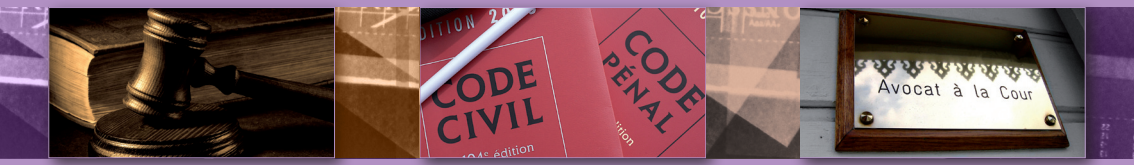
LES GUIDES DE LA CNIL



GUIDE

LES AVOCATS ET LA LOI INFORMATIQUE ET LIBERTÉS

Édition 2011

CNIL
Commission Nationale de l'Informatique et des Libertés

Sommaire

Ce guide est téléchargeable sur le site Internet de la CNIL : www.cnil.fr

Avant-propos

A l'heure où les dispositifs de traçage de l'individu dans l'espace et dans le temps se multiplient et portent en eux des atteintes potentielles à nos libertés fondamentales et notre vie privée, le rôle de l'avocat rejoint celui de notre Commission.

Lors des rencontres régionales organisées sur l'ensemble du territoire par la CNIL, j'ai pu échanger de façon très constructive avec nombre de vos confrères. J'ai constaté, à cette occasion, que vos missions et celles de la CNIL étaient analogues : nous devons faire en sorte que chaque citoyen maîtrise ces nouveaux outils et soit en mesure de défendre ses droits. De ces échanges est née la volonté d'élaborer ce guide en concertation avec le Conseil National des Barreaux dans le cadre d'une Convention.

Celle-ci prévoit aussi le développement de la formation du correspondant informatique et libertés (CIL) au sein de la profession d'avocat et de ses structures représentatives. L'indépendance dont le CIL doit faire preuve pour mener à bien ses missions fait de l'avocat un intervenant naturel pour assumer une telle fonction. Le règlement intérieur de la profession a d'ailleurs encadré celle-ci.

Bien entendu, l'avocat, d'une part, et notre Commission, d'autre part, conservent leur totale indépendance mais ils sont côte à côte pour assurer la protection de la vie privée. C'est dans cet esprit que le présent guide a été élaboré.

Je suis convaincu qu'il apportera des réponses concrètes à vos questions et vous permettra de jouer un rôle essentiel en matière de protection des données et de la vie privée, tant comme responsable de traitement que comme conseil auprès de vos clients.

Alex TÜRK
Président de la CNIL

LA CNIL ET LES AVOCATS :
un intérêt réciproque à la protection des données à caractère personnel

Dès lors qu'elles sont susceptibles de relever de la vie privée de leurs clients et que leur divulgation peut porter atteinte aux droits et libertés des personnes concernées, les informations traitées par les avocats dans leurs fichiers pour l'exercice de leur profession doivent être protégées.

Le respect du secret professionnel, tel que défini par l'article 2 du règlement intérieur national (RIN) et protégé par l'article 226-13 du code pénal, les conduit à être particulièrement vigilants à l'égard de la protection des données personnelles de leurs clients et, par conséquent, aux obligations qui découlent de la loi informatique et libertés.

Le respect par les avocats des règles de protection des données à caractère personnel est un facteur de transparence et de confiance à l'égard de la profession. C'est également un gage de sécurité juridique pour les avocats eux-mêmes qui, responsables des fichiers mis en œuvre, doivent veiller à ce que la finalité de chaque traitement informatique et les éventuelles transmissions d'informations soient clairement définies, les dispositifs de sécurité informatique précisément déterminés et les mesures d'information des personnes concernées appliquées.

I. LE CADRE GÉNÉRAL DE LA PROTECTION DES DONNÉES À CARACTÈRE PERSONNEL

La loi du 6 janvier 1978 modifiée en 2004, également connue sous le nom de loi informatique et libertés, s'applique aux traitements automatisés de données à caractère personnel, ainsi qu'aux fichiers dits « papier » qui contiennent des données personnelles appelées à figurer dans un traitement automatisé. Cette loi ne s'applique pas aux traitements mis en œuvre pour l'exercice d'activités exclusivement personnelles.

La loi définit la notion de donnée à caractère personnel comme toute information relative à une personne physique identifiée ou pouvant l'être, directement ou indirectement, par référence à un numéro d'identification ou à des éléments qui lui sont propres.

Pour déterminer si une personne est identifiable, il convient de considérer l'ensemble des moyens dont dispose ou auxquels peut avoir accès le responsable du traitement ou toute autre personne.

A. LES CINQ PRINCIPES CLEFS À RESPECTER

La loi informatique et libertés définit les principes à respecter lors de la collecte, du traitement et de la conservation de données personnelles. Elle garantit également un certain nombre de droits pour les personnes concernées.

1. Le principe de finalité : une utilisation encadrée des fichiers

Les données à caractère personnel ne peuvent être recueillies et traitées que pour un usage déterminé explicite et légitime, correspondant aux missions de l'avocat responsable du traitement. En tant que responsable d'un fichier, l'avocat a l'obligation d'en fixer la finalité.

Ainsi, à titre illustratif, lorsqu'il accède au serveur professionnel des données cadastrales de la direction générale des impôts, un avocat ne doit pas porter atteinte à la vie privée de la personne concernée par ces informations, ou utiliser les données qu'il consulte à des fins de démarchage commercial, politique ou électoral.

Tout détournement de finalité est passible de 5 ans d'emprisonnement et de 300.000 € d'amende (article 226-21 du code pénal).

2. Le principe de proportionnalité

Seules les informations pertinentes et nécessaires peuvent faire l'objet d'un enregistrement dans un traitement de données à caractère personnel. Par exemple, il n'est pas utile d'enregistrer des informations sur l'entourage familial d'une personne lorsque, au regard des finalités d'un traitement et de la nature de l'affaire traitée, seuls sont nécessaires des éléments relatifs à sa vie professionnelle.

3. Le principe d'une durée de conservation limitée des données

Les informations figurant dans un fichier ne peuvent être conservées indéfiniment. Une durée de conservation doit être établie en fonction de la finalité de chaque fichier. Les enregistrements de vidéoprotection, par exemple, ne doivent en principe être conservés qu'un mois. Les informations ayant trait à des clients, quant à elles, ne doivent pas être conservées au-delà d'un an à l'issue de la relation contractuelle.

Toutefois, cette obligation de fixer une durée de conservation limitée dans le temps ne prive pas les responsables de traitements de la possibilité d'archiver des informations, notamment à des fins probatoires. Lorsque cet archivage est réalisé sous forme électronique, il convient de respecter la recommandation n° 2005-213 de la CNIL du 11 octobre 2005 relative à l'archivage électronique de données à caractère personnel dans le secteur privé.

4. Les principes de sécurité et de confidentialité

Les données contenues dans les fichiers ne peuvent être consultées que par les personnes habilitées à y accéder en raison de leurs fonctions. Les dossiers des avocats ne peuvent être communiqués qu'à des personnes autorisées à en connaître, en application de dispositions législatives particulières et sous réserve du respect du secret professionnel.

L'avocat, en qualité de responsable d'un traitement, est astreint à une obligation de sécurité. Il doit ainsi prendre toutes les mesures nécessaires pour en garantir la confidentialité et éviter toute divulgation d'information. Il convient, par exemple, de veiller à ce que chaque personne habilitée à accéder aux informations dispose d'un mot de passe individuel (composé d'au moins 8 caractères alphanumériques et régulièrement changé) et que les droits d'accès soient précisément définis en fonction des besoins réels.

5. Le principe du respect des droits des personnes

L'article 32 de la loi informatique et libertés prévoit que les personnes physiques concernées par un traitement de données à caractère personnel doivent être préalablement informées de l'identité de son responsable (ou de son représentant), de sa finalité, du caractère obligatoire ou facultatif du recueil des données, des destinataires, des modalités d'exercice des droits d'accès et de rectification ainsi que, le cas échéant, des transferts de données vers un État non-membre de l'Union européenne.

L'exception à l'obligation d'information prévue par l'alinéa 2 de l'article 32-III de la loi du 6 janvier 1978 modifiée, c'est-à-dire une information impossible ou exigeant des efforts disproportionnés par rapport à l'intérêt de la démarche, n'est pas applicable aux traitements de gestion de contentieux des avocats, et ce, en raison des intérêts et enjeux présents dans ce domaine. En effet, dès lors que des poursuites judicaires peuvent être engagées sur la base de ce type de traitements, les diligences à accomplir pour informer les personnes concernées n'apparaissent pas disproportionnées par rapport à l'intérêt d'une telle démarche.

Les avocats, lorsqu'ils agissent en qualité de responsable de traitement, sont libres de déterminer les moyens à mettre en œuvre pour assurer l'information des personnes.

Toute personne a le droit de s'opposer, **pour un motif légitime**, à ce que des données la concernant soient enregistrées dans un fichier informatique, sauf si ce dernier présente un caractère obligatoire.

Par ailleurs, toute personne physique justifiant de son identité a le droit d'interroger le responsable d'un traitement de données à caractère personnel pour :

- savoir si des données qui la concernent y figurent ou non ;
- obtenir la communication des données qui la concernent sous une forme compréhensible, d'une part, et de toutes les informations disponibles quant à leurs origines, d'autre part ;
- obtenir des informations sur la finalité du traitement, les données collectées et les destinataires.

B. LES CINQ MISSIONS DE LA CNIL

La Commission nationale de l'informatique et des libertés est une autorité administrative indépendante chargée d'assurer le respect des dispositions de la loi du 6 janvier 1978 modifiée. Elle est ainsi chargée de veiller à ce que l'informatique soit au service du citoyen et qu'elle ne porte atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques.

1. Informer les personnes concernées de leurs droits et les responsables de traitements de leurs obligations

La CNIL informe les personnes de leurs droits et obligations.

Elle propose également au Gouvernement les mesures législatives ou réglementaires de nature à adapter la protection des libertés et de la vie privée à l'évolution des techniques.

L'avis de la CNIL doit être sollicité avant toute transmission au Parlement d'un projet de loi relatif à la protection des données à caractère personnel.

2. Garantir le droit d'accès

La CNIL veille à ce que les citoyens accèdent efficacement aux données contenues dans les traitements les concernant, notamment, par l'intermédiaire de son service des plaintes.

En outre, elle exerce, pour le compte des citoyens qui le souhaitent, l'accès aux fichiers intéressant la sûreté de l'État, la défense et la sécurité publique (fichiers de police et de gendarmerie, fichiers de renseignement, fichier Schengen, etc.).

Certains de ces fichiers peuvent être consultés lors du recrutement, de l'agrément ou de l'habilitation des personnels de professions diverses (surveillance, gardiennage, emplois dans des zones aéroportuaires, fonction publique...) ou bien encore pour la délivrance ou le renouvellement de titres pour l'entrée et le séjour des étrangers. Les informations qu'ils comportent ou, le cas échéant, leurs inexactitudes peuvent ainsi être à l'origine d'un licenciement, d'un refus d'embauche ou d'attribution d'un visa et peuvent entraîner de graves conséquences sur la situation des personnes. Les informations du fichier des comptes bancaires (FICOBA) tenu par la direction générale des finances publiques, qui sont relatives aux ouvertures et mouvements de comptes, relèvent également de cette procédure.

