6 2004 for protection of natural persons with regard to processing of personal data, which was introduced to implement directive 95/46/EC dated 24 October 1995 for protection of natural persons with regard to processing of personal data and free circulation of those data.

French data protection authority the Commission Nationale de l'Informatique and des Libertés (CNIL) is tasked with monitoring compliance with the Data Protection and Privacy Act, which gives it five main responsibilities:

- *to inform and advise controllers and data processing subjects of their rights and duties;*
- *to guarantee the right of access of data subjects to processed data;*
- *to inventory files and issue authorisations for processing "at-risk" data, issue notices with respect to public processing using an individual's national ID number, and receive declarations with respect to other processing;*
- *to oversee automatic processing of personal information, check compliance with the Data Protection and Privacy Act, and impose penalties for breaches;*
- *to regulate activity of this type, through simplified procedures or specific approvals allowing the most common, least dangerous kinds of processing to be carried out with reduced formality, or under waivers dispensing with the need for any declaration in the case of kinds of processing judged to pose no risk to individual liberty.*

Définitions

Afin de comprendre le fonctionnement pratique de la loi « Informatique et Libertés », il est nécessaire de clarifier certaines notions clés de ce texte.

- **Destinataire d'un traitement de données à caractère personnel** – le destinataire d'un traitement de données à caractère personnel est toute personne habilitée à recevoir communication de ces données autre que la personne concernée, le responsable du traitement, le sous-traitant et les personnes qui, en raison de leurs fonctions, sont chargées de traiter les données ;
- **Donnée à caractère personnel** – 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 ;
- **Donnée sensible** – constitue une donnée sensible toute information concernant l'origine raciale ou ethnique, les opinions politiques, philosophiques ou religieuses, l'appartenance syndicale, la santé ou la vie sexuelle. En principe, les données sensibles ne peuvent être recueillies et exploitées qu'avec le consentement explicite des personnes ;
- **Fichier de données à caractère personnel** – constitue un fichier de données à caractère personnel tout ensemble structuré et stable de données à caractère personnel accessibles selon des critères déterminés ;
- **Personne concernée par un traitement de données à caractère personnel** – la personne concernée par un traitement de données à caractère personnel est celle à laquelle se rapportent les données qui font l'objet du traitement ;
- **Responsable du traitement** – le responsable d'un traitement de données à caractère personnel est la personne, l'autorité publique, le service ou l'organisme qui détermine ses finalités et ses moyens ;
- **Traitement de données à caractère personnel** – constitue un traitement de données à caractère personnel toute opération ou tout ensemble d'opérations portant sur de telles données, quel que soit le procédé utilisé, et notamment la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction ;
- **Transfert de données** – constitue un transfert de données toute communication, copie ou déplacement de données à caractère personnel ayant vocation à être traitées dans un pays tiers à l'Union européenne.

Definitions

In order to understand the practical operation of the Data Protection and Privacy Act, some key concepts in the legislation need to be clarified.

- **Recipient of processed personal data** – “recipient of processed personal data” means any person empowered to receive the said data other than the data subject, the controller, the subcontractor or persons responsible for processing data by reason of their employment;
- **Personal data** – “personal data” means any information about a natural person identified or capable of being identified, directly or indirectly, by reference to an ID number or one or more features specific to him;
- **Sensitive data**– “sensitive data” means any information regarding racial or ethnic origin; political, philosophical or religious opinions; union membership; or health or sexuality. In principle, sensitive data may only be collected and used with a person’s express consent;
- **Personal data file** – “a personal data file” means any structured and stable suite of personal data accessible in accordance with specified criteria;
- **Subject of personal data processing** – “subject of personal data processing” means the person to whom the processed data relate;
- **Controller** –“controller” of personal data processing means the person, public body, department or organisation which determines its proposed use and the means of processing;
- **Personal data processing** – “personal data processing” means any operation or series of operations applied to such data, whatever method is employed, and in particular collection, recording, organisation, preservation, adaptation or modification, extraction, consultation, use, communication by transmission, broadcasting or any other means of providing access, reconciliation or interconnection, and locking, deletion or destruction;
- **Data Transfer** – “data transfer” means any communication, copy or movement of personal data intended to be processed in a country external to the European Union.

Champ d'application de la loi « Informatique et Libertés »

La loi « Informatique et Libertés » s'applique à toute personne agissant sur le territoire français en tant que responsable d'un traitement de données à caractère personnel. Lorsque la personne mettant en œuvre le traitement est établie sur le territoire français (notons qu'une personne pourra être regardée comme établie en France dans le cadre d'une installation ou d'un établissement, quelque soit sa forme juridique) ou que, sans être établie sur le territoire français ou sur celui d'un autre État membre de la Communauté européenne, elle recourt à des moyens de traitement situés sur le territoire français (à l'exclusion des traitements qui ne sont utilisés qu'à des fins de transit sur ce territoire ou sur celui d'un autre État membre de la Communauté européenne), la loi « Informatique et Libertés » aura vocation à s'appliquer.

Principes relatifs à la qualité des données

La loi « Informatique et Libertés » prévoit cinq principes relatifs à la qualité des données devant être respectés par le responsable du traitement.

Traitement loyal et licite

Les données à caractère personnel doivent être collectées et traitées de manière loyale et licite, et doivent respecter les conditions de licéité des traitements de données (voir paragraphe « Conditions de licéité des traitements de données » ci-après). Pour déterminer si une donnée est collectée de manière loyale, il est tenu compte de la méthode utilisée pour la collecte, ce qui implique de déterminer si la personne concernée a été trompée ou induite en erreur s'agissant des finalités pour lesquelles les données ont été collectées. Par ailleurs, une donnée pourra être regardée comme ayant été traitée de manière non loyale si les personnes concernées n'ont pas été dûment informées au moment de la collecte des données (voir paragraphe « Information de la personne concernée » ci-après).

Finalités déterminées, explicites et légitimes

Les données à caractère personnel doivent être collectées par le responsable du traitement pour une ou plusieurs finalité(s) déterminée(s), explicite(s) et légitime(s), et ne doivent pas être traitées d'une manière incompatible avec cette (ces) finalité(s). Les finalités des traitements ultérieurs à la collecte ne peuvent pas être incompatibles avec les finalités spécifiées à l'origine. Les finalités légitimes sont celles portées à la connaissance de la personne concernée (conformément à l'exigence d'information mentionnée ci-après), ou celles mentionnées dans la déclaration préalable faite par le responsable du traitement auprès de la CNIL.

Adéquates, pertinentes et non excessives

Toute donnée à caractère personnel traitée par le responsable du traitement doit être adéquate, pertinente et non excessive eu égard aux finalités de la collecte et du ou des traitements ultérieurs.

Exactes, complètes et mises à jour

Les données à caractère personnel doivent être exactes, complètes et, si nécessaire, mises à jour. Le responsable du traitement a l'obligation de prendre toutes les mesures appropriées pour que les données inexactes ou incomplètes, eu égard aux finalités pour lesquelles elles sont collectées ou traitées, soient effacées ou rectifiées.

Conservées pendant une durée n'excédant pas la durée nécessaire aux finalités

Les données à caractère personnel collectées pour une ou plusieurs finalités déterminées ne doivent pas être conservées au-delà de la durée nécessaire aux finalités pour lesquelles elles ont été collectées et traitées.

Scope of the Data Protection and Privacy Act

The Data Protection and Privacy Act applies to any person acting as a controller of personal data processing in French territory. The Data Protection and Privacy Act will be applicable where the person performing the processing is based in French territory (note that a person may be considered to be based in France in the form of a facility or branch, whatever legal form it may take) or, not being in French territory or the territory of another European Union Member State, uses a means of processing located in French territory (excluding processing which is only used for transit within that territory or the territory of another European Union Member State).

Data Quality Principles

The Data Protection and Privacy Act sets out five data quality principles which must be observed by the controller.

Fair and Lawful Processing

Personal data must be collected and processed fairly and lawfully, and must comply with the conditions governing the lawfulness of data processing (see the paragraph on lawfulness of data processing below). To determine whether a data item is collected fairly, the collection method used is taken into account, which entails determining whether the data subject has been deceived or misled with respect to the end use for which the data have been collected. Moreover, a data item may be regarded as not having been fairly processed if data subjects have not been properly informed at the time of the data collection (see the paragraph on informing the data subject below).

Specific, Express and Legitimate Purposes

Personal data must be collected by the controller for one or more specific, express and legitimate purposes, and must not be processed in a way that is incompatible with the said purpose(s). Post-collection processing must not be incompatible with the purposes originally specified. Legitimate purposes are those which are brought to the data subject's attention (in accordance with the information requirement referred to below), or those referred to in the prior declaration made to CNIL by the controller

Appropriate, Relevant and not Excessive

Any personal data processed by the controller must be appropriate, relevant and not excessive in the light of the purposes of collection and subsequent processing.