Dans ces cas précis, l'avocat peut conseiller à son client de s'adresser au service du droit d'accès indirect (DAI) de la CNIL, afin de vérifier s'il est fiché et, le cas échéant, demander la rectification ou l'effacement des données inexactes. Un magistrat de la Commission exercera, pour son compte, son droit d'accès.

3. Recenser les fichiers et réglementer

Les traitements de données personnelles dits *« à risques »* du fait de leurs finalités (listes noires, interconnexions…) ou de la nature des informations traitées (données biométriques, données comportant des appréciations sur

les difficultés sociales, données relatives aux infractions, condamnations ou mesures de sûreté…) sont soumis à une autorisation de la CNIL préalablement à leur mise en œuvre.

S'agissant des autres traitements de données à caractère personnel, la CNIL reçoit et recense les déclarations correspondantes. En application de l'article 31 de la loi informatique et libertés, elle tient ainsi à la disposition du public le *« fichier des fichiers »*, c'est-à-dire la liste des traitements déclarés et leurs principales caractéristiques.

Par ailleurs, pour assurer sa mission de réglementation, la Commission rend des avis, notamment, sur les traitements publics qui utilisent le numéro de sécurité sociale ou ceux qui intéressent la sûreté de l'Etat.

Elle peut également établir des dispenses de déclaration ou encore des normes simplifiées, afin que les traitements les plus courants et les moins dangereux pour les libertés individuelles fassent l'objet de formalités allégées. Dans les domaines relevant de la procédure d'autorisation elle peut élaborer des autorisations uniques.

Le non-respect des formalités préalables par les responsables de traitements est passible de sanctions administratives ou pénales.

4. Contrôler

La CNIL vérifie que la loi du 6 janvier 1978 modifiée est respectée, notamment, en contrôlant les applications informatiques lors des missions que son Président diligente.

La Commission use de ses pouvoirs de vérification et d'investigation pour instruire les plaintes, disposer d'une meilleure connaissance de certains fichiers, mieux apprécier les conséquences du recours à l'informatique dans certains secteurs, ou assurer un suivi de ses délibérations.

La CNIL surveille, par ailleurs, la sécurité des systèmes d'information en s'assurant que toutes les précautions sont prises pour empêcher que les données ne soient déformées ou communiquées à des personnes non-autorisées.

5. Sanctionner

A l'issue des contrôles ou de l'instruction de plaintes, la formation contentieuse de la CNIL, composée de cinq membres et d'un Président distinct du Président de la CNIL, peut prononcer diverses sanctions à l'égard des responsables de traitements qui ne respecteraient pas la loi.

Par ailleurs, en cas d'atteinte grave et immédiate aux droits et libertés garanties par la loi du 6 janvier 1978 modifiée, la formation contentieuse de la Commission peut adopter des mesures en urgence.

En outre, le Président de la Commission dispose d'un pouvoir qui lui est propre, celui de dénoncer au Procureur de la République les violations de la loi (Cf. fiche n°9).

C. LES TYPES DE FORMALITÉS PRÉALABLES À LA MISE EN ŒUVRE D'UN TRAITEMENT

La déclaration est une obligation légale dont le non-respect est pénalement sanctionné. En effet, l'article 226-16 du code pénal dispose :

« Le fait, y compris par négligence, de procéder ou de faire procéder à des traitements de données à caractère personnel sans qu'aient été respectées les formalités préalables à leur mise en œuvre prévues par la loi est puni de cinq ans d'emprisonnement et de 300.000 € d'amende ».

Tout fichier ou traitement informatisé comportant des données personnelles doit être déclaré à la CNIL préalablement à sa mise en œuvre, sauf s'il bénéficie expressément d'un allègement des formalités préalables (dispense de déclaration ou déclaration simplifiée) ou relève du régime de l'autorisation préalable.

1. La dispense de déclaration

Certaines catégories de traitements sont dispensées de déclaration par une décision expresse de la CNIL (paie des personnels, dématérialisation du contrôle de légalité ou des marchés publics…). La liste des dispenses de déclaration est consultable sur le site internet de la CNIL (http://www.cnil.fr/en-savoir-plus/deliberations/dispenses-de-declaration).

Le fait d'être dispensé de déclaration n'exonère pas pour autant le responsable de traitement des autres obligations issues de la loi du 6 janvier 1978 modifiée, notamment en matière d'information des personnes concernées et de sécurité des données.

Le cas particulier des audits

Au regard de la loi informatique et libertés, les avocats qui interviennent dans ce domaine peuvent se prévaloir de la qualité de sous-traitant, dès lors qu'ils agissent sur la base d'instructions strictement définies par leurs clients. Il en résulte que les avocats n'ont pas à déclarer les fichiers nécessairement mis en œuvre lors de ces opérations.

En revanche, au même titre que les éventuels prestataires spécialisés dans l'hébergement et la gestion de documents, ils sont tenus de présenter des garanties suffisantes pour assurer la sécurité et la confidentialité des données auxquelles ils accèdent, en application de l'article 35 de la loi informatique et libertés.

La mission de conseil des avocats devra néanmoins les conduire à s'assurer que leurs clients se sont acquittés auprès de la CNIL des formalités applicables et, notamment, que les déclarations correspondantes mentionnent la réalisation d'audits ou encore que l'information des personnes physiques concernées a été assurée.

A savoir : Les avocats, en raison de leur qualité de sous-traitant, n'ont pas à figurer au nombre des destinataires énumérés par une déclaration effectuée par leurs clients.

2. La déclaration normale

Le régime de droit commun des formalités préalables à accomplir auprès de la CNIL est la déclaration normale. Il est applicable lorsqu'un fichier ne relève pas d'une procédure particulière (art. 22 de la loi du 6 janvier 1978). Le traitement peut être mis en œuvre dès réception du récépissé délivré par la CNIL.

Ce récépissé atteste de l'accomplissement de la formalité de déclaration, mais n'exonère pas le responsable du traitement des autres obligations prévues par la loi (respect de la finalité du fichier, sécurité et confidentialité, respect des droits des personnes…).

Les déclarations peuvent être effectuées directement en ligne sur le site de la CNIL à l'adresse suivante : http://www.cnil.fr/vos-responsabilites/declarer-a-la-cnil.

A savoir : Une seule et même déclaration ne peut être effectuée pour plusieurs fichiers ayant des finalités distinctes. Pour déclarer des fichiers de finalités distinctes, il convient de faire une déclaration par finalité.

La gestion des affaires contentieuses

Les avocats agissent dans ce cadre en qualité de responsable de traitement. Ils doivent, par conséquent, déclarer les fichiers qu'ils mettent en œuvre à cette fin (déclaration normale).

Si des données personnelles concernant des personnes physiques sont recueillies directement par les avocats, il convient d'informer les personnes concernées des droits qu'elles tirent de la loi du 6 janvier 1978 modifiée lors de cette collecte.

Dans l'hypothèse inverse, lorsque les données personnelles n'ont pas été directement recueillies par les avocats, aux termes de l'alinéa 1er de l'article 32-III de la loi du 6 janvier 1978 modifiée, le responsable du traitement doit fournir aux personnes concernées les informations mentionnées au I de l'article 32 de la loi susvisée, dès l'enregistrement des données ou, si une communication à des tiers est envisagée, au plus tard lors de la première communication des données.

Lorsque des mesures conservatoires sont nécessaires, notamment pour prévenir la destruction de preuves, l'information de la personne concernée peut intervenir après leur adoption.

3. La déclaration simplifiée

Un grand nombre de fichiers peut faire l'objet de déclarations simplifiées (article 24 de la loi informatique et libertés). Ces dernières peuvent être effectuées directement sur le site internet de la CNIL (http://www.cnil.fr/vos-responsabilites/declarer-a-la-cnil).

Concrètement, il s'agit d'un engagement de conformité à un acte réglementaire préalablement élaboré par la Commission.

4. La demande d'autorisation

Certains traitements relèvent d'un régime d'autorisation préalable de la CNIL. Il s'agit d'un régime plus protecteur, qui s'applique aux fichiers considérés comme « sensibles » ou comportant des risques pour la vie privée ou les libertés individuelles. Une fois obtenue l'autorisation de la CNIL, le traitement doit respecter en tout point le cadre fixé.

En application de l'article 25 de la loi informatique et libertés, la procédure d'autorisation concerne notamment :

- les traitements, automatisés ou non, justifiés par un intérêt public ou appelés à faire l'objet à bref délai d'un procédé d'anonymisation et qui font apparaître, directement ou indirectement, les origines raciales ou ethniques, les opinions politiques, philosophiques ou religieuses, l'appartenance syndicale, ou qui comportent des données relatives à la santé ou à la vie sexuelle ;
- les traitements automatisés portant sur des données génétiques, à l'exception de ceux d'entre eux qui sont mis en œuvre par des médecins ou des biologistes et qui sont nécessaires aux fins de la médecine préventive, des diagnostics médicaux ou de l'administration de soins ou de traitements ;
- les traitements, automatisés ou non, portant sur des données relatives aux infractions, condamnations ou mesures de sûreté, **sauf ceux qui sont mis en œuvre par des auxiliaires de justice pour les besoins de leurs missions de défense des personnes concernées qui relèvent de la procédure de déclaration ;**
- les traitements automatisés susceptibles, du fait de leur nature, de leur portée ou de leurs finalités, d'exclure des personnes du bénéfice d'un droit, d'une prestation ou d'un contrat en l'absence de toute disposition législative ou réglementaire ;
- les traitements automatisés ayant pour objet, d'une part, l'interconnexion de fichiers relevant d'une ou de plusieurs personnes morales gérant un service public et dont les finalités correspondent à des intérêts publics différents ou, d'autre part, l'interconnexion de fichiers relevant d'autres personnes et dont les finalités principales sont différentes ;
- les traitements portant sur des données parmi lesquelles figure le numéro de sécurité sociale ou impliquant la consultation du répertoire national d'identification des personnes physiques ;
- les traitements automatisés de données comportant des appréciations sur les difficultés sociales des personnes ;
- les traitements automatisés comportant des données biométriques nécessaires au contrôle de l'identité des personnes.

Attention : Les interconnexions de fichiers relevant de personnes privées et ayant des finalités distinctes doivent, en vertu de l'article 25-I-5° de la loi du 6 janvier 1978 modifiée, être autorisées par la CNIL, et ce, même si elles sont mises en œuvre par les avocats pour les besoins de leurs missions de défenses de leurs clients.

En vertu de l'article 25-II de la loi du 6 janvier 1978 modifiée, la Commission peut, par une décision unique, autoriser une catégorie de traitements répondant aux mêmes finalités, portant sur des catégories de données identiques et ayant les mêmes catégories de destinataires. Le responsable d'un traitement conforme à cette décision unique peut alors se limiter à adresser à la Commission un engagement de conformité à l'autorisation unique préalablement adoptée.

Les autorisations peuvent être effectuées directement en ligne sur le site à l'adresse suivante : http://www.cnil.fr/vos-responsabilites/declarer-a-la-cnil.

5. La demande d'avis

Les organismes publics qui mettent en œuvre certains types de traitements de données à caractère personnel doivent préalablement recueillir l'avis de la CNIL (articles 26 et 27 de la loi informatique et libertés).