Correct, Complete and Up to Date

Personal data must be correct, complete and, if necessary, updated.

The controller has a duty to take all appropriate steps to see that data which are incorrect or incomplete in light of the purposes for which they are collected or processed, are erased or corrected.

Preserved no longer than is necessary for their purpose

Personal data collected for one or more pre-determined purposes must not be preserved beyond the period necessary for the purposes for which they were collected and processed.

Règles à respecter dans la collecte des données

Le responsable du traitement doit s'assurer que la personne concernée a donné son consentement préalable au traitement. Un tel consentement peut être simple ou exprès mais il doit être dépourvu d'ambiguïté, en relation avec le traitement concerné, et être obtenu de manière loyale et libre. En d'autres termes, la personne concernée doit avoir pleinement conscience de ce à quoi elle consent, et dans une certaine mesure, des implications de son consentement.

Par exception, le consentement de la personne concernée peut ne pas être recueilli, quand le traitement satisfait à l'une des conditions suivantes :

- Le traitement est nécessaire au respect par le responsable du traitement d'une obligation légale à laquelle il est soumis ;
- Le traitement est nécessaire à la sauvegarde de l'intérêt vital de la personne concernée ;
- Le traitement est nécessaire à l'exécution d'une mission de service public dont est investi le responsable ou son destinataire ;
- Le traitement est nécessaire :
 - à l'exécution d'un contrat auquel la personne concernée est partie ; ou
 - à l'exécution de mesures précontractuelles prises à la demande de la personne concernée (par exemple, estimer un risque avant de conclure un contrat d'assurance) ;
- Le traitement est nécessaire à 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.

S'agissant des données sensibles, il est interdit par principe de les collecter ou de les traiter. Toutefois, par exception, et dans la mesure où la finalité du traitement l'exige, l'interdiction peut être levée à condition que l'une des conditions suivantes soit remplie :

- La personne concernée a donné son consentement exprès au traitement de ses données à caractère personnel. Une fois encore, un tel consentement doit être spécifiquement en rapport avec la finalité concernée, être dépourvu d'ambiguïté, préalable, donné librement et en connaissance de cause. Dans cette hypothèse, le consentement ne peut pas être implicite. Il doit être explicite, mais pas nécessairement donné par écrit (bien qu'en pratique, d'un point de vue probatoire, l'écrit semble bien nécessaire.). En raison du caractère sensible des données, il est essentiel que la personne concernée soit pleinement informée des implications consécutives à la communication des données à caractère personnel concernées.
- Le traitement est nécessaire à la sauvegarde de la vie humaine, mais la personne concernée ne peut donner son consentement par suite d'une incapacité juridique ou d'une impossibilité matérielle.
- Le traitement est mis en œuvre par une association ou tout autre organisme à but non lucratif et à caractère religieux, philosophique, politique ou syndical :
 - pour des données sensibles correspondant à l'objet de ladite association ou dudit organisme ;
 - sous réserve qu'il ne concerne que les membres de cette association ou de cet organisme et, le cas échéant, les personnes qui entretiennent avec celui-ci des contacts réguliers dans le cadre de son activité ;

Data Collection Rules

The controller must satisfy himself that the data subject has given his prior consent to processing. Such consent may be simple or express but must be free of ambiguity, must relate to the processing in question, and must be obtained fairly and freely. In other words, the data subject must be fully aware of what he is consenting to, and to some extent the implications of his consent.

Exceptionally, the data subject's consent need not be obtained when processing meets one of the following conditions:

- *The processing is necessary for the controller's compliance with a legal duty to which he is subject;*
- *The processing is necessary for protecting the data subject's vital interests;*
- *The processing is necessary for performance of a public service assignment to be performed by the controller or his recipient;*
- *The processing is necessary for:*
 - *performance of a contract to which the data subject is a party; or*
 - *performance of precontractual steps at the data subject's request (for instance, assessing a risk before taking out an insurance policy);*
- *The processing is necessary for achieving a legitimate interest pursued by the processing controller or the data recipient, provided that the interests and fundamental rights and liberties of the data subject are respected.*

In principle, the collection and processing of sensitive data is prohibited. Exceptionally, however, insofar as the purpose of the processing requires it, the prohibition may be removed where one of the following conditions is met:

- *The data subject has given his express consent to processing of his personal data. Once again, such consent must specifically relate to the purpose in question, be free of ambiguity, be given in advance, and be given freely and with full knowledge of the facts.
*In those circumstances consent may not be implied. It must be express, but not necessarily in writing (although in practice, from an evidential point of view, written consent would appear to be essential). Because of the sensitive nature of data, it is essential that the data subject should be fully informed of the implications flowing from communication of the personal data in question.**
- *The processing is necessary for protection of human life, but the data subject cannot give consent because of legal incapacity or practical impossibility.*
- *The processing is conducted by a not-for-profit organisation of a religious, philosophical or political character, or in the nature of a trade union and:*
 - *the sensitive data relates to the aims of that organisation;*
 - *it only concerns members of the said association or body and, where relevant, persons in regular contact with the same in the course of its activity; and*
 - *it only involves data which are not disclosed to third parties, unless the data subjects expressly consent thereto.*
- *The processing involves personal data made public by the data subject.*
- *The processing is necessary to establish, exercise or defend a legal right.*

- et qu'il ne porte que sur des données non communiquées à des tiers, à moins que les personnes concernées n'y consentent expressément.

- Le traitement porte sur des données à caractère personnel rendues publiques par la personne concernée.
- Le traitement est nécessaire à la constatation, à l'exercice ou à la défense d'un droit en justice.
- Le traitement est nécessaire aux fins de la médecine préventive, des diagnostics médicaux, de l'administration de soins ou de traitements, ou de la gestion de services de santé et mis en œuvre par un membre d'une profession de santé, ou par une autre personne à laquelle s'impose en raison de ses fonctions l'obligation de secret professionnel prévue par l'article 226-13 du Code pénal.
- Le traitement concerné est un traitement statistique réalisé par l'Institut national de la statistique et des études économiques ou l'un des services statistiques ministériels dans le respect de la loi n° 51-711 du 7 juin 1951 sur l'obligation, la coordination et le secret en matière de statistiques, après avis du Conseil national de l'information statistique. Ce type de traitement est soumis à l'autorisation de la CNIL.
- Le traitement est nécessaire à la recherche dans le domaine de la santé selon les modalités prévues au chapitre IX de la loi « Informatique et Libertés ».
- Les données à caractère personnel sensibles sont appelées à faire l'objet à bref délai d'un procédé d'anonymisation. Toutefois, il est nécessaire que la CNIL ait préalablement reconnu conforme le procédé aux dispositions de la loi « Informatique et Libertés », et qu'elle ait autorisé, tenu de sa finalité, la catégorie de traitement concerné.
- Le traitement est justifié par l'intérêt public et autorisé par la CNIL.

Information de la personne concernée

Comme cela a été mentionné ci-dessus, pour que le traitement des données soit licite, le responsable du traitement a, dans la plupart des cas, l'obligation de fournir à la personne concernée des informations concernant le traitement mis en œuvre.

Lorsque les données sont collectées directement auprès de la personne concernée, le responsable du traitement doit informer la personne concernée au moment de la collecte des données. Lorsque les données à caractère personnel sont collectées auprès de tiers, les informations doivent être fournies 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.

Les informations devant être fournies sont l'identité du responsable du traitement (et, le cas échéant, celle de son représentant), la ou les finalités poursuivies par le traitement auquel les données sont destinées, le caractère obligatoire ou facultatif des réponses, les conséquences éventuelles d'un défaut de réponse, les destinataires ou catégories de destinataires des données, les droits d'opposition, d'accès et de rectification de la personne concernée, et, le cas échéant, les transferts de données à caractère personnel envisagés à destination d'un État non membre de l'Espace Économique Européen. S'agissant de certains types de traitement, telle que la collecte de données sur Internet et, dernièrement, les plans de continuation d'activité mis en place en prévision d'une pandémie grippale, la CNIL a publié des modèles de mentions d'information.

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

- *The processing is necessary for the purposes of preventive medicine, medical diagnosis, or treatment, or management of health services and action by a health professional or any other person whose duties render him subject to the professional confidentiality prescribed in article 226-13 of the Penal Code.*
- *The processing in question is statistical processing carried out by the French national institute of statistics and economic studies, or one of the ministerial statistics departments pursuant to Act No. 51-711 dated June 7 1951 regarding obligations, coordination and confidentiality relating to statistics, after approval by the French national council for statistical information. This type of processing is subject to CNIL's authorisation.*
- *The processing is necessary for health research in accordance with the terms set out in Chapter IX of the Data Protection and Privacy Act.*
- *Sensitive personal data must quickly be anonymised. However, CNIL must first have recognised the process as being in compliance with the provisions of the Data Protection and Privacy Act, and must have authorised the category of processing in question in the light of its purpose.*
- *The processing is justified as being in the public interest and authorised by CNIL.*

Informing the data subject

As stated above, for data processing to be lawful the processing controller is in most cases under a duty to supply the data subject with information about the processing being carried out.

When data are collected directly from the data subject, the processing controller must advise the data subject at the time of data collection. When personal data are collected from third parties, the information must be supplied at the time the data is recorded or, if it is intended to communicate the data to other parties, no later than the time of the first such communication.

The information to be supplied is the controller's identity (and where relevant that of his representative), the purpose(s) of the processing which the data are to undergo, whether responses are mandatory or optional, the possible consequences of not responding, the recipients or categories of recipients of data, the data subject's rights to object, access data and correct data, and, where relevant, intended transfers of personal data outside the European Economic Area. CNIL has published model information notices for some types of processing, such as collection of data on the internet and, recently, activity continuation plans put in place in anticipation of a flu pandemic.

The duty to inform does not apply where the data subject is already aware of the processing or when his information proves to be irretrievable or requires disproportionate effort in relation to the benefit to be gained from the procedure.

The Data Protection and Privacy Act does not define what would constitute a "disproportionate effort". However, account must be taken of the consequences for the data subject of data processing, which includes any material or non-pecuniary loss capable of arising from the processing. The nature of the data processed must be taken into account, as must the purpose of the processing to be carried out. The cost and financial burden which would be occasioned by the information procedure must also be assessed. Hence, if data are not sensitive, if it is unlikely that the processing would cause any material or non-pecuniary loss to the data subject, and if the supply of information would give rise to considerable cost and financial strain for the controller, then it would be possible to resort to the exception. Nevertheless, note that this exception must be interpreted strictly.

La loi « Informatique et Libertés » ne définit pas ce que constituerait un « effort disproportionné ». Cependant, il doit être tenu compte des conséquences du traitement sur la personne concernée, ce qui inclut tout dommage matériel ou moral susceptible de résulter du traitement. La nature des données traitées doit être prise en compte, de même que la finalité du traitement à intervenir. Le coût et les efforts financiers qui seraient générés par les mesures d'information devront être estimés. Dès lors, si les données ne sont pas des données sensibles, qu'il est peu probable que le traitement cause quelque dommage matériel ou moral à la personne concernée, et si la fourniture des informations engendrerait un coût et un effort financier considérables pour le responsable du traitement, alors il serait possible de se prévaloir de l'exception. Notons néanmoins que cette exception devra être interprétée strictement.

Licéité des traitements

Outre l'exigence de loyauté, les traitements doivent être licites. Cette notion de licéité doit être entendue largement. Il est possible en effet qu'au delà des exigences de la loi « Informatique et Libertés », le responsable du traitement ou le sous-traitant doivent se conformer à d'autres règles pour s'assurer la licéité du traitement. Ainsi, le transfert de données vers les États-Unis dans le cadre d'une procédure de « discovery » ne peut s'opérer que conformément à la Convention de La Haye. De même, un traitement ne pourra être regardé comme licite que si les obligations de confidentialité sont respectées. Ces obligations peuvent résulter d'engagements spécifiques pris à l'égard des personnes, consister dans une obligation implicite induite des circonstances dans lesquelles l'information a été initialement communiquée, ou dans une obligation résultant de circonstances postérieures à la communication et acceptée par le responsable. Des dispositions légales ou réglementaires peuvent également venir imposer une telle confidentialité.

Le responsable devra en toute hypothèse limiter le traitement des données en tenant compte des obligations de confidentialité dont il est débiteur à l'égard des personnes concernées. Ainsi, lorsqu'une information sera communiquée à une société dans le cadre d'un service déterminé, il pourra être déduit des circonstances de cette communication que la société s'interdit d'utiliser la même information pour une finalité autre que celle déterminée par le service concerné. Dans ces circonstances, l'obligation de confidentialité interdira à la société d'utiliser cette information à des fins différentes de celles pour lesquelles elle a initialement obtenu l'information.

Conservation et mise à jour des données

La loi « Informatique et Libertés » interdit que les données soient conservées pour des durées excessives compte tenu de la finalité de leur traitement. Les données doivent être régulièrement mises à jour, détruites lorsqu'elles deviennent obsolètes ou inutiles, et la CNIL a publié diverses recommandations concernant les durées et modalités de conservation et d'archivage des données.

A titre d'exemple, les données collectées et utilisées à des fins de marketing posent souvent la question de savoir combien de temps ces informations peuvent être utilisées à cette fin. Il est inévitable que les données deviennent incorrectes avec le temps et cette obsolescence doit être prise en compte dans le contexte des obligations incombant au responsable du traitement d'assurer que les données concernées sont à jour, exactes et appropriées. La règle générale ci-dessus rappelée a vocation à s'appliquer, les données ne peuvent être conservées au-delà de la durée nécessaire à la réalisation des finalités du traitement. Sauf circonstances particulières justifiant une conservation plus longue, la CNIL recommande que les données collectées à des fins de prospection soient supprimées au maximum un an après le dernier contact avec la personne concernée ou lorsque celle-ci n'a pas répondu à deux sollicitations successives.

Lawfulness of Data Processing

Beside the fairness requirement, processing must be lawful. The concept of lawfulness must be understood broadly. In fact it may be that beyond the prescriptions of the Data Protection and Privacy Act, the controller or the subcontractor must comply with further rules to satisfy himself of the lawfulness of the processing. Thus transfer of data to the United States pursuant to a discovery procedure may only be done in accordance with the Hague Convention. Similarly, processing may only be regarded as lawful if confidentiality obligations are observed. The said obligations may arise from specific undertakings to individuals, or consist of an obligation implied from the circumstances in which information was initially passed on, or an obligation resulting from circumstances arising subsequently and accepted by the controller. Statutory or regulatory provisions may likewise impose such confidentiality.

At all events, the controller must limit the processing of data with reference to confidentiality obligations he owes to data subjects. Hence, when information is given to a company in connection with a particular service, it may be inferred from the circumstances of that disclosure that the company agrees not to use the information for a purpose other than that relating to the service in question. In those circumstances, the confidentiality obligation will prevent the company from using the information for different purposes than those for which it initially obtained the information.

Preservation and updating of data

The Data Protection and Privacy Act prohibits preservation of data for periods of time that are excessive in relation to the purpose for their processing. Data must be regularly updated and destroyed when they become obsolete or useless, and CNIL has published various recommendations with respect to time limits and means of preserving and archiving data.

For instance, data collected and used for marketing purposes often raise the question of the amount of time for which information may be used for that purpose. It is inevitable that data become incorrect over time and that obsolescence must be taken into account in the context of the controller's duties to ensure that the data in question are current, correct and appropriate. The general rule referred to above is applicable and data may not be preserved beyond the time necessary to achieve the purposes of processing. In the absence of special circumstances justifying longer preservation, CNIL recommends that data collected for prospecting purposes be deleted a maximum of one year after the last contact with the data subject, or when the data subject has not replied to two successive requests.

Déclarations et demandes d'autorisation

Les traitements de données nominatives doivent préalablement à leur mise en œuvre, faire l'objet d'une déclaration ou d'une demande d'autorisation auprès de la CNIL.

La CNIL a publié certaines dispenses de formalités qui concernent les traitements les moins susceptibles de porter atteinte aux droits des individus.

La CNIL a également publié des normes simplifiées concernant les traitements les plus courants de données nominatives. Si le traitement mis en œuvre par le responsable du traitement est conforme à une norme simplifiée publiée par la CNIL, le responsable pourra procéder à une simple déclaration de conformité à la norme concernée.

Si le traitement diffère des termes de la norme simplifiée, le responsable procèdera à une déclaration dite « normale » de son traitement.

Dans l'hypothèse où le traitement est susceptible de porter atteinte à certain droits des individus, une autorisation expresse de la CNIL devra être obtenue avant que le traitement puisse être mis en œuvre.

Notons que la désignation d'un correspondant Informatique et Libertés dispense le responsable des formalités de déclaration simplifiée et de déclaration normale.

Sous-traitance

Est considérée comme sous-traitant au sens de la loi « Informatique et Libertés » toute personne traitant des données à caractère personnel pour le compte du responsable du traitement.

Le recours à la sous-traitance impose certaines obligations au responsable du traitement visant à garantir que le traitement concerné continue à être loyal et licite, et plus généralement conforme à la loi « Informatique et Libertés ».

Le responsable du traitement doit toujours veiller à ce que l'exigence de sécurité soit respectée dans le cadre du traitement des données. Il doit dès lors choisir un sous-traitant présentant des garanties suffisantes pour assurer la mise en œuvre des mesures de sécurité et de confidentialité exigées par la loi « Informatique et Libertés ».