Cette procédure est applicable aux traitements mis en œuvre par des organismes publics, ou des organismes privés gérant un service public, qui concerne :

- la sûreté, la défense ou la sécurité publique ;
- la prévention, la recherche, la constatation ou la poursuite d'infractions pénales ou l'exécution des condamnations pénales ou des mesures de sûreté ;
- l'utilisation du numéro de sécurité sociale ou la consultation du répertoire national d'identification des personnes physiques lorsque les organismes ne sont pas déjà habilités ;
- l'utilisation de données biométriques (empreintes digitales, contour de la main, iris de l'œil, etc.) ;
- le recensement de la population ;
- les téléservices de l'administration.

La demande d'avis doit être accompagnée selon le cas d'un projet de décret en Conseil d'État, d'arrêté ou de décision de l'organe délibérant destiné à autoriser le traitement une fois rendu l'avis de la CNIL.

Les demandes d'avis peuvent être effectuées directement en ligne sur le site à l'adresse suivante : http://www.cnil.fr/vos-responsabilites/declarer-a-la-cnil.

6. Les suites données par la CNIL

Pour les déclarations effectuées sur le site internet de la CNIL, un récépissé électronique est immédiatement envoyé au déclarant ;

Pour les procédures particulières d'autorisation ou d'avis, la CNIL adresse au déclarant une notification de l'autorisation ou de l'avis qu'elle a rendu.

A savoir : La désignation d'un correspondant « informatique et libertés » dispense l'organisme concerné de déclarer ses fichiers auprès de la CNIL, qu'il s'agisse des déclarations normales ou des déclarations simplifiées.

D. Le Correspondant informatique et libertés (CIL) : un vecteur de diffusion de la culture informatique et libertés

1. Le Correspondant informatique et libertés

Introduit en août 2004 à l'occasion de la refonte de la loi informatique et libertés, le correspondant à la protection des données constitue un moyen efficace de veiller à la bonne application de la loi et d'assurer le respect du droit fondamental à la protection des données personnelles. Au 1er octobre 2011 environ 2 200 CIL représentant 8 262 organismes ont été désignés.

Aux termes de l'article 44 du décret du 20 octobre 2005, lorsque moins de cinquante personnes sont chargées de la mise en œuvre de traitements, ou peuvent y accéder directement, le responsable peut désigner un correspondant extérieur à l'organisme concerné. De même, lorsque le responsable des traitements fait partie d'un organisme professionnel ou d'un organisme regroupant des responsables de traitements d'un même secteur d'activité, ce responsable peut désigner un correspondant spécialement mandaté extérieur à l'organisme.

La désignation d'un CIL permet un allègement des formalités préalables. En effet, une fois le correspondant désigné, seuls les traitements soumis à autorisation ou avis préalables de la CNIL devront faire l'objet des formalités adéquates. Les autres traitements n'auront plus qu'à être référencés dans une liste tenue localement par le correspondant.

2. L'avocat Correspondant informatique et libertés

Un avocat peut être désigné en qualité de CIL pour le compte de l'un de ses clients.

Cette désignation n'entraîne pas de risque de violation du secret professionnel, dès lors qu'aucune obligation de dénonciation des manquements constatés n'est mise à la charge du CIL avocat. En effet, à la différence des CIL « classiques » qui doivent dénoncer à la CNIL les manquements qu'ils constatent et ne peuvent résoudre seuls, le CIL avocat à l'interdiction de porter à la connaissance de la Commission les manquements de son client. Il ne peut que se démettre de ses fonctions de CIL si ce dernier refuse de se mettre en conformité.

Un avocat peut également être désigné en tant que CIL du cabinet pour le compte duquel il exerce.

Les conditions dans lesquelles un avocat peut devenir CIL sont précisées à l'article 6.2.2 du règlement intérieur national de la profession (RIN).

Le CIL doit systématiquement informer le responsable des traitements préalablement à toute saisine de la CNIL (art. 49 et 51 du décret). Ainsi, un avocat désigné en qualité de CIL doit, dans le cadre du mandat qui le lie à son client, obtenir son accord préalable avant toute saisine de la CNIL.

Attention : La désignation d'un CIL n'entraîne aucune exonération de responsabilité civile ou pénale pour le responsable de traitement. Un avocat désigné comme CIL est susceptible de voir engager sa responsabilité civile professionnelle.

Ainsi que cela a été précédemment exposé, il existe plusieurs types de formalités préalables à effectuer auprès de la CNIL. Le niveau de complexité de certaines d'entre elles peut justifier l'intervention d'un professionnel du droit, tel qu'un avocat. Cela peut permettre d'accompagner utilement un responsable de traitement dans l'accomplissement des formalités préalables obligatoires prévues par la loi informatique et libertés.

Cet accompagnement apparaît particulièrement utile pour les traitements relevant du régime de l'autorisation préalable.

Le CIL - Informations pratiques

Pourquoi désigner un CIL ?

Sa désignation, qui est facultative, exonère de déclaration la plupart des fichiers. Il contribue à une meilleure application de la loi.

Quels avantages pour l'organisme ?

Le CIL est un acteur de la sécurité juridique au sein de l'organisme. Son action peut prendre plusieurs formes : le conseil, la recommandation, la sensibilisation, la médiation et l'alerte en cas de dysfonctionnement.

Comment désigner un CIL ?

C'est simple, il suffit de compléter en ligne le formulaire de désignation sur le site internet de la CNIL.

Comment le CIL pourrait-il/elle être formé(e) ?

La CNIL propose des ateliers d'information gratuits, généralistes et thématiques, animés par ses propres experts.

Quelle relation avec la CNIL ?

La CNIL a mis en place un service spécifique pour garantir au CIL une réponse rapide et de qualité. Il s'agit d'un guichet unique pour toutes les questions juridiques ou les éclairages liés à l'exercice de la fonction.

D'autres avantages ?

Le CIL est un interlocuteur privilégié de la CNIL. Ses demandes sont donc traitées en priorité.

Il fait partie du réseau des CIL animé par la CNIL.

Il participe à la réflexion liée à l'évolution de la fonction, à la création d'outils de travail, des textes juridiques …

II. FICHES PRATIQUES

Fiche n° 1 : Les fichiers relatifs aux clients

A. Les traitements informatisés concernant des clients potentiels

Le règlement intérieur national de la profession d'avocat interdit toute offre de service personnalisée à destination d'un client potentiel (art. 15 décret n° 2005-790 du 12 juillet 2005 relatif aux règles de déontologie de la profession d'avocat ; art. 10.2 RIN). En principe, les avocats ne peuvent donc effectuer aucune prospection commerciale entendue au sens commun du terme.

Toutefois, les avocats peuvent utiliser certaines formes de publicité, à condition que ces dernières ait été préalablement communiquées à l'ordre, procurent une information au public, respectent les principes essentiels de la profession et ne s'apparentent pas à une forme de démarchage (art. 15 décret du 12 juillet 2005 ; article 10.1 RIN). Des mentions laudatives ou comparatives, de même que des indications relatives à l'identité des clients du cabinet, sont donc impossibles. Du point de vue informatique et libertés, en raison de l'impossibilité de démarcher des clients potentiels, cette situation peut juridiquement s'analyser en une opération de communication externe non commerciale.

Or, en se fondant sur l'article 24-II de la loi informatique et libertés, la CNIL a adopté la dispense de déclaration n° 7 (délibération de la CNIL n° 2006-138 du 9 mai 2006) pour les traitements de données personnelles mis en œuvre par tout organisme privé ou public à des fins d'information et de communication externe, qui exclut toute utilisation commerciale ou politique des données traitées.

> Lors de la collecte des données, les clients potentiels doivent être informés que les données collectées ont pour finalité la constitution et l'exploitation d'un fichier d'adresses à des fins d'information ou de communication externe et doivent être mis en mesure de s'y opposer.

Cette dispense prévoit que seules peuvent être enregistrées les données relatives à l'identité, à la vie professionnelle et aux centres d'intérêts des personnes concernées, à l'exception des données dites sensibles (origines raciales ou ethniques, opinions politiques, philosophiques ou religieuses, appartenance syndicale, état de santé ou vie sexuelle).

Les données peuvent être conservées pendant toute la durée nécessaire à la réalisation des opérations de communication externe et une mise à jour annuelle doit être assurée.

Si les cabinets d'avocats se conforment à ces prescriptions dans le cadre de leurs relations avec des clients potentiels, aucune déclaration ne doit être effectuée auprès de la CNIL. Dans l'hypothèse inverse, il convient d'adresser à la CNIL une déclaration normale ou, pour les traitements relevant de l'article 25 de la loi informatique et libertés, une demande d'autorisation.

Rappel : Etre dispensé de déclaration n'exonère pas des obligations que la loi informatique et libertés impose aux responsables de traitement. Quel que soit le régime déclaratif applicable, il convient d'informer les personnes concernées des objectifs poursuivis, du caractère obligatoire ou facultatif de leurs réponses, des destinataires des données, des modalités d'exercice des droits d'accès, d'opposition et de rectification, ainsi que de garantir la sécurité des données.

B. Les traitements informatisés concernant les clients du cabinet

1. Une dispense de déclaration des traitements constitués à des fins d'information de la clientèle

Il a été précédemment indiqué que la CNIL a adopté une dispense de déclaration pour les traitements mis en œuvre à des fins d'information ou de communication externe (dispense de déclaration n° 7).

Les campagnes d'information non commerciales à destination des clients d'un cabinet d'avocats, par exemple sur l'actualité juridique ou la vie du cabinet, peuvent également relever de cette dispense de déclaration, sous réserve d'en respecter les conditions.

2. Une déclaration simplifiée pour les opérations de gestion de la clientèle les plus courantes

En application de l'article 24-I de la loi informatique et libertés, la CNIL a adopté la norme simplifiée n° 48 (délibération de la CNIL n° 2005-112 du 7 juin 2005) qui permet aux responsables de traitement d'effectuer une déclaration simplifiée pour certains des traitements relatifs aux personnes avec lesquelles des relations contractuelles sont nouées.

Les opérations relatives à la gestion des clients qui concernent les contrats, les commandes, les livraisons, les factures et la comptabilité, en particulier la gestion des comptes clients, sont couvertes par cette norme.

Les logiciels de facturation au temps passé utilisés par les cabinets d'avocats relèvent de cette norme, sous réserve de respecter les garanties prévues par la norme simplifiée n° 48. A défaut, il convient d'effectuer une déclaration normale.

Dès lors, les cabinets d'avocats peuvent, en respectant les finalités mentionnées ci-dessus, collecter et traiter les données relatives :

- à l'identification des clients : nom, prénoms, adresse, numéros de téléphone et de télécopie, adresse de courrier électronique, date de naissance, code interne de traitement permettant l'identification du client (ce code doit être

distinct du numéro de sécurité sociale ou du numéro de carte bancaire) ;

- aux moyens de paiement (relevé d'identité postale ou bancaire, numéro de la transaction, numéro de chèque, numéro de carte bancaire) ;
- à la situation familiale, économique et financière des clients (vie maritale, nombre et âge des enfants du foyer, profession, domaine d'activité, catégorie socio-professionnelle) ;
- à la relation commerciale ;
- aux règlements des factures ;

Les courriers de relance consécutifs au non paiement de factures, ainsi que l'activité du service chargé du suivi des règlements, relèvent de la norme simplifiée n° 48. Tel n'est pas le cas des traitements ayant pour finalité la constitution d'une liste de mauvais payeurs (Cf. infra).