La désignation d'un sous-traitant doit obligatoirement être faite par le biais d'un contrat. Celui-ci doit comporter l'indication des obligations incombant au sous-traitant en matière de protection de la sécurité et de la confidentialité des données et prévoir que le sous-traitant ne peut agir que sur instruction du responsable du traitement. Par ailleurs, le responsable du traitement doit veiller à choisir un sous-traitant capable de se conformer à ces exigences, et 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. Le responsable doit s'assurer de pouvoir démontrer, en cas de mise en cause ultérieure, qu'il a mis en œuvre un contrôle approprié des mesures de sécurité et de confidentialité mises en place par le sous-traitant. Le contrat de sous-traitance devra donc prévoir des clauses d'audit.

Le contrat doit également prévoir que le sous-traitant 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.

Declarations and requests for authorisation

A declaration or a request for authorisation must be made to CNIL, in advance, in respect of any processing of personal data.

CNIL has published some dispensations from formalities for the types of data processing which are least likely to infringe the rights of individuals.

Likewise, CNIL has published simplified standards for the most common types of processing of individual data. If the processing performed by the controller complies with the simplified standard published by CNIL, the controller may make a simple declaration of compliance with the standard in question.

If the processing departs from the terms of the simplified standard, the controller will make a "standard" declaration in respect of it.

In the event that the processing is capable of infringing certain individual rights, express authorisation by CNIL must be obtained before processing can be performed.

Note that the appointment of a data protection and privacy officer relieves the controller of the formal requirements for a simplified declaration and standard declaration.

Subcontracting

Any person processing personal data on behalf of the controller is deemed to be a subcontractor within the meaning of the Data Protection and Privacy Act.

Subcontracting imposes certain obligations on the controller to ensure that the processing in question continues to be fair and lawful, and more generally complies with the Data Protection and Privacy Act.

The controller must be ever-vigilant to see that security requirements are observed in the course of processing data. Thus, he must select a subcontractor who can offer safeguards which are adequate to ensure implementation of security and confidentiality processes prescribed by the Data Protection and Privacy Act.

It is mandatory for a subcontractor (in the wide sense above) to be appointed by means of a contract. The contract must include the subcontractor's duties with respect to protection of the security and confidentiality of data and provide that the subcontractor may only act on the controller's instructions. Moreover, the controller must take care to select a subcontractor able to comply with those requirements, and is obliged to take all precautions appropriate to the nature of the data and the risks occasioned by the processing to preserve the security of data.

The controller must satisfy himself that in the event of a subsequent challenge he can demonstrate that he has implemented an appropriate audit of the security and confidentiality processes established by the subcontractor. Thus the subcontract must contain audit clauses.

Likewise, the contract must provide that the subcontractor is obliged to take all proper precautions having regard to the nature of the data and the risks presented by the processing, so as to maintain the security of the data and, in particular, prevent it from being corrupted or damaged, or accessed by unauthorised third parties.

Enfin, le responsable du traitement doit s'assurer que son propre sous-traitant ne sous-traite pas à son tour tout ou partie de ses obligations à un tiers n'assurant pas une sécurité suffisante aux données ou simplement localisé dans un État n'assurant pas un niveau adéquat de protection des données personnelles.

Agir en tant que sous-traitant

Dans certains contrats, il peut s'avérer délicat de déterminer si une personne agit en tant que responsable du traitement ou sous-traitant. Il est cependant indispensable d'établir la nature exacte des relations contractuelles pour s'assurer leur conformité avec la loi « Informatique et Libertés ». Si une personne agit en tant que sous-traitant, elle ne sera pas en principe responsable en application de la loi « Informatique et Libertés » et sera dispensée de ce fait de toute formalité de déclaration ou de demande d'autorisation auprès de la CNIL. Sa responsabilité sera déterminée contractuellement dans le cadre de l'acte conclu avec le responsable du traitement. Il est cependant important d'observer que si une société traite des données à caractère personnel et est dans une situation de contrôle des finalités et des moyens du traitement de ces données, alors cette société sera considérée comme responsable du traitement et sera soumise à toute la rigueur imposée par la loi « Informatique et Libertés », et indépendamment du point de savoir si un tiers dispose corrélativement d'un pouvoir de contrôle similaire.

Transfert des données à caractère personnel en dehors de l'UE

La loi « Informatique et Libertés » prévoit expressément que les données à caractère personnel ne peuvent pas être transférées en dehors de l'Espace Economique Européen, à moins que l'État destinataire assure un niveau adéquat de protection de la vie privée et des libertés et droits fondamentaux des personnes à l'égard du traitement dont les données font ou peuvent faire l'objet.

Le caractère suffisant du niveau de protection assuré par un État est apprécié par la Commission Européenne qui publie une liste des États n'assurant pas un niveau adéquat, parmi lesquels figurent notamment les États-Unis. Le transfert de données vers cette catégorie d'États est par principe interdit.

Toutefois, le responsable d'un traitement peut transférer des données à caractère personnel vers un État ne présentant pas un caractère suffisant du niveau de protection si la personne concernée a consenti expressément à leur transfert ou si le transfert est nécessaire :

- à la sauvegarde de la vie de cette personne ;
- à la sauvegarde de l'intérêt public ;
- au respect d'obligations permettant d'assurer la constatation, l'exercice ou la défense d'un droit en justice ;
- à la consultation, dans des conditions régulières, d'un registre public qui, en vertu de dispositions législatives ou réglementaires, est destiné à l'information du public et est ouvert à la consultation de celui-ci ou de toute personne justifiant d'un intérêt légitime ;
- à l'exécution d'un contrat entre le responsable du traitement et l'intéressé, ou de mesures précontractuelles prises à la demande de celui-ci ;

Finally, the controller must satisfy himself that his own subcontractor will not subcontract in turn all or part of his obligations to a third party which does not provide adequate security for data, or which is simply located in a state that does not ensure a proper level of protection for personal data.

Acting as a Subcontractor

In some contracts, it may prove to be a delicate matter to determine whether a person is acting as a data controller or a subcontractor. However, it is imperative to establish the precise nature of the contractual relationship, in order to establish compliance with the Data Protection and Privacy Act. If a person acts as a subcontractor, he will not in principle be a controller under the Data Protection and Privacy Act, and will thereby be relieved of any formal requirements as to declarations or requests for CNIL's authorisation. His liability will be determined contractually under the agreement with the controller. However, it is important to note that if a company processes personal data and is in a position to control the purposes and means of processing such data, that company will be deemed to be a controller and will be subject to the full rigour of the Data Protection and Privacy Act, irrespective of whether a third party has concomitant and similar control.

Transfer of personal data outside the EU

The Data Protection and Privacy Act expressly provides that personal data may not be transferred outside the European Economic Area, unless the receiving state provides an adequate level of protection of privacy and fundamental personal rights and freedoms with respect to processing to which the data are or may be subject.

The adequacy of the level of protection provided by a state is evaluated by the European Commission, which publishes a list of states which do not provide the proper level, the United States being among them. In principle, data transfer to this category of states is prohibited.

However, a processing controller may transfer personal data to a state which does not have a sufficient level of protection if the data subject has expressly consented to their transfer, or if the transfer is necessary for:

- protecting the life of the person;
- protection of the public interest;
- compliance with obligations designed to ensure that a legal right can be established, exercised or defended;
- consultation in proper circumstances of a public record which by reason of statutory or regulatory provisions is intended for public information and is open to consultation by the public or any person demonstrating a legitimate interest;
- performance of a contract between the controller and the party concerned, or precontractual steps taken at the request of the said party;
- formation or performance of a contract in the data subject's interest made or to be made between the controller and a third party.

In the last-mentioned situation it is advisable to use standard contractual clauses issued by the European Commission and available on the CNIL website, in order to bind either the controller or the subcontractor receiving the data to obligations regarding respect for privacy and protection of personal data. If the transfer occurs within a group of companies, they may choose to adopt binding corporate rules.

- à la conclusion ou à l'exécution d'un contrat conclu ou à conclure, dans l'intérêt de la personne concernée, entre le responsable du traitement et un tiers.

S'agissant de la dernière condition, il est conseillé d'utiliser les clauses contractuelles types émises par la Commission européenne, et consultables sur le site de la CNIL, afin d'imposer soit au responsable du traitement, soit au sous-traitant destinataire des données, des obligations en matière de respect de la vie privée et de protection des données à caractère personnel. Si le transfert intervient au sein d'un groupe de sociétés, celles-ci peuvent choisir de conclure des « règles contraignantes internes » ou « binding corporate rules ».

Marketing ciblé

Le marketing ciblé est défini par le Code de déontologie européen en matière d'utilisation de données à caractère personnel dans le marketing direct de la Fédération Européenne de Marketing direct (FEDMA) comme « la communication par quel moyen que ce soit (comprenant de manière non limitative le courrier, la télécopie, le téléphone, les services en ligne, etc.) de toute offre de publicité ou marketing, qui est réalisée par le professionnel même ou sous sa responsabilité et qui s'adresse à des particuliers ».