Les clients doivent être informés, au moment de la collecte de leurs données, de l'identité du responsable du traitement, des finalités poursuivies, du caractère obligatoire ou facultatif des réponses à apporter, des conséquences éventuelles à leur égard d'un défaut de réponse, des destinataires des données, de leurs droits d'accès, de rectification et d'opposition pour des motifs légitimes au traitement de leurs données ainsi que, le cas échéant, des transferts de données à caractère personnel envisagés à destination d'un État non membre de l'Union européenne.

Il convient, en outre, de veiller à ce que ne puissent accéder à ces informations que les avocats en charge des dossiers correspondants et, le cas échéant, les personnes chargées du service commercial, des services administratifs et du contrôle (interne et externe), ainsi que les entreprises extérieures liées contractuellement pour l'exécution d'un contrat.

En raison de l'obligation de confidentialité renforcée qui pèse sur les avocats, **aucune cession, vente ou location de ces données ne peut être envisagée,** et ce, alors même que la norme simplifiée n° 48 précise que les informations relatives à la situation familiale, économique et financière peuvent être cédées, louées ou échangées dès lors que les organismes destinataires s'engagent à ne les exploiter que pour s'adresser directement aux intéressés pour des finalités exclusivement commerciales.

Les informations ne peuvent être conservées au-delà de la durée strictement nécessaire à la gestion de la relation commerciale, à l'exception de celles nécessaires à l'établissement de la preuve d'un droit ou d'un contrat qui peuvent être archivées, conformément aux dispositions de la recommandation de la CNIL n°2005-213.

Enfin, le responsable du traitement doit prendre toutes les précautions utiles pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées ou que des tiers non autorisés y aient accès.

La norme simplifiée n° 48 autorise les **transferts de données** personnelles relatives à la gestion des fichiers clients **vers des pays non-membres de l'Union européenne,** à condition qu'ils garantissent un niveau suffisant de protection. Ce niveau peut-être obtenu notamment par la mise en œuvre des clauses contractuelles types de la Commission européenne ou de règles internes ayant fait l'objet d'une décision favorable de la CNIL. Le responsable du traitement doit clairement informer les personnes concernées du transfert, de sa finalité, des données transmises, des destinataires ainsi que des moyens d'encadrement mis en place.

3. Une déclaration normale pour les autres traitements ayant trait à la clientèle

En application de l'article 22-I de la loi informatique et libertés, les traitements qui ne relèvent pas des dispositions de ses articles 25, 26 et 27, d'une dispense de déclaration ou d'une norme simplifiée doivent être déclarés à la CNIL avant leur mise en œuvre.

Cette déclaration peut être effectuée par voie électronique.

Les traitements, automatisés ou non, portant sur des **données relatives aux infractions, condamnations ou mesures de sûreté** peuvent être mis en œuvre par les auxiliaires de justice pour les besoins de l'exercice des missions qui leur sont confiées par la loi (art. 9-2° de la loi informatique et libertés). Ils n'ont pas à être préalablement autorisés par la CNIL mais doivent lui être déclarés au moyen d'une déclaration normale (art. 25-I-3° de la loi informatique et libertés).

A titre illustratif, les **traitements** informatiques mis en œuvre par les cabinets d'avocats **pour éviter qu'un conflit d'intérêts** surgisse à l'occasion de l'exercice de leurs missions de conseil, de représentation et de défense, doivent être déclarés à la CNIL.

De même, les traitements dits de « **Client Relationship Management** » (CRM), qui s'apparentent à des annuaires partagés de clients intégrant un historique des relations de ces derniers avec le cabinet, relèvent de la norme simplifiée n° 48 ou, si le traitement mis en œuvre ne correspond pas au champ défini par celle-ci, du régime de la déclaration normale.

Il faut veiller à ce qu'un éventuel espace « champ libre » des CRM ne contienne aucune appréciation subjective sur les clients.

4. Une autorisation préalable de la CNIL pour les traitements listés à l'article 25 de la loi informatique et libertés :

Les traitements portant sur des données relatives aux infractions, condamnations ou mesures de sûreté qui sont mis en œuvre par les avocats pour les besoins de leur mission de défense des justiciables, n'ont pas à être préalablement autorisés par la CNIL. Il existe néanmoins des cas dans lesquels les cabinets doivent solliciter une autorisation de la CNIL.

Il en est ainsi, notamment, lorsque la mission de défense d'un client ne peut être avancée comme finalité et que le traitement en cause est susceptible d'exclure une personne d'un droit, d'une prestation ou d'un contrat en l'absence de toute disposition législative ou réglementaire, ou que des fichiers sont interconnectés.

a - Le cas des listes d'exclusion

Une liste d'exclusion, plus communément appelée liste noire, est un fichier recensant des personnes indésirables. Si aucune disposition légale ou réglementaire n'interdit la constitution de telles listes, le risque d'exclusion et de marginalisation des personnes fichées a néanmoins conduit le législateur à encadrer leur mise en œuvre.

Ainsi, l'article 25 I-4° de la loi informatique et libertés dispose :

« Sont mis en œuvre après autorisation de la CNIL […] les traitements automatisés susceptibles, du fait de leur nature, de leur portée ou de leurs finalités, d'exclure des personnes d'un droit, d'une prestation ou d'un contrat en l'absence de toute disposition législative ou réglementaire ».

La mise en œuvre de **traitements automatisés visant à éviter les conflits d'intérêts** entre plusieurs clients d'un cabinet peuvent conduire à la constitution de liste d'exclusion. Toutefois, ces traitements ne sont pas soumis à une autorisation de la CNIL, en raison de l'existence d'une disposition les prévoyant (art. 7 décret n°2005-790 du 12 juillet 2005 relatif aux règles de déontologie de la profession d'avocat ; art. 4.1 RIN). Ils doivent cependant faire l'objet d'une déclaration normale.

Si un cabinet d'avocats, au-delà de la gestion des relances et des impayés, envisage d'établir un fichier pour lister les clients que le cabinet ne souhaite plus conseiller ou représenter, en raison d'un risque de non paiement des honoraires par exemple, une autorisation préalable doit être sollicitée auprès de la CNIL. De la même manière, la constitution d'une liste d'exclusion de stagiaires ou de collaborateurs indélicats devrait, le cas échéant, également être autorisée par la CNIL.

A cet égard, la Commission recommande que l'inscription d'une personne ou l'enregistrement de données la concernant dans un fichier destiné à recenser des mauvais payeurs repose sur des motifs objectivement vérifiables, d'une part, et fasse abstraction de tout jugement de valeur ou appréciation de son comportement, d'autre part.

Les motifs d'inscription doivent être préétablis et l'inscription doit être effectuée par des agents habilités disposant de moyens pour vérifier le caractère certain du manquement imputé à la personne concernée.

Il convient, en outre, d'assurer une gestion rigoureuse des habilitations et des contrôles d'accès, ainsi que de définir une politique de journalisation et de gestion des mots de passe afin de se prémunir contre les risques d'intrusion et de détournement.

Afin de garantir le droit à l'oubli, dont le principe est tiré des dispositions de l'article 6 de la loi du 6 janvier 1978 modifiée, les durées de conservation des données doivent être proportionnées au regard des motifs de l'inscription.

Des procédures de mise à jour régulières doivent ainsi être mises en place, afin de garantir que l'inscription dans une liste noire sera supprimée dès régularisation de l'incident. En cas de non régularisation, le maintien de l'inscription ne peut toutefois être considéré comme proportionné que s'il est assorti d'une limite raisonnable dans le temps.

Eu égard à la protection particulière du droit reconnu à tous d'être assisté ou représenté en justice par un avocat et à la protection de ces données par le secret professionnel (art. 2 du RIN), la mutualisation de listes noires entre l'ensemble des cabinets d'avocats n'est pas envisageable.

b - Le cas des interconnexions de fichiers

L'article 25-I-5° de la loi informatique et libertés dispose :

« Sont mis en œuvre après autorisation de la CNIL […] les traitements automatisés ayant pour objet :

- *l'interconnexion de fichiers relevant d'une ou plusieurs personnes morales gérant un service public et dont les finalités correspondent à des intérêts publics différents ;*
- *l'interconnexion de fichiers relevant d'autres personnes et dont les finalités principales sont différentes. »*

Les cabinets qui envisagent d'interconnecter des fichiers de finalités distinctes doivent, dès lors, solliciter une autorisation de la CNIL.

Ils seront ainsi invités à adresser à la CNIL un organigramme fonctionnel de l'application en vue de permettre un contrôle, par le service de l'expertise de la Commission, des différents processus d'interrogation et d'intégration des données issues de fichiers extérieurs.

Le service juridique vérifiera, ensuite, qu'aucune décision ne peut être fondée sur la seule base de ce traitement automatisé conformément aux dispositions de l'article 10 de la loi du 6 janvier 1978 modifiée.

Fiche n° 2 : L'accès au dossier professionnel

Par principe, tout salarié, ancien salarié ou collaborateur justifiant de son identité a le droit d'accéder à son dossier professionnel auprès du service du personnel.

1. Un droit d'accès à quelles données ?

L'intéressé peut obtenir communication de l'ensemble des données le concernant, qu'elles soient conservées sur support informatique ou sur un support papier. Par exemple, il a le droit d'accéder aux données relatives à :

- son recrutement ;
- son historique de carrière ;
- sa rémunération ;
- l'évaluation de ses compétences professionnelles (entretiens d'évaluation, notation).

2. Limites au droit d'accès

Un salarié, ancien salarié ou collaborateur n'a pas le droit d'accéder :

- aux données concernant la situation personnelle d'un tiers ;
- aux données prévisionnelles de carrière qui n'ont pas été utilisées pour prendre une décision le concernant (potentiel de carrière, classement ou « ranking ») ;

Par exception, il est possible d'accéder aux données prises en compte pour décider d'une augmentation de rémunération, d'une promotion, d'une affectation ou, plus généralement, à toute donnée ayant servi à prendre une décision à l'égard d'un membre du cabinet.

Il est possible de s'opposer aux demandes manifestement abusives (demandes répétitives …). En cas de contestation, il convient de pouvoir démontrer ce caractère manifestement abusif.

3. Comment s'exerce le droit d'accès ?

Le droit d'accès peut s'exercer sur place ou par écrit.

Il faut répondre immédiatement si la demande est effectuée sur place ou dans un délai maximal de 2 mois si la demande est écrite (ou s'il est impossible de répondre immédiatement à la demande sur place). Un éventuel refus doit être écrit, motivé et mentionner les voies et délais de recours.

Une copie des données est délivrée à l'intéressé à sa demande. Seul le coût de la copie peut éventuellement lui être réclamé.

Les codes, sigles et abréviations figurant dans les documents communiqués doivent être expliqués, si nécessaire à l'aide d'un lexique.

Comment déclarer les dossiers professionnels ?

La norme simplifiée n° 46 concerne, notamment, la gestion des dossiers professionnels des employés tenus conformément aux dispositions législatives et réglementaires, ainsi qu'aux dispositions statutaires, conventionnelles ou contractuelles qui régissent les intéressés. Il faut procéder à un engagement de conformité en référence à cette norme, sauf si un correspondant informatique et libertés a été désigné (dispense de déclaration dans ce dernier cas).

Fiche n° 3 : Le contrôle de l'activité des membres du cabinet

Afin d'assurer la sécurité de leur réseau et/ou de leurs ressources informatiques, les cabinets d'avocats peuvent être amenés à mettre en place des outils visant à contrôler l'utilisation des logiciels informatiques mis à disposition de leurs membres.