C'est une définition large qui englobe les courriers postaux, les télécopies, les courriers électroniques, et les SMS-MMS envoyés à des fins marketing à des personnes physiques. Le marketing ciblé comprend également toute promotion des mérites d'une organisation déterminée.

Conformément à l'article 38 de la loi « Informatique et Libertés », toute personne physique a le droit de s'opposer, sans frais, à ce que les données la concernant soient utilisées à des fins de prospection, notamment commerciale, par le responsable du traitement ou un cessionnaire ultérieur. Si le responsable n'accède pas à la demande de la personne concernée, cette dernière pourra saisir la CNIL d'une plainte. La CNIL a d'ores et déjà sanctionné un responsable de traitement ayant refusé à une personne physique, sans raisons légitimes, de lui donner accès aux données la concernant.

Collecte des données de prospects

Les traitements de données de prospects doivent en principe être déclarés auprès de la CNIL selon les modalités de déclaration normale.

Néanmoins, la CNIL a adopté une norme simplifiée relative à la gestion de fichiers de clients et prospects (norme simplifiée n°48). Entre dans le champ de la norme tout traitement automatisé relatif à la gestion des fichiers de clients et de prospects. Cette norme permet aux responsables de traitements d'effectuer une déclaration simplifiée, dans le respect des conditions qu'elle précise, pour les traitements relatifs aux personnes avec lesquelles des relations contractuelles ont été nouées, les clients, et les clients potentiels, simples prospects, à l'exclusion de ceux mis en œuvre par les établissements bancaires ou assimilés, les entreprises d'assurances, de santé et d'éducation. Pour bénéficier de la procédure de déclaration simplifiée, le traitement doit répondre aux conditions fixées par la norme s'agissant des finalités des traitements, des données susceptibles d'être traitées, des destinataires et des personnes habilitées à traiter les données, de la durée de conservation des données, de l'information des personnes concernées, des précautions prises pour préserver la sécurité des données ou encore des conditions dans lesquelles les données seront éventuellement transférées.

Tout traitement ne se conformant pas strictement aux dispositions de la norme ne peut faire l'objet d'une déclaration simplifiée de conformité à la norme. Le cas échéant, une déclaration normale sera nécessaire.

Direct marketing

Direct marketing is defined by the Federation of European Direct and Interactive Marketing (FEDMA), in its European code of practice for the use of personal data in direct marketing, as “the communication by whatever means (including but not limited to mail, fax, telephone, on-line services etc...) of any advertising or marketing material, which is carried out by the Direct Marketer itself or on its behalf and which is directed to particular individuals”.

This is a wide definition that encompasses postal mail, faxes, electronic mail and SMS/MMS, sent for the purposes of marketing to natural persons. Direct marketing also includes any promotion of the qualities of a specific organisation.

Under Article 38 of the Data Protection and Privacy Act, any natural person has the right to object, at no cost, to the use of any data concerning him for the purposes of prospecting, in particular commercial prospecting, by the data controller or by a subsequent transferee. If the person responsible does not comply with the request of the person concerned, the latter can submit a complaint to the CNIL.

The CNIL has already imposed sanctions on a data controller who refused, without legitimate grounds, to give a natural person access to data concerning him.

Prospect Data Collection

In principle, the processing of prospect data must be declared to the CNIL in the normal way.

However, the CNIL has adopted a simplified code of practice for managing the files of clients and prospects (simplified code of practice no 48). Included in this category will be any automated processing in respect of such files. This code of practice allows data controllers, in specified circumstances, to make a simplified declaration in respect of processing for those with whom contractual relationships have been established, clients and potential clients, and mere prospects (excluding of those of banking or similar institutions, insurance, health and educational bodies).

To benefit from the simplified declaration procedure, the processing must comply with the conditions stipulated by the code of practice in respect of the purposes of the processing, the type of data to be processed, recipients and those entitled to process the data, the length of time for which the data may be retained, the information given to data subjects, the precautions taken to ensure security of the data, and the circumstances in which the data may be transferred.

A simplified declaration of conformity may not be made in respect of any processing that does not strictly conform to the code. In such a case, a normal declaration will be required.

Sites Internet

Les principes mentionnés ci-dessus s'appliquent quel que soit le moyen de collecte utilisé par le responsable du traitement. La collecte par le biais d'un site Internet appelle cependant, certaines observations spécifiques.

- Il est nécessaire de conserver à l'esprit que les visiteurs d'un site peuvent y accéder par d'autres pages que la page d'accueil. Les liens hypertextes permettent aux utilisateurs d'accéder aux différentes pages d'un site. Il est dès lors important de s'assurer que les mentions obligatoires sont accessibles depuis chaque page du site sur lequel les données à caractère personnel sont susceptibles d'être collectées.
- S'agissant d'un même site Internet, plusieurs responsables du traitement peuvent être identifiés. Il est possible que dans le cadre d'un contrat d'hébergement, une société ait accès à des données à caractère personnel pour sa campagne publicitaire en ligne. En bénéficiant d'un tel accès, la société sera souvent considérée comme responsable du traitement des données concernées. Certaines informations peuvent également être communiquées à un tiers responsable du traitement ; par exemple au fournisseur d'un système sécurisé de paiement en ligne mis en place sur le site concerné. Une fois encore, ces observations concernent à la fois les dispositions contractuelles liant le responsable du traitement au tiers concerné, et avec les mentions d'information devant être présentes sur le site. Lorsqu'une personne a recours à des services d'hébergement, le fournisseur sera considéré comme un sous-traitant et l'accord avec le sous-traitant devra contenir les mentions requises par la loi « Informatique et Libertés ». (voir paragraphe « Sous-traitance » ci-dessus).
- Lorsque les données sont utilisées ou communiquées à des fins de marketing ciblé, les personnes concernées doivent avoir été mises en mesure de s'opposer à une telle utilisation. Depuis la loi du n°2004-801 du 6 août 2004, le principe est celui de l' « opt-in ».
- Les mentions d'information obligatoires doivent être communiquées aux personnes concernées et il est préférable de les indiquer en toutes lettres plutôt que de renvoyer à un lien du type « cliquez ici pour accéder à la charte de confidentialité ».
- La charte de confidentialité doit faire apparaître non seulement ce que le responsable du site fait des données à caractère personnel, mais également ce qu'il ne fait pas. Elle doit également indiquer aux personnes quels sont leurs droits (par exemple le droit d'accès) et comment les exercer, et doit mentionner l'adresse physique du responsable du site.
- Le consentement explicite et préalable ne peut pas être obtenu par le simple biais d'une case pré-cochée. La personne concernée doit entreprendre une action positive pour exprimer son consentement et doit toujours avoir la possibilité de ne pas consentir. La CNIL recommande que le consentement soit recueilli par le biais d'une case à cocher.
- Si les données à caractère personnel ne sont pas strictement nécessaires à la transaction à l'occasion de laquelle elles sont recueillies, il est nécessaire que la personne concernée soit clairement informée, au moment de la collecte, que ces informations sont fournies à sa seule discrétion et des modalités d'utilisation de ces informations dont la fourniture est optionnelle.
- La collecte de données relatives au profil d'une personne doit être réalisée en parfaite transparence. Certaines données de profil ne sont pas, en elles mêmes des données à caractère personnel. Néanmoins, dès lors qu'elles sont combinées avec un nom, un identifiant ou autre information permettant d'identifier la personne, elles doivent être considérées comme revêtant un caractère personnel.

Websites

The principles mentioned above apply irrespective of the means of information gathering used by the data controller. However, the collection of information via a website calls for certain specific observations.