Ce contrôle est légitime s'il est réalisé de manière transparente, c'est-à-dire avec une parfaite information des utilisateurs. La rédaction d'une Charte d'utilisation des outils informatiques apparaît particulièrement utile pour rappeler les obligations mutuelles du cabinet et des utilisateurs, définir les modalités de contrôle et les sanctions auxquelles s'exposerait un utilisateur qui ne respecterait pas les règles d'utilisation.

Attention ! Les traitements de contrôle de l'activité des membres de cabinets d'avocats peuvent concerner les salariés d'un cabinet. En ce qui concerne les collaborateurs libéraux, l'absence de tout lien de subordination associée à leur indépendance (art. 7 de la loi n° 71-1130 du 31 décembre 1971 modifié par la loi n° 2005-882 du 2 août 2005 ; art. 1er et 14 du RIN) exclut en principe tout contrôle de leur activité, notamment à l'occasion des échanges avec leur clientèle personnelle. Il est donc nécessaire de prendre en compte les principes essentiels régissant la profession d'avocat dans la Charte d'utilisation des outils informatiques.

A. Le contrôle du temps passé sur les dossiers

Pour facturer ses prestations, un cabinet d'avocat peut mettre en place un logiciel de facturation permettant de calculer le temps passé sur les dossiers et d'identifier les diligences accomplies. Ce logiciel a une finalité spécifique qui ne saurait être détournée à des fins de contrôle de l'activité des membres du cabinet.

Ce type de logiciel est soumis au régime de la déclaration normale, conformément à l'article 22 de la loi du 6 janvier 1978 modifiée.

B. L'accès aux dossiers contenus dans un poste informatique

Le cas des fichiers et des répertoires créés par un salarié

Il a été jugé que les fichiers créés par un salarié grâce à l'outil informatique mis à sa disposition par son employeur sont présumés avoir un caractère professionnel, sauf s'ils sont identifiés comme étant personnels, de sorte que l'employeur peut y accéder hors la présence du salarié (Cass. soc. 18 octobre 2006, pourvois n°04-48025 et 04-47400). Il convient de préciser que l'identification d'un dossier par les initiales d'un salarié ne permet pas de le considérer comme étant personnel (Cass. soc. 21 octobre 2009, pourvoi n°07-43877).

Si un fichier est identifié comme étant personnel, l'employeur ne peut y avoir accès « ***qu'en présence du salarié ou si celui-ci a été dûment appelé, ou en cas de risque ou événement particulier*** **»**. Le salarié ne peut pas s'opposer à un tel accès si ces conditions ont été respectées.

Le contrôle d'un poste informatique doit se faire à l'exclusion de toute considération morale. La chambre sociale de la Cour de cassation considère en effet que *« la seule conservation sur son poste informatique de trois fichiers contenant des photos à caractère pornographique sans caractère délictueux ne constituait pas, en l'absence de constatation d'un usage abusif affectant son travail, un manquement du salarié aux obligations résultant de son contrat susceptible de justifier son licenciement »* (Cass. Soc. 8 décembre 2009, n° 08-42097).

Il n'est cependant pas impossible d'interdire aux salariés de détenir de telles images sur leurs postes informatiques professionnels. La détention d'images pornographiques sur un poste informatique professionnel peut être sanctionnée, si une Charte informatique intégrée au règlement intérieur le prévoit (Cass. soc. 15 décembre 2010, pourvoi n° 09-42691).

Les collaborateurs et les salariés sont-ils tenus de communiquer leurs mots de passe ?

Les mots de passe constituent des mesures de sécurité visant à protéger les données figurant dans les postes informatiques. Ils doivent être fréquemment modifiés et, en principe, ne pas être portés à la connaissance de tiers.

Toutefois, si un membre du cabinet détenant sur son poste informatique des informations nécessaires à la poursuite de l'activité est absent, il est possible de lui demander de communiquer son mot de passe et, le cas échéant, de passer outre son refus. L'associé ou le collaborateur mandaté pour récupérer ces informations ne doit toutefois pas accéder au contenu personnel de l'intéressé et, notamment, aux informations concernant l'éventuelle clientèle personnelle d'un avocat collaborateur. Dans cette hypothèse, le recours aux services d'un administrateur réseau, soumis à une obligation de confidentialité vis-à-vis de son employeur, serait ainsi préférable.

La CNIL recommande que les modalités d'accès aux données stockées sur l'environnement informatique d'une personne absente soient préalablement définies en concertation et diffusées auprès des personnes susceptibles d'être concernées (via une Charte par exemple).

Comment organiser la fermeture du compte utilisateur lors du départ d'un collaborateur ou d'un salarié ?

Il est souhaitable que les modalités de fermeture d'un compte soient prévues dans une Charte informatique. Il est notamment recommandé d'avertir la personne concernée de la date de fermeture de son compte afin qu'elle puisse vider son espace privé.

C. Le contrôle de l'utilisation d'internet et des messageries électroniques

Pour l'exercice de leur activité professionnelle, les salariés et les collaborateurs libéraux ont généralement à disposition un poste de travail informatique connecté à internet et doté d'une messagerie électronique.

L'utilisation sur le lieu de travail de ces outils à des fins autres que professionnelles est généralement tolérée. Elle doit rester raisonnable et ne doit pas affecter la sécurité des réseaux ou la productivité du cabinet.

Après l'information et la consultation des instances représentatives du personnel**,** lorsqu'elles existent, les membres du cabinet doivent être individuellement informés de la finalité et des modalités du dispositif de contrôle, ainsi que de la durée de conservation des données de connexion. L'information des personnes peut se faire par la diffusion d'une Charte d'utilisation des réseaux.

La CNIL recommande une durée de conservation ne dépassant pas six mois. En cas d'archivage automatique des messages électroniques, les salariés et les collaborateurs salariés doivent également être informés de la durée de conservation des messages, des modalités d'archivage et d'exercice de leurs droits. Les messages électroniques identifiés comme étant personnels ne doivent pas être archivés.

Le contrôle de l'utilisation d'internet

Un cabinet d'avocat peut fixer des conditions et limites à l'utilisation d'internet, lesquelles ne constituent pas, en soi, des atteintes à la vie privée de ses membres.

A titre illustratif, il est possible de mettre en place des dispositifs de filtrage des sites non autorisés (à caractère pornographique, pédophile, incitant à la haine raciale …). Un cabinet peut également fixer des limites dictées par une exigence de sécurité, telles que l'interdiction de télécharger des logiciels, de se connecter à un forum, d'utiliser un « chat », ou d'accéder à une boîte aux lettres personnelle compte tenu des risques de virus qu'un tel accès est susceptible de présenter.

Comment déclarer : Lorsqu'un cabinet met en place un dispositif de contrôle individuel des salariés destiné à produire un relevé des connexions ou des sites visités, poste par poste, le traitement mis en œuvre doit être déclaré à la CNIL **(déclaration normale**), sauf si un correspondant informatique et libertés a été désigné en son sein.

Si un cabinet décide de mettre en place un dispositif ne permettant pas de contrôler individuellement l'activité des salariés, ce dispositif peut faire l'objet d'une déclaration de conformité en référence à la **norme simplifiée n° 46**.

Le contrôle de l'utilisation de la messagerie

Une communication électronique pouvant avoir le caractère d'une correspondance privée, elle est protégée par le secret des correspondances (art. 226-15 et 432-9 du code pénal).

Les courriels émis ou reçus grâce à un outil informatique professionnel sont toutefois présumés avoir un caractère professionnel, à moins d'être clairement identifiés comme étant « ***personnels*** » (Cass. soc. 30 mai 2007, pourvoi n°05-43102). À défaut d'une telle identification, l'employeur peut y accéder en dehors de la présence du salarié.

Il appartient ainsi aux salariés et collaborateurs salariés d'identifier leurs messages personnels en les nommant comme tels.

Si un message non identifié comme personnel s'avère relever en réalité de la vie privée de la personne concernée, ce message ne peut être utilisé à l'appui d'une sanction (Cass. soc. 5 juillet 2011, pourvoi n°10-17284).

Les messages électroniques adressés ou reçus par les collaborateurs libéraux, qu'ils soient professionnels ou personnels, ne peuvent être consultés par un tiers non autorisés.

Comment déclarer

Si un dispositif de contrôle individuel n'est pas mis en place, une messagerie professionnelle peut faire l'objet d'un engagement de conformité en référence à la **norme simplifiée n° 46**.

Dans l'hypothèse inverse, le traitement doit être déclaré à la CNIL (déclaration normale), sauf désignation d'un correspondant informatique et libertés au sein du cabinet.

D. Le contrôle de la téléphonie

Les « Smartphones », ou téléphones intelligents, proposent des applications et des services qui utilisent des informations sensibles qui peuvent concerner tant les membres du cabinet que les clients (localisation, mails, contacts, pièces jointes, agendas, comptabilités …).

Afin de prévenir le risque de détournement de ces informations, un cabinet doit, par conséquent, prendre toutes les précautions utiles pour s'assurer de leur confidentialité.

A cet égard, il est souhaitable que les avocats protègent l'utilisation de leurs téléphones par un code de verrouillage après une courte période d'inactivité, le code PIN de la carte SIM ne suffisant pas.

1. L'utilisation du téléphone

Un usage personnel du téléphone sur le lieu de travail est toléré à condition que cette utilisation demeure raisonnable et non préjudiciable pour le cabinet.

Il est dès lors légitime de s'assurer de ce caractère non abusif. Le contrôle doit toutefois s'opérer dans des conditions propres à garantir le respect de la vie privée et des libertés de chacun.

La mise en place d'autocommutateurs

Les autocommutateurs sont des standards téléphoniques qui permettent d'orienter l'ensemble des communications téléphoniques. Ils peuvent servir à la comptabilisation statistique des flux entrants et sortants au niveau du cabinet, d'un département, d'un service ou d'un poste en particulier. Reliés à des logiciels « de taxation », ils peuvent également permettre d'imputer et de contrôler les dépenses téléphoniques du cabinet.

Ces appareils pouvant enregistrer les numéros de téléphone composés, ou celui d'un interlocuteur, ils sont susceptibles d'être utilisés pour identifier les communications relevant d'un usage non professionnel.

Lorsque des relevés sont établis, les quatre derniers chiffres des numéros composés doivent par défaut être occultés.

En cas d'utilisation manifestement abusive du téléphone au regard de son utilisation moyenne au sein du cabinet, un relevé justificatif complet des numéros composés ou des services de téléphonie utilisés peut toutefois être établi par le responsable de la personne concernée. Cette dernière doit avoir la possibilité d'apporter d'éventuelles explications.

La CNIL recommande que la durée de conservation des données relatives à l'utilisation des services de téléphonie n'excède pas un an.

La situation des salariés protégés

Il est **interdit de contrôler les appels** émis ou reçus par les personnes investies d'un mandat de représentation du personnel, lorsqu'elles sont dans le cadre de l'exercice de leur mandat.

Depuis un arrêt de la Cour de cassation du 6 avril 2004, les employés investis d'un mandat électif ou syndical doivent disposer d'un matériel excluant l'interception de leurs communications téléphoniques et l'identification de leurs correspondants.

Il convient ainsi, par exemple, de leur mettre à disposition un poste téléphonique non connecté à l'autocommutateur ou disposant d'une fonction de désactivation de ce dernier.

Comment déclarer ?

Les fichiers mis en œuvre dans le cadre de l'utilisation d'un service de téléphonie fixe ou mobile peuvent être déclarés par un engagement de conformité à la **norme simplifiée n° 47**.

Si le dispositif excède le cadre prévu par cette norme, le cabinet doit effectuer une déclaration normale sauf s'il a désigné un correspondant informatique et libertés en son sein. Dans ce dernier cas, il est en effet dispensé de déclaration.

2. L'enregistrement et l'écoute de conversations téléphoniques

Il est possible de procéder à l'enregistrement et à l'écoute d'une conversation téléphonique tenue par un salarié sur son lieu de travail, **sous réserve de l'application des principes essentiels régissant la profession d'avocat**.

L'écoute clandestine de conversations tenues entre un avocat collaborateur et sa clientèle personnelle apparaît quant à elle impossible.

Quelles garanties pour les salariés ?

Après l'information et la consultation préalable des institutions représentatives du personnel (voir notamment l'art. L.2323-33 du code du travail pour l'information obligatoire du comité d'entreprise sur les moyens et techniques de contrôle de l'activité), les salariés et leurs interlocuteurs doivent être informés de la mise en place du dispositif, de son objectif, de ses conséquences individuelles éventuelles, des destinataires des enregistrements, ainsi que des modalités d'exercice de leurs droits d'accès.

L'enregistrement ainsi que l'écoute de conversations de salariés ne peuvent être des opérations permanentes, sauf législation particulière l'imposant. Ces opérations ne peuvent être réalisées qu'en cas de nécessité reconnue et doivent être

proportionnées au but recherché. Il peut s'agir, par exemple, d'un enregistrement limité dans le temps à des fins de formation ou d'évaluation des compétences.

Les employés doivent disposer de lignes téléphoniques non reliées au système d'enregistrement ou d'un dispositif technique leur permettant, en cas de conversation privée, de se mettre hors du champ du dispositif d'enregistrement, tant pour les appels entrants que sortants.

Les employés investis d'un mandat électif ou syndical doivent disposer d'un matériel excluant l'interception de leurs communications téléphoniques et l'identification de leurs correspondants, par exemple via une ligne non connectée à l'autocommutateur ou ne pouvant donner lieu à la production d'une facturation détaillée.

Lorsqu'un enregistrement est réalisé à des fins de formation, la CNIL recommande une durée de conservation maximale de 6 mois.

Comment déclarer ?

L'enregistrement de conversations téléphoniques doit faire l'objet d'une déclaration normale auprès de la CNIL si le dispositif repose sur des moyens numériques.

L'écoute de conversations téléphoniques doit, quant à lui, faire l'objet d'une déclaration normale auprès de la CNIL si elle est suivie d'un compte rendu ou d'une grille d'analyse.

En cas de désignation d'un correspondant informatique et libertés, aucune déclaration n'est nécessaire.

E. Les frais professionnels

Les frais de déplacement

Dans le cadre de leurs missions, les avocats peuvent être amenés à recourir à des services de transport (taxi, train, avion…). Ces services peuvent faire l'objet d'un abonnement et d'un décompte financier facturable aux clients.

Dans le cadre du contrôle des notes de frais que le Cabinet doit être en mesure de produire à ses clients, le contrôle des déplacements effectués par des membres du cabinet doit avoir pour unique finalité de rendre la facturation transparente.

Attention ! Tout déplacement facturé à un client est présumé revêtir un caractère professionnel. Dès lors, le contrôle de ces déplacements grâce à un compte ouvert dans une entreprise de transport n'est pas susceptible, par principe, de porter atteinte à la vie privée des collaborateurs.

Néanmoins, conformément à l'article 32 de la loi du 6 janvier 1978 modifiée, les avocats doivent être informés des conditions d'un éventuel contrôle de leurs déplacements.

Les « frais de bouche »

Les avocats peuvent se voir rembourser une partie forfaitaire de leurs « frais de bouche ». Ces services peuvent faire l'objet d'une facturation et d'une comptabilité à part entière.

Tout déjeuner ou diner facturé étant présumé revêtir un caractère professionnel, le contrôle de ces frais n'est pas susceptible de porter atteinte à la vie privée des collaborateurs.

Néanmoins, les avocats doivent être informés des éventuelles modalités de contrôle.

Les traitements informatisés ayant trait aux frais professionnels des avocats doivent faire l'objet d'une **déclaration normale**, dès lors qu'ils permettent un contrôle individuel de leur activité.

Fiche n° 4: Le contrôle de l'accès aux locaux

Sur le lieu de travail, les associés agissant en qualité d'employeur peuvent être amenés à contrôler les accès aux locaux ou la gestion de la restauration (badges électroniques, dispositifs biométriques ou encore vidéoprotection).

A. L'utilisation de badges sur le lieu de travail

Des badges électroniques (cartes magnétiques ou à puce) peuvent servir au contrôle des accès aux locaux ou à la gestion de la restauration.

Ces dispositifs, qui comportent des données permettant l'identification des personnes concernées, sont soumis à la loi informatique et libertés. Ils doivent donc être déclarés à la CNIL sauf désignation d'un correspondant informatique et libertés.

Quelles garanties prévoir ?

Chaque passage du badge dans un lecteur permet l'enregistrement de données relatives à son détenteur. Ces enregistrements présentent des risques d'utilisation détournée et sont susceptibles de tracer les déplacements des avocats et salariés à des fins de surveillance.

Des garanties particulières doivent donc être apportées par le cabinet pour éviter de tels détournements. Il convient notamment de préciser :

- la finalité du dispositif (ex : contrôle des accès, gestion des temps de présence des salariés, gestion de la restauration …) ;
- les informations collectées ;
- les services destinataires des données ;
- les modalités d'exercice des droits d'accès et de rectification aux données.

Les membres d'un cabinet d'avocats doivent être parfaitement informés de ces modalités, préalablement à la mise en œuvre du système (Cf. modèle proposé en annexe).

Comment déclarer ?

Si le dispositif envisagé respecte en tous points le cadre fixé par la **norme simplifiée n° 42**, le cabinet peut effectuer un simple engagement de conformité à cette norme, sauf désignation d'un correspondant informatique et libertés qui l'exonérerait de déclaration. A défaut, il devra effectuer une déclaration normale.

B. La biométrie sur le lieu de travail

Les dispositifs biométriques, parce qu'ils permettent d'identifier une personne par ses caractéristiques physiques, biologiques voire comportementales, sont particulièrement sensibles et soumis à un contrôle particulier de la CNIL.

Ces dispositifs ne peuvent être mis en œuvre sans autorisation préalable de la CNIL.

1. Le cadre juridique

Tous les dispositifs de reconnaissance biométrique sont soumis à une autorisation préalable de la CNIL, quel que soit le procédé technique utilisé (contour ou forme de la main, empreinte digitale, réseau veineux …).

Il appartient à chaque cabinet d'avocats d'adresser une demande d'autorisation à la CNIL ou, le cas échéant, un engagement de conformité à une autorisation unique.

2. Des formalités allégées pour certains dispositifs biométriques

La CNIL a élaboré des autorisations uniques pour certains dispositifs biométriques. Lorsqu'un cabinet souhaite mettre en œuvre un dispositif biométrique répondant aux conditions de ces autorisations, il lui suffit d'adresser à la Commission un simple engagement de conformité.

La procédure d'autorisation unique peut concerner les dispositifs biométriques reposant sur la reconnaissance :

- du contour de la main pour assurer le contrôle d'accès et la gestion des horaires et de la restauration sur les lieux de travail (autorisation unique n°7) ;
- de l'empreinte digitale, exclusivement enregistrée sur un support individuel détenu par la personne concernée, pour contrôler l'accès aux locaux professionnels (autorisation unique n°8) ;
- du réseau veineux des doigts de la main pour le contrôle de l'accès aux locaux sur les lieux de travail (autorisation unique n°19) ;
- de l'empreinte digitale pour le contrôle de l'accès aux postes informatiques portables professionnels (autorisation unique n°27).

Attention : L'utilisation de dispositifs de reconnaissance biométrique, pour la gestion des contrôles d'accès aux locaux, des horaires et de la restauration ne peut être déclarée en référence à la norme simplifiée n° 42, relative aux traitements de contrôle d'accès.

3. La nécessaire information préalable des intéressés

Les personnes concernées par un dispositif biométrique doivent être clairement informées de ses conditions d'utilisation, de son caractère obligatoire ou

facultatif, des destinataires des informations et des modalités d'exercice de leurs droits d'opposition, d'accès et de rectification (Cf. modèle proposé en annexe).

En outre, conformément au code du travail, les institutions représentatives du personnel doivent, le cas échéant, être consultées et informées avant la mise en œuvre du dispositif.

4. Comment déclarer ?

Si le dispositif biométrique est conforme à l'une des autorisations uniques adoptées par la CNIL, il suffit d'adresser à la Commission une simple déclaration de conformité qui peut s'effectuer directement sur son site internet.

Les traitements ne relevant pas de l'une de ces autorisations uniques doivent faire l'objet d'une demande d'autorisation disponible en ligne sur le site de la CNIL

B. La vidéoprotection

Une réflexion préalable à l'installation d'un système de vidéoprotection, basée sur une analyse précise des risques tenant compte des incidents éventuellement survenus, doit être menée afin d'identifier des solutions alternatives pour le cabinet. Une sécurisation des accès au moyen de badges magnétiques peut, par exemple, constituer une réponse adaptée à l'objectif poursuivi.

Le déploiement de caméras sur un lieu de travail doit répondre à un fort impératif de sécurité pour des personnes ou des zones de travail exposées à un risque particulier. Il ne peut avoir pour objectif la mise sous surveillance spécifique d'un ou plusieurs salariés.

La mise en œuvre de dispositifs de vidéoprotection doit nécessairement s'effectuer de façon adéquate, pertinente, non excessive et strictement nécessaire par rapport à l'objectif poursuivi.

Le nombre, l'emplacement, l'orientation, les fonctionnalités, les périodes de fonctionnement ou encore la nature des tâches accomplies par les personnes filmées sont autant d'éléments à prendre en compte lors de l'évaluation du caractère proportionné du système.

L'état actuel du droit se caractérise par la concurrence de deux régimes juridiques distincts. Celui de la loi du 6 janvier 1978 modifiée (déclaration normale), ainsi que celui de l'article 10 de la loi du 21 janvier 1995 modifiée d'orientation et de programmation pour la sécurité (autorisation préfectorale). Le régime juridique applicable en matière de vidéoprotection peut, dès lors, s'avérer complexe à appréhender.

Une circulaire du Premier ministre en date du 14 septembre 2011 (NOR : PRMX1124533C) relative au cadre juridique applicable à l'installation de caméras de vidéoprotection sur la voie publique et dans des lieux ou établissements ouverts au public, d'une part, et dans des lieux non ouverts au public, d'autre

part, apporte des précisions sans toutefois résoudre l'ensemble des difficultés.

Pour connaitre la formalité applicable, il convient de déterminer si le dispositif concerne un lieu public (ou un lieu ouvert au public) ou un lieu privé (ou un lieu non ouvert au public).

A savoir : La CNIL est compétente pour contrôler tous les systèmes de vidéoprotection, qu'ils soient installés dans des lieux publics ou dans des lieux fermés au public.