- *It is essential to bear in mind that visitors to a site can gain access via pages other than the home page. Hyperlinks allow users to access the various pages of a site. It is therefore important to ensure that the obligatory notices are accessible from each page of the site on which personal data are likely to be gathered.*
- *Several data controllers may be identified on a single website. It is possible that in the context of a hosting agreement, a company could gain access to personal data for its online advertising campaign. In taking advantage of such access, the company will often be considered to be responsible for the processing of the data concerned. Certain information can also be communicated to a third party who is responsible for processing, for example the provider of an online secure payment system set up on the site concerned. Once again, these observations concern both the contractual arrangements linking the data controller to the third party concerned, and the information notices required to be displayed on the site. When a person uses hosting services, the service provider will be considered to be a subcontractor and the agreement with the subcontractor must include the clauses required by the Data Protection and Privacy Act (see the paragraph on subcontractors above).*
- *When the data are used or transferred for the purposes of direct marketing, the person concerned must have been given the opportunity to object to such use. Since the coming into force of the Act of 6 August 2004 No. 2004 - 801, the principle is that of "opt-in".*
- *The obligatory notices must be given to the persons concerned and it is preferable to set these out in full rather than by reference to a link marked (for example) "click here to see our privacy policy".*
- *The privacy policy must show not only what the person responsible for the site does with personal data but also what he does not do. It must also indicate the rights of data subjects (for example, the right of access) and how to exercise them, and must give the postal address of the person responsible for the site.*
- *Express prior consent cannot be validly obtained using a pre-ticked box alone. The person concerned must actively give his consent and must always have the option to refuse it. The CNIL recommends that consent be obtained by means of a tick box.*
- *If the personal data are not strictly required for the transaction in respect of which they are gathered, it is essential that the person concerned is clearly informed, at the point of collection, that such information is given optionally, and of the way in which this optional information is to be used.*
- *The collection of profile data must be done with clarity and transparency. Certain profile data are not in themselves personal data. Nevertheless, when they are combined with a name, a means of identification or other information that allows the person to be identified, they must be considered as such.*
- *The person concerned must be informed if a cookie is used with the objective of collecting data and must be given the opportunity to refuse the cookie (see the paragraph on cookies below).*
- *The use of an IP address, insofar as it is linked to an individual, constitutes processing of personal data.*

- La personne concernée doit être informée si un « cookie » est utilisé dans le but de collecter des données, et doit se voir offrir la possibilité de désactiver le « cookie » (voir paragraphe « Cookies » ci-après).
- L'utilisation d'une adresse IP, dans la mesure où elle est liée à un individu constitue un traitement de données à caractère personnel.
- Le fait que la personne concernée divulgue son adresse électronique (par exemple en participant à un site de discussion) ne signifie pas qu'elle consent à l'utilisation de cette adresse électronique à des fins de prospection ou à d'autres fins. L'utilisation de toiles d'araignées, ou autres types de programme de récupération d'adresses électroniques risque de constituer une atteinte à la loi « Informatique et Libertés », à moins que l'utilisation qui est faite des données soit conforme à la finalité pour laquelle elles ont été initialement communiquées par la personne concernée.
- Parfois des « web espions » sont utilisés de la même manière que les « cookies » afin de collecter des informations sur les personnes utilisant un site en particulier. Il est probable que la collecte des données à caractère personnel sera considérée comme déloyale, sauf à ce que la personne concernée soit informée de l'utilisation d'un « web espion » ou d'outils similaires, et à condition qu'elle ait reçu la possibilité de refuser ou de désactiver l'outil.
- Les sites collectant des informations sur des mineurs doivent mettre en place des garanties encore plus rigoureuses afin d'assurer que le traitement des données les concernant est loyal. L'information concernant les modalités d'utilisation des données doit être rédigée spécialement à l'attention des enfants, et facilement compréhensible. Les sites s'adressant à des mineurs ne doivent collecter que les données strictement nécessaires à la finalité du traitement. Enfin, la collecte des données sensibles doit être considérée comme interdite.
- Il est interdit de collecter auprès de mineurs des données concernant des tiers, l'entourage familial, le mode de vie des parents, les amis, etc. La mise en œuvre d'un jeu à destination des mineurs ne doit en aucun cas conduire à céder à des tiers les données recueillies dans le cadre de ce jeu, si le responsable du site n'est pas en mesure de rapporter la preuve que les parents ou le tuteur y ont expressément consenti.
- Des informations concernant un mineur ne sauraient être publiées sur Internet sans le consentement exprès et préalable des parents ou du tuteur.
- Lorsque le consentement est exigé, le responsable du traitement doit être en mesure de démontrer que ce consentement a bien été recueilli.
- Le degré de sécurité requis pour la collecte, la conservation, et la transmission des données sur Internet dépendra du type de données concerné. Le responsable du traitement est tenu de prendre « toutes précautions utiles » afin de préserver la sécurité de la collecte, de la conservation, et de la transmission des données. Un procédé de chiffrement des données peut être nécessaire pour se conformer à cette obligation, notamment pour des données particulièrement sensibles telles que les informations relatives à une carte de crédit.
- Le contrat d'hébergement relatif à un site Internet ou tout autre contrat de fourniture de service en relation avec un site Internet (dans lequel des données à caractère personnel pourraient être communiquées) doit être conforme aux conditions mentionnées ci-dessus à propos de la sous-traitance.
- Des données à caractère personnel ne doivent pas être publiées sur un site Internet sans que la personne concernée ait été préalablement informée et y ait librement consentie. Il est également nécessaire d'avoir à l'esprit qu'une publication sur Internet peut impliquer un transfert de données en dehors de l'Espace Economique Européen (voir le paragraphe « Transfert des données à caractère personnel en dehors de l'UE » ci-dessus).

- *The fact that the person concerned divulges his email address (for example by participating in a site discussion) does not imply that he consents to the use of such email address for the purposes of prospecting or for other purposes. The use of web crawlers or other types of program for harvesting email addresses, risks infringing the Data Protection and Privacy Act unless the use that is made of the data conforms to the end purpose for which they were initially communicated by the person concerned.*
- *Sometimes “web bugs” are used in the same way as cookies in order to gather information on people using a particular site. It is probable that the collection of personal data will be considered to be unfair unless the person concerned is informed of the use of a “web bug” or similar tool, and given the opportunity to refuse or deactivate the tools.*
- *Even more stringent security must be put in place by sites that gather information on minors. This is to ensure that the processing of data concerning them is fair. Information concerning the terms of use of the data must be specially drafted with children in mind and must be easily understood. Sites intended for minors must gather only the data that is strictly required for the processing purposes. The collection of sensitive data must be considered to be prohibited.*
- *The gathering from minors of data in respect of third parties, the family circle, parents’ lifestyle, friends etc, is prohibited. The setting up of a game for minors must not, under any circumstances, lead to the transfer to third parties of data gathered in the context of such a game if the person responsible for the site is not in a position to provide proof that the parents or guardian have expressly consented thereto.*
- *Information concerning a minor cannot be published on the internet without the express prior consent of the parents or guardian.*
- *When consent is required, the data controller must be in a position to demonstrate that such consent has in fact been given.*
- *The degree of security required for the collection, retention and transmission of data via the internet will depend on the type of data concerned. The data controller is obliged to take “all appropriate precautions” in order to safeguard the collection, retention and transmission of the data. Encryption of the data may be required in order to comply with this obligation, notably for particularly sensitive data such as credit card information.*
- *The hosting agreement relating to an internet site, and any other contract for the provision of a service relating to such a site (being one through which personal data could be communicated) must comply with the above-mentioned conditions in respect of subcontracting.*
- *Personal data cannot be published on an internet site unless the person concerned has been informed in advance and has freely consented thereto. It is important also to bear in mind that publishing information on the internet can involve the transfer of data outside the European Economic Area (see the paragraph on transfer of data outside the EU below).*
- *Amendments to the privacy policy or information notices will not affect the use that may be made of the personal data previously gathered. The position is that data subjects receive assurances in respect of the manner and the purposes for which personal data will be used, at the time when they provide the information to the controller of the site. It is therefore necessary to obtain the consent of the person concerned for any use that was not anticipated at the time when consent was first obtained. The absence of a reply to an electronic message is not a sufficient ground for considering consent to have been obtained. It is therefore essential that the privacy policy available on the site is drafted in such a way as to anticipate not only existing uses but also uses that may be made of data in the future.*

- Des modifications ultérieures de la charte de confidentialité ou des mentions d'information seront sans effet sur l'utilisation pouvant être faite des données à caractère personnel. En effet, les personnes concernées reçoivent des garanties concernant la manière et les finalités pour lesquelles les données à caractère personnel seront utilisées, et ce au moment où elles fournissent les informations au responsable du site. Dès lors il est nécessaire d'obtenir le consentement de la personne concernée pour toute utilisation qui n'aurait pas été prévue lors du recueil initial du consentement. L'absence de réponse à un courrier électronique ne saurait être suffisant pour considérer que le consentement a été obtenu. Il est dès lors essentiel que la charte de confidentialité présente sur le site soit rédigée de telle manière qu'elle prévoit non seulement les utilisations existantes mais également les utilisations qui pourraient être faites des données dans le futur.
- En cas d'acquisition d'une entité exploitant un site Internet, l'acquéreur ne saurait déduire de la seule acquisition qu'il est en droit de contacter les utilisateurs qui se seraient inscrits sur ce site, ou encore d'utiliser les données collectées par le biais du site. Toute utilisation postérieure des données doit être loyale et réalisée en accord avec la charte de confidentialité du site. La communication des informations à l'acquéreur pourrait être considérée comme une atteinte à l'obligation de confidentialité incombant au responsable du traitement, ou encore comme une utilisation des données à laquelle la personne concernée n'aurait pas consentie. Dès lors, il est nécessaire dans ce cas d'obtenir le consentement de la personne concernée avant d'entreprendre toute opération de marketing la concernant.

Fichiers de marketing direct

Les traitements de données à caractère personnel à des fins de marketing direct doivent être déclarés auprès de la CNIL selon les modalités de déclaration normale. Ici tout particulièrement, la collecte des informations doit être faite de manière loyale et licite. Il convient également de veiller à l'information préalable et au respect du droit d'accès des personnes concernées.

En concertation avec la CNIL, les professionnels de ventes à distance et du marketing direct ont dégagé des règles de déontologie dans le secteur du marketing qui ont débouché sur l'adoption du Code de déontologie du marketing direct de 1993, et du Code de déontologie de la communication directe électronique de 2005 présentés respectivement par le SNCD (Syndicat National de la Communication directe), et l'UFMD (Union Française du Marketing Direct). Ces projets prévoient notamment qu'une adresse de courrier électronique ne peut être utilisée à des fins de prospection que si la personne auprès de laquelle elle a été collectée a été mise en mesure, au moment de la collecte, de consentir ou dans certains cas spécifiques, de s'opposer à une telle utilisation ;

Si un responsable acquiert un fichier d'adresses auprès d'un tiers, il doit s'assurer que les informations ont été obtenues de manière loyale et licite et que l'utilisation qu'il entend faire des données ainsi acquises entre dans le champ du consentement de la personne concernée. Il est de l'obligation du responsable du traitement d'assurer qu'il a obtenu l'autorisation d'utiliser les informations qu'il a acquises. Des garanties en ce sens peuvent bien entendu être obtenues du vendeur mais de telles garanties ne sauraient exclure que l'utilisation de ces fichiers par le responsable du traitement puisse enfreindre les dispositions de la loi « Informatique et Libertés ».

- *In the event of the purchase of an entity which makes use of an internet site, the purchaser cannot treat the fact of purchase alone as giving him the right to contact users who are subscribers to that site, or to use the data collected via the site. Any subsequent use of the data must be fair and must be carried out in accordance with the site's privacy policy. The communication of information to the purchaser can be construed as a breach of the obligation of confidentiality incumbent upon the data controller, or even as a use of the data to which the person concerned has not consented. It is therefore necessary, in such a case, to obtain the consent of the data subject before undertaking any marketing activity concerning him.*

Direct marketing files

The processing of personal data, for the purposes of direct marketing must be declared to the CNIL in the form of a standard declaration. Here particularly, the gathering of data must be done in a fair and lawful manner. It is also important to observe the advance information requirements and the right of access of the persons concerned.

In concert with the CNIL, distance selling and direct marketing professionals have formulated rules of professional conduct for the marketing sector, which have resulted in the adoption of a 1993 code of professional ethics in direct marketing, and a 2005 code of professional ethics for direct electronic communication, produced respectively by the SNCD (National Syndicate of Direct Communication) and the UFMD (French Union of Direct Marketing). These documents provide, in particular, that an email address cannot be used for the purposes of prospecting unless the person from whom it has been obtained was given the opportunity, at the time of collection, to consent or in certain specific cases to object to such use.

If a data controller acquires a file of addresses from a third party, he must ensure that the information was obtained fairly and lawfully and that the use that he intends to make of the data thus acquired is within the consent given by the person concerned. It is incumbent upon the data controller to obtain authorisation for the use of the information he has acquired. Assurances of this kind can, of course, be obtained from the seller but such assurances cannot exempt the data controller's use of such files from the provisions of the Data Protection and Privacy Act.

Cookies

Un « cookie » est un enregistrement d'informations par un serveur dans un fichier texte situé sur l'ordinateur client (celui de l'utilisateur d'un réseau), informations que ce même serveur (et lui seul) peut aller relire et modifier ultérieurement. (Lexique CNIL). Les informations pouvant être collectées via un cookie correspondent à deux types de catégories : les informations de passage (pages visitées, navigateur, etc.), et les informations personnelles (nom, adresse, etc.) de la personne concernée. Les « cookies » sont souvent utilisés pour permettre un accès et une utilisation plus aisés d'un site, mais peuvent également être utilisés afin de déterminer les habitudes de consommation de l'utilisateur à des fins de marketing.

La loi « Informatique et Libertés » précise dans son article 32-II les obligations incombant aux éditeurs de sites qui utilisent des procédés de collecte automatisée de données.

Le principe posé par la loi est celui d'une information claire et complète de l'utilisateur :

- 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.

Toutefois, la loi a prévu que cette obligation d'information n'était pas nécessaire si le « cookie » :

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

Prospection par automates d'appel

Il n'est pas autorisé d'appeler ou d'être à l'initiative de publicité par automates d'appel à moins que la personne concernée ait explicitement donné son accord pour être démarchée au moment de la collecte de son numéro de téléphone (opt-in).

Un automate d'appel est défini par la CNIL comme un appareil permettant de déclencher par programme un grand nombre d'appels téléphoniques simultanés afin de délivrer un message pré-enregistré.

La publicité par fax est possible à condition que la personne concernée ait explicitement donné son accord pour être démarchée, au moment de la collecte de son numéro de fax.

Le consentement préalable est exigé pour toute personne physique, y compris dans le cadre de son activité professionnelle. La CNIL recommande que le consentement préalable soit recueilli par le biais d'une case à cocher (opt-in).

Cookies

A cookie is a record of information made by a server in a textfile located in a client computer (that is, one used to access a network). The same server (and only it) can re-read and subsequently modify this information (CNIL glossary). The information that can be collected via a cookie falls into two categories: browsing information (pages visited, browser etc.) and personal information (name, address etc.) of the person concerned. Cookies are often used to enable easier access and use of a site but can also be used to ascertain the consumer habits of the user, for the purposes of marketing.

Clause 32–11 of the Data Protection and Privacy Act specifies the obligations incumbent upon the editors of sites who use the results of automated data collection.

The principle imposed by the law is that the user must be clearly and fully informed as to:

- *the end purpose of any action leading to access, by means of electronic transmission, to information stored in his terminal, or to storage by such means of information on his terminal*
- *the means of objection available to him.*

However, the law provides that this obligation to inform does not apply where:

- *the ultimate aim of the cookie is to enable or to facilitate electronic communication, or*
- *the cookie is strictly necessary for the provision of an online communication service at the express request of the user.*

Prospecting via automated calls

It is not permitted to make automated calls, or to have such calls made for the purposes of advertising, unless the person concerned expressly agreed, when his phone number was obtained, to be canvassed (opt-in).

An automated call is one made by certain equipment, defined by the CNIL as apparatus programmed to make a large number of simultaneous telephone calls in order to deliver a pre-recorded message.

Advertising by fax is possible provided that the person concerned expressly agreed to be canvassed at the time his fax number was obtained.

Prior consent is required for any natural person, even within the context of his business activity. The CNIL recommends that prior consent be given by means of a tick box (opt-in).

Prospection téléphonique (télémarketing)

La prospection par téléphone (télémarketing) est possible à condition que la personne soit, au moment de la collecte de son numéro de téléphone :

- informée de son utilisation à des fins de prospection ;
- en mesure de s'opposer de manière simple et gratuite, notamment par le biais d'une case à cocher (opt-out).

La CNIL ne distingue pas selon que la personne concernée par l'appel est un particulier ou un professionnel.

Prospection par courrier électronique

La prospection par courrier électronique à l'attention des particuliers est possible à condition que la personne ait, au moment de la collecte de son adresse électronique expressément donné son accord pour être démarchée (opt-in).

Le consentement doit être spécifiquement donné à la personne morale concernée, et pour la prospection par email. Dès lors, il ne serait certainement pas suffisant pour une personne morale de se fonder sur un consentement général de la personne concernée à être prospectée, sans que la voie du courrier électronique soit spécifiée.

Par exception, une personne morale peut procéder à une prospection par courrier électronique, si la personne prospectée est déjà cliente de l'entreprise et si la prospection concerne des produits ou services analogues à ceux déjà fournis par l'entreprise, ou si la prospection n'est pas de nature commerciale. Dans ces deux cas, la CNIL exige que la personne soit, au moment de la collecte de son adresse de messagerie, informée de son utilisation à des fins de prospection, et en mesure de s'y opposer de manière simple et gratuite.

Dissimulation d'identité

Dans tous les cas, conformément à l'article 32 de la loi « Informatique et Libertés » et 34-5 du code des postes et des communications électroniques, le message électronique doit comporter l'identité de l'annonceur, et proposer un moyen simple de s'opposer à la réception de nouvelles sollicitations.

Dès lors, les personnes morales ne doivent en aucun cas transmettre ou faire transmettre des messages à des fins de marketing ciblé par voie de courrier électronique si l'identité de la personne pour le compte de laquelle le message est envoyé est dissimulée ou cachée, ou sans qu'un moyen simple et gratuit de s'opposer ne soit proposé à la personne concernée, par le biais par exemple d'une adresse électronique valable.

Telephone prospecting

Prospecting by telephone (telemarketing) is possible provided that the person, at the time his phone number was obtained:

- *was informed that it was to be used for the purposes of prospecting;*
- *was given a simple means of refusing, at no cost (opting out by means of a tick box, to give a notable example)*

The CNIL does not make a distinction on the basis of whether the person called is a private individual or a business person.