Le régime juridique peut se présenter de la manière suivante :

- **Lieu ouvert au public** : seule une **autorisation préfectorale** est nécessaire si le système de vidéoprotection est installé dans un lieu auquel le public peut accéder librement (ex : accueil du cabinet, parking ouvert au public…).
- **Lieu fermé au public :** seule une **déclaration normale** auprès de la CNIL est nécessaire si le système de vidéoprotection est installé dans un lieu non accessible au public (parking réservé au personnel, salle de serveurs informatiques …), d'une part, et que les images sont enregistrées ou conservées dans des traitements informatisés (vidéo IP, stockage des images sur support numérique …), d'autre part. Lorsque les images ne sont pas enregistrées (ex : surveillance en temps réel), le système n'a pas à être déclaré à la CNIL.
- **Lieu mixte** : il est nécessaire d'obtenir une **autorisation préfectorale** et d'effectuer une **déclaration normale** auprès de la CNIL.

Précision : Lorsque le dispositif de vidéoprotection s'accompagne d'un **dispositif biométrique** (reconnaissance faciale, analyse comportementale…), il doit faire l'objet d'une **autorisation** préalable de la CNIL.

1. L'obligation d'information : pas de surveillance à l'insu des personnes

- **La consultation des représentants du personnel**

S'il existe des institutions représentatives du personnel au sein du cabinet, elles doivent être consultées avant toute mise en œuvre d'un système de vidéoprotection et précisément informées des fonctionnalités envisagées.

- L'information des personnes concernées

Les personnes concernées (collaborateurs libéraux, salariés, clients, visiteurs) doivent être informées, au moyen d'un panneau affiché de façon visible dans les locaux, de l'existence du dispositif, des destinataires des images, ainsi que des modalités concrètes d'exercice de leur droit d'accès aux enregistrements visuels les concernant (Cf. modèle proposé en annexe).

2. Une visualisation des images restreinte aux seuls destinataires habilités

Les images enregistrées ne peuvent être visionnées que par les seules personnes habilitées dans le cadre de leurs fonctions, par exemple, les responsables de la sécurité du cabinet. Ces personnes doivent être particulièrement formées et sensibilisées aux règles encadrant la mise en œuvre d'un système de vidéoprotection.

3. Une durée de conservation des images limitée

Sauf enquête ou information judiciaire, la durée de conservation des images enregistrées par un dispositif de vidéoprotection ne doit pas excéder quelques jours.

Lorsque cela est techniquement possible, une durée maximale de conservation doit être paramétrée dans le système. Elle ne doit pas être fixée en fonction de la capacité de stockage.

En tout état de cause, les images ne doivent pas être gardées au-delà d'un mois.

4. Comment déclarer ?

Un système de vidéoprotection numérique ne peut être mis en œuvre que s'il a préalablement fait l'objet d'une déclaration normale auprès de la CNIL, sauf désignation d'un correspondant informatique et libertés.

Un système qui n'aurait pas fait l'objet d'une telle déclaration ne serait pas opposable.

Fiche n° 5: Les avocats et internet

Dans le cadre de leur activité professionnelle, les avocats peuvent être amenés à créer ou alimenter des sites internet.

Depuis la suppression en 2006 de la déclaration spécifique des sites internet, ces derniers n'ont plus à être déclarés en tant que tels auprès de la CNIL.

Cependant, si un traitement de données à caractère personnel est réalisé à partir d'un site internet, il convient de déclarer ce traitement s'il ne relève pas d'une dispense de déclaration ou d'une déclaration simplifiée.

A. Une dispense de déclaration des sites internet exclusivement créés à des fins d'information ou de communication externe

Les traitements constitués à des fins d'information ou de communication externe sont des traitements courants qui ne paraissent pas susceptibles de porter atteinte à la vie privée des personnes dans le cadre d'une utilisation régulière.

La CNIL estime, en conséquence, qu'il y a lieu de faire bénéficier les sites internet purement informatifs d'un allègement des formalités préalables. Les traitements réalisés sur ces sites sont dispensés de déclaration en vertu de la dispense n° 7 (délibération n° 2006-138).

Les données enregistrées ne peuvent faire l'objet d'un traitement ultérieur, d'une interconnexion ou d'une mise en relation avec d'autres applications. Les données enregistrées ne peuvent pas être utilisées à des fins de démarchage politique, électoral ou commercial.

La dispense n° 7 fixe une liste limitative des données pouvant être enregistrées:

- **identité des personnes** : nom, prénom, adresse, n° de téléphone (fixe ou mobile), n° de télécopie, adresse électronique ;
- **vie professionnelle** : adresse professionnelle, qualité ou fonction, titres et distinctions ;
- **centres d'intérêts**, à l'exclusion de ceux faisant apparaître, directement ou indirectement, les origines raciales ou ethniques, les opinions politiques, philosophiques ou religieuses, l'appartenance syndicale, ou qui sont relatifs à la santé ou la vie sexuelle ;
- **données de connexion** à des seules fins statistiques d'estimation de la fréquentation du site: date, heure, adresse IP de l'ordinateur du visiteur, page consultée ;

> Les « *newsletters* » envoyées par voie électronique aux clients de cabinets d'avocats peuvent bénéficier de la dispense de déclaration n° 7.

En revanche, ne peuvent prétendre au bénéfice de l'exonération les traitements automatisés impliquant la transmission de données vers des pays tiers à l'Union européenne ne garantissant pas un niveau de protection adéquat, y compris lorsque cette transmission est réalisée à des fins de sous-traitance. Ces traitements font l'objet de formalités déclaratives préalables auprès de la CNIL, dans les conditions prévues par la loi du 6 janvier 1978 modifiée (demande d'autorisation).

Attention : Le fait d'être dispensé de déclaration n'exonère pas le responsable de traitement des autres obligations issues de la loi du 6 janvier 1978 modifiée.

Les personnes concernées doivent notamment être informées, au moment de la collecte de leurs données, de l'identité du responsable de traitement, des finalités poursuivies par le traitement, du caractère obligatoire ou facultatif des réponses à apporter, des conséquences éventuelles, à leur égard, d'un défaut de réponse, des destinataires des données, de leur droit d'opposition, d'accès et de rectification ainsi que des modalités d'exercice de leurs droits d'accès et de rectification.

Par ailleurs, lors de la réalisation des opérations d'information ou de communication, les droits d'accès, de rectification et d'opposition doivent être rappelés aux personnes concernées.

Le responsable de traitement est également tenu de prendre toutes précautions utiles pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées ou que des tiers non autorisés y aient accès.

B. Les offres de service en ligne des avocats

Prenant acte de l'évolution des technologies et de la dématérialisation de certaines procédures, les avocats proposent désormais certains de leurs services en ligne.

Ils peuvent bénéficier de la norme simplifiée n° 48 dans ce cadre, laquelle concerne les traitements automatisés de données à caractère personnel relatifs à la gestion des fichiers de clients et de prospects. Ils doivent toutefois respecter strictement son champ d'application.

Dans la mesure où les données traitées dans le cadre de l'exercice de la profession d'avocat excédent généralement celles qui sont susceptibles d'être collectées conformément à la norme simplifiée n° 48, il apparaît plus opportun d'effectuer une déclaration normale au regard de la nature des opérations envisagées.

Quelle que soit la formalité préalable accomplie, les informations ne peuvent être conservées au-delà de la durée strictement nécessaire à la gestion de la

relation contractuelle, à l'exception de celles nécessaires à l'établissement de la preuve d'un droit ou d'un contrat qui peuvent être archivées conformément aux dispositions de la recommandation de la CNIL n° 2005-213.

Le responsable du traitement doit prendre toutes les précautions utiles pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées ou que des tiers non autorisés y aient accès.

Distinction annuaire interne / annuaire externe

Les annuaires internes, c'est-à-dire diffusés sur intranet ou support papier et uniquement accessibles aux seuls membres du cabinet, peuvent être déclarés en référence à la norme simplifiée n° 46.

Les annuaires externes (ex : annuaire diffusé sur internet) doivent, quant à eux, faire l'objet d'une déclaration normale.

C. La communication électronique de pièces

1. Communication au moyen du réseau privé virtuel des avocats (RPVA)

Face aux enjeux du développement de la dématérialisation des procédures et de son nécessaire encadrement, le Conseil national des barreaux (CNB) a décidé de doter les avocats d'un réseau informatique national sécurisé permettant de communiquer avec les greffes et, notamment, d'échanger des pièces et des courriers électroniques avec les juridictions.

Dans le cadre de sa mission de représentation et d'organisation de la profession d'avocat, le CNB a développé la plateforme « ***e-barreau*** » et déployé le RPVA. Ce dernier étant connecté au réseau privé virtuel justice (RPVJ) qui est mis en œuvre dans les juridictions.

L'article 3 de la convention conclue le 16 juin 2010 entre la Chancellerie et le CNB, qui concerne la communication électronique entre les juridictions ordinaires du premier et second degré et les avocats, prévoit que le ministère et le CNB sont chacun responsables de leur réseau. Dès lors, les avocats faisant le choix d'adhérer au RPVA sont exonérés de toute formalité auprès de la CNIL.

2. Communication au moyen d'une messagerie classique

Une communication électronique de pièces sans recours au RPVA implique que la messagerie utilisée soit déclarée à la CNIL (déclaration simplifiée en référence à la norme n°46 ou déclaration normale en cas de contrôle individuel), d'une part, et que cette communication soit suffisamment sécurisée pour garantir le secret de cette correspondance, d'autre part.

Le chiffrement des pièces apparaît comme une solution satisfaisante en terme de sécurité, sous réserve de respecter les précautions élémentaires présentées dans le guide pratique de la CNIL intitulé « ***la sécurité des données personnelles*** » (fiches n°14 et 17).

D. L'anonymisation des décisions de justice citées sur internet

Les bases de données jurisprudentielles constituent, lorsqu'elles comportent l'identité des parties ou permettent indirectement leur identification, des traitements automatisés de données à caractère personnel soumis aux dispositions de la loi du 6 janvier 1978 modifiée.

La CNIL a ainsi adopté le 29 novembre 2001 une recommandation relative à la diffusion de décisions de justice sur internet.

Cette recommandation, répondant au souci de concilier la diffusion en libre accès sur internet de décisions de justice avec la protection des personnes physiques et, par conséquent, d'assurer un juste équilibre entre le caractère public des décisions de justice et les droits et libertés des personnes concernées, devrait conduire les avocats à rendre anonymes les décisions de justice qu'ils diffusent sur internet.

Fiche n° 6: Les transferts de données à caractère personnel en dehors de l'Union européenne

La globalisation des échanges et l'utilisation croissante des nouvelles technologies, tant dans la sphère privée que commerciale, rend sans cesse croissant le nombre de transferts de données à caractère personnel à travers le monde.

Les cabinets d'avocats n'échappent pas à ce mouvement de fond. Ils sont en effet régulièrement amenés à collaborer avec des structures situées à l'étranger, qu'il s'agisse de cabinets tiers, de bureaux secondaires ou encore de clients.

Le règlement intérieur national des avocats contient des dispositions visant à assurer la confidentialité des échanges avec les avocats établis dans l'Union Européenne (art. 3.3) et hors de l'Union Européenne (art. 3.4).

A. Qu'est-ce qu'un transfert de données au sens de la loi informatique et libertés?

On parle de transfert de données lorsque des données à caractère personnel sont transférées **depuis le territoire européen vers un pays situé en dehors de l'Union européenne**.

Le transfert peut s'effectuer par copie, déplacement de données ou l'intermédiaire d'un réseau.

On considère également qu'il y a transfert de données, si ces dernières sont rendues accessibles à une entité située hors de l'Union européenne, et ce, même si les données ne sont pas matériellement déplacées. On parle ainsi de transferts lorsqu'un serveur localisé en France est rendu accessible à une entité située dans un pays tiers à l'Union européenne.