Email prospecting

In respect of private individuals, prospecting by email is possible provided that the person expressly gave his consent to be contacted (opted-in) when his email address was obtained.

The consent must be given specifically to the organisation concerned, and in relation to prospecting by email. It would not therefore be sufficient for an organisation to proceed on the basis of general consent by the person concerned to be prospected unless electronic mail is specified.

An organisation can, exceptionally, carry out electronic canvassing if the person prospected is already a client of the business, and if the prospecting concerns products or services similar to those already provided by the business, or if the prospecting is not of a commercial nature.

In these two cases, the CNIL requires that the person is informed, when his email address is obtained, that it may be used for the purposes of prospecting, and that he is given a simple means of refusing at no cost.

Identity concealment

Under Clause 32 of the Data Protection and Privacy Act and 34-5 of the Code of Postal and Electronic Communications, the electronic message must include the identity of the advertiser and offer a simple means of refusing to accept any further requests.

Therefore, organisations must not in any circumstances transmit messages or have messages transmitted for the purposes of direct marketing by means of electronic mail, if the identity of the person on whose behalf the message is sent is concealed or disguised, or if the person concerned is not given a free and simple means of refusal, for example by means of a valid electronic address.

Sites Internet situés en dehors de l'UE

La collecte de données directement auprès de la personne concernée, par le biais de sites situés aux États-Unis, ne constitue pas un traitement de données sur le territoire français, à moins que :

- le responsable du traitement ait recours à des moyens de traitement situés sur le territoire français, à des fins autres que le simple transit des informations ;
- le traitement soit entrepris par le biais d'une entreprise établie sur le territoire français.

Il convient cependant de noter que l'utilisation de « cookies » qui sont téléchargés sur un équipement informatique situé en France peut constituer une utilisation de moyens sur le territoire français, et dès lors entrer dans le champ d'application de la loi « Informatique et Libertés ».

Messages électroniques adressés à des employés de sociétés

Les règles énoncées ci-dessus concernant la prospection par courrier électronique (voir paragraphe « Prospection par courrier électronique ») s'appliquent uniquement aux particuliers (B to C). Il est possible dès lors d'envoyer des courriers électroniques non sollicités aux employés d'une société à condition que de tels courriers soient envoyés à leur adresse professionnelle.

Néanmoins, les principes généraux relatifs au traitement des données à caractère personnel définis par la loi « Informatique et Libertés » trouvent à s'appliquer à ce type de traitement. La prospection par courrier électronique est dès lors possible à condition que la sollicitation soit en rapport avec la profession de la personne démarchée, et que la personne concernée soit, au moment de la collecte de son adresse de messagerie, informée de son utilisation à des fins de prospection, et en mesure de s'opposer de manière simple et gratuite. Chaque message doit obligatoirement préciser l'identité de l'annonceur, et proposer un moyen simple de s'opposer à la réception de nouvelles sollicitations. La CNIL recommande que le consentement préalable ou le droit d'opposition soit recueilli par le biais d'une case à cocher.

Websites located outside the EU

The collection of data directly from the person concerned, via sites situated in the United States, does not constitute processing of data on French territory unless:

- *the data controller uses means of processing which are situated on French territory, for purposes other than the simple transmission of information;*
- *the processing is undertaken via a business established in French territory.*

It should be noted however, that the use of cookies which are downloaded from computer equipment located in France can constitute a use of means on French territory and the Data Protection and Privacy Act therefore applies.

Emails to company employees

The regulations set out above in respect of prospecting by electronic mail (see the paragraph on email prospecting) apply only to private individuals (B to C). It is therefore possible to send unsolicited electronic messages to company employees provided that such messages are sent to their business address.

Nevertheless, the general principles relating to the processing of personal data, as defined by the Data Protection and Privacy Act are found to apply to this type of processing. Prospecting by electronic mail is therefore possible provided that the soliciting is connected with the occupation of the person canvassed and that at the time of obtaining his electronic address, the person is informed that it is to be used for the purposes of prospecting, and is given a simple means of refusing at no cost. It is obligatory for each message to specify the identity of the advertiser and to offer a simple means of refusing to accept any new requests. The CNIL recommends that prior consent should be given, and the right to refuse should be exercised, by means of a tick box.

Informations obtenues dans le cadre de relations commerciales

Les informations obtenues dans le cadre de la fourniture de produits ou de services seront dans la plupart des cas recueillies aux fins de la fourniture du produit ou du service, ou encore pour la formation, la conclusion ou l'exécution d'un contrat avec la personne concernée. Les informations ont été communiquées à cette seule fin et l'on ne saurait déduire de cette communication que la personne concernée a consenti à l'utilisation de ces informations à des fins de prospection.

S'il est dans l'intention du responsable du traitement d'utiliser les informations collectées à des fins de prospection, il devra obtenir de la personne concernée son consentement à cet usage spécifique. Le consentement donné devra être spécifique aux moyens qui seront utilisés pour la transmission du message, aux types de biens ou de services qui seront proposés. Il sera également mentionné au moment de la collecte si la prospection sera effectuée par le responsable du traitement ou par des tiers (éventuellement appartenant à un même groupe de sociétés), les informations concernant tout tiers à qui les données pourraient être communiquées, et la durée pendant laquelle celles-ci pourront être utilisées à des fins de marketing. Enfin, la CNIL exige que la personne soit, au moment de la collecte de son adresse de messagerie, en mesure de s'y opposer.

Employés du responsable du traitement

Les principes et règles posés par la loi « Informatique et Libertés » s'appliquent aux données à caractère personnel détenues par une société en relation avec ses propres employés, candidats postulant, ou cocontractants de la même manière qu'ils s'appliquent aux données à caractère personnel des clients actuels ou potentiels. La loi « Informatique et Libertés » s'applique aux données à caractère personnel concernant une personne dans le contexte de son emploi qui sont contenues dans un ordinateur mais également aux fichiers « papiers ».

La CNIL a publié un guide à destination des employeurs et employés.

Ce guide a plus particulièrement été rédigé afin d'aider les employeurs à se conformer à la loi « Informatique et Libertés », et à les conseiller sur les mesures à adopter à cette fin, notamment quant à l'utilisation des outils et fichiers mis en œuvre en matière de ressources humaines. Il traite notamment des problèmes liés aux opérations de recrutement, aux annuaires du personnel, à l'accès au dossier professionnels, aux transferts internationaux de données, au contrôle de l'utilisation de l'Internet et de la messagerie, à la vidéosurveillance, la gestion de la téléphonie, etc. Il donne des indications relatives à la collecte des informations concernant les employés, les données pouvant être collectées, l'accès au dossier professionnel, etc.

D'une manière générale, la mise en œuvre de traitements impliquant des salariés impose une étude de la licéité desdits traitements au regard du droit social autant qu'au regard du droit de la protection des données personnelles. Les institutions représentatives du personnel devront souvent être consultées avant que le traitement puisse être mis en œuvre.

Information obtained in the course of commercial relationships

Information obtained in the context of the provision of services will, in most cases, be gathered for the purposes of the supply of a product or service or even for the formation, conclusion or execution of a contract with the person concerned. The information has been communicated with this sole aim and it cannot be inferred from such communication that the person concerned has consented to the use of the information for the purposes of prospecting.

If it is the intention of the data controller to use the information gathered for the purposes of prospecting, he must obtain the consent of the person concerned for this specific use. The consent given must be specific as to the means that will be used for the transmission of the message, and the types of goods or services that are offered. It must also be stated, at the time the information is collected, whether the prospecting will be carried out by the data controller or by third parties (possibly belonging to the same group of companies), and information must be given concerning any third party to whom the data could be communicated, as well as the length of time for which it can be used for the purposes of marketing. Finally, the CNIL requires that at the time his electronic address is obtained, the person concerned has the opportunity to refuse.

Data controller employees

The principles and regulations imposed by the Data Protection and Privacy Act apply to personal data held by a company in respect of its own employees, applicants or contractual partners, in the same manner as they apply to the personal data of existing or potential clients. The Data Protection and Privacy Act applies to personal data concerning a person in the context of his employment whether it is held on a computer or in hard copy.

The CNIL has published a guide for use by employers and employees.

More specifically, this guide has been produced to help employers comply with the Data Protection and Privacy Act and to advise them on the measures to be adopted for this purpose, especially in relation to HR tools and files. It covers, in particular, issues relating to recruitment activities, personnel directories, access to professional records, international transfer of data, control of the use of the internet and electronic communication systems, management of telephone systems etc. It gives guidance in respect of the collection of information concerning employees, the data that can be gathered, access to professional records etc.

In general, the legality of processing relating to employees demands consideration from the perspective of employment law as much as from the perspective of the law for the protection of personal data. The institutions that represent employees will often have to be consulted before such processing can be implemented.