Par principe, **les transferts de données à caractère personnel hors de l'Union européenne sont interdits**, **à moins que le pays ou le destinataire des données assure un niveau de protection adéquat** à celui dont bénéficieraient les données au sein de l'Union européenne.

Cette protection adéquate peut être apportée de plusieurs manières.

B. Comment apporter un niveau de protection adéquat ?

Les transferts de données hors de l'Union européenne sont possibles dans plusieurs hypothèses. Il s'agit des transferts :

- réalisés vers un pays dont la législation a été reconnue par la Commission européenne comme offrant une protection adéquate.

Pour connaître le niveau de protection d'un État, il est possible de consulter la carte interactive diffusée sur le site internet de la CNIL (http://www.cnil.fr/pied-de-page/liens/les-autorites-de-controle-dans-le-monde).

- vers une entreprise américaine ayant adhéré aux principes du Safe Harbor ;
- encadrés par la signature entre les entités exportatrice et importatrice d'un

contrat rédigé sur le modèle de l'une des clauses contractuelles types adoptées par la Commission européenne ;

- réalisés au sein d'une société ayant adopté des règles d'entreprises contraignantes (également appelés binding corporate rules ou BCR) ;
- réalisés dans le cadre d'une des exceptions de l'article 69 de la loi du 6 janvier 1978 modifiée.

1. Le *Safe harbor*

La Commission européenne et le Département du Commerce américain se sont mis d'accord sur un ensemble de principes de protection des données personnelles.

Les entreprises américaines qui ont adhéré à ces principes peuvent recevoir des données à caractère personnel en provenance de l'Union européenne.

La liste des entreprises ayant adhéré à ces principes est consultable à partir de l'adresse suivante : https://safeharbor.export.gov/list.aspx

2. Les clauses contractuelles types

La Commission européenne a adopté des modèles de clauses contractuelles permettant d'encadrer les transferts de données personnelles effectués par des responsables de traitement vers des destinataires hors de l'Union européenne.

Elles ont pour but de faciliter la tâche des responsables de traitement dans la mise en œuvre des contrats de transferts.

Ces clauses sont disponibles sur le site de la CNIL à partie de l'adresse suivante : http://www.cnil.fr/vos-responsabilites/transferer-des-donnees-a-letranger/contrats-types-de-la-commission-europeenne/

3. Les règles internes d'entreprises ou *binding corporate rules (BCR)*

Les BCR désignent un code de conduite définissant la politique interne d'un groupe en matière de transferts de données personnelles hors de l'Union européenne.

Il s'agit d'une alternative aux Clauses contractuelles types de la Commission européenne puisque les BCR permettent d'assurer un niveau de protection suffisant aux données transférées hors de l'Union européenne.

Pour en savoir plus sur les BCR

Les cabinets qui peuvent avoir un intérêt à adopter des BCR sont ceux qui disposent de plusieurs bureaux à travers le monde échangeant régulièrement des données personnelles.

Pour plus de renseignements, consultez le guide transfert diffusé sur le site de la CNIL (http://www.cnil.fr/fileadmin/documents/Vos_responsabilites/Transferts/GUIDE-transferts-integral.pdf). Il est également possible d'adresser un courriel à bcr@cnil.fr ou de contacter le service international de la CNIL.

4. Cas particulier : les exceptions de l'article 69 de la loi informatique et libertés

Outre les transferts bénéficiant d'une protection adéquate, la loi informatique et libertés prévoit également des exceptions au principe d'interdiction des transferts. Celles-ci sont d'interprétation stricte.

Ces exceptions sont listées à l'article 69 de la loi informatique et libertés du 6 janvier 1978 modifiée (par exemple, il est permis de transférer des données personnelles vers un pays n'offrant pas de protection adéquate lorsque le transfert est nécessaire à la sauvegarde de la vie de la personne).

Attention ! Les exceptions de l'article 69 ne concernent pas les transferts massifs, répétitifs et structurés.

C. Quelles formalités accomplir en cas de transfert de données hors de l'Union européenne ?

En toutes hypothèses, les transferts de données hors de l'Union européenne doivent être notifiés à la CNIL.

En pratique, le responsable de traitement doit effectuer une déclaration ou une demande d'autorisation (selon le régime applicable au traitement principal) et remplir une annexe relative au transfert de données.

Il faut indiquer dans cette annexe, notamment, le pays destinataire, la nature des données transférées, la finalité du transfert, ainsi que les garanties permettant un niveau de protection « adéquat » (exemple : entreprise adhérente au Safe Harbor, clauses contractuelles types, BCR ou exceptions visées à l'article 69 de la loi du 6 janvier 1978 modifiée).

En fonction de la garantie apportée au transfert, ce dernier pourra être mis en œuvre :

- Soit à compter de la réception du récépissé pour les transferts :

- vers un pays dont la législation apporte un niveau de protection adéquat ;
- vers une entreprise ayant adhéré aux principes du Safe harbor ;
- reposant sur une des exceptions de l'article 69 de la loi informatique et libertés modifiées) ;

- Soit à compter de la réception du courrier de notification d'autorisation de transfert pour les transferts encadrés par :

- des clauses contractuelles types ;
- des règles internes d'entreprises.

D. Les transferts réalisés dans le cadre d'une procédure de *Discovery*

Une procédure dite de *Discovery* est une phase d'investigation et d'instruction préalable lors des procès civils ou commerciaux aux Etats-Unis. Elle fait

obligation à chaque partie de divulguer à son contradicteur tous les éléments de preuve pertinents dont elle dispose, même si elles lui sont contraires, et ce, quelles que soient leur localisation et leur forme.

Le périmètre de ces échanges peut être très large et le refus de communication peut aboutir à un jugement défavorable à la partie s'opposant à cette communication.

Depuis 2007, la CNIL a constaté un accroissement des demandes de communication de données personnelles détenues par des entreprises françaises dans le cadre de procédures de « ***Discovery*** ». Elle a mis en place un groupe de travail et mené de nombreuses auditions (pouvoirs publics, avocats, entreprises) afin d'identifier les solutions permettant de répondre à ces demandes tout en respectant la loi informatique et libertés.

La recommandation de la CNIL du 23 juillet 2009 (délibération n° 2009-474) rappelle le cadre juridique dans lequel doivent s'inscrire les demandes américaines.

- Un transfert de données à caractère personnel opéré dans le cadre d'une procédure de « Discovery » vise à la constatation, à la sauvegarde ou à la défense d'un droit en justice. L'article 69-3° de la loi du 6 janvier 1978 modifiée peut, dès lors, être invoqué pour justifier le transfert des données. Ce dernier ne doit ainsi pas faire l'objet d'une autorisation de la CNIL mais doit néanmoins lui être déclaré.
- Une information générale, claire et complète de toute personne potentiellement concernée doit être réalisée préalablement à la mise en place du traitement pouvant faire l'objet d'un transfert à l'étranger dans le cadre de procédures judiciaires.

En outre, une information spécifique doit être assurée au moment du transfert de données hors de l'Union européenne. Cette information, réalisée selon des modalités permettant de s'assurer de sa délivrance, précise notamment l'entité responsable du traitement, les faits du procès et le lien nécessitant la communication de ses données personnelles, le caractère facultatif ou non du traitement, les conséquences en cas de refus de communication, les services éventuellement chargés de la recherche, les éventuels transferts de données à caractère personnel à destination d'un Etat non membre de l'Union européenne, ainsi que les modalités d'exercice des droits d'accès, d'opposition et de rectification.

Lorsqu'il existe un risque que l'information de la personne concernée mette en danger la possibilité pour la partie au procès de mener une enquête ou de rassembler des preuves, l'information de la personne concernée peut être retardée tant que ce risque existe. Lorsque des mesures conservatoires sont nécessaires, notamment pour prévenir la destruction de preuves, l'information peut intervenir après l'adoption de ces mesures.

- Il convient de recueillir le consentement libre et éclairé des personnes concernées et de pouvoir en rapporter la preuve.
- Les personnes concernées doivent bénéficier en toutes circonstances d'un droit d'opposition, sur la base de motifs légitimes.
- Les données collectées dans le cadre d'une procédure de « Discovery » doivent être adéquates, pertinentes et non excessives au regard des finalités pour lesquelles le traitement est mis en œuvre.

La procédure américaine intègre le principe de proportionnalité grâce aux *Stipulatives Court Orders*. Il s'agit d'ordonnances prises par le juge américain garantissant que les pièces communiquées dans le cadre de la procédure seront utilisées selon des conditions définies entre les parties et conservées de manière confidentielle. Elles peuvent limiter le périmètre des pièces à communiquer, spécifier les conditions liées à l'utilisation et la communication à des tiers des données et prévoir des mesures de sécurité et de confidentialité à respecter.

- Les données doivent être conservées pour le seul temps de la procédure ;
- L'accès aux données doit être limité aux seules personnes qui, dans le cadre de leurs fonctions, peuvent légitimement en avoir connaissance ;
- Le responsable du traitement doit garantir le droit d'accéder aux données et d'en demander, si elles sont inexactes, incomplètes, équivoques ou périmées, la rectification ou la suppression ;
- Le responsable du traitement doit prendre les mesures utiles pour préserver la sécurité des données et tracer les consultations.

Fiche n° 7 : Le rôle de l'avocat en cas de contrôle sur place

A. La procédure de décision d'un contrôle

La décision de procéder à un contrôle est prise par le Président de la CNIL, sur proposition du service des contrôles.

La décision de prévenir, ou non, le responsable de traitement auprès duquel est effectué le contrôle est prise au regard des caractéristiques de ce contrôle. Il peut être demandé, à cette occasion, communication préalable de documents particuliers relatifs, par exemple, aux moyens informatiques utilisés ou à l'organisation générale de l'organisme contrôlé.

La décision du Président de la CNIL est notifiée au début du contrôle au responsable des lieux où se situent le ou les traitements qui font l'objet des vérifications. Le procureur de la République territorialement compétent est informé, quant à lui, de la date, de l'heure et de l'objet du contrôle avant que celui-ci ne débute.

B. Les pouvoirs de la CNIL

Un avocat peut assister l'un de ses clients tout au long d'un contrôle de la CNIL.

Ce type de mission vise prioritairement à obtenir copie du maximum d'informations (éléments techniques et juridiques) permettant d'apprécier les conditions dans lesquelles sont mis en œuvre des traitements automatisés de données à caractère personnel (sécurité, information des personnes, modalités de collecte de données, etc.).

La délégation de la CNIL peut demander communication de tout document nécessaire à l'accomplissement de sa mission, quel qu'en soit le support, et en prendre copie.

Les membres de la délégation peuvent également accéder aux programmes informatiques et aux données, ainsi qu'en demander la transcription par tout traitement approprié dans des documents directement utilisables pour les besoins du contrôle.

La délégation peut ainsi demander copie :

- de contrats (contrat de location de fichiers, de sous-traitance informatique etc.)
- de formulaires ;
- de dossiers « *papiers* » ;
- de bases de données informatiques, etc.

La copie des données lors du contrôle et leur conservation ultérieure font l'objet de procédures particulières définies par le service des contrôles, afin de garantir leur authenticité et leur confidentialité.

Un procès verbal, qui précise notamment la liste des documents dont une copie aura été effectuée, est établi à l'issue de chaque mission de contrôle.

L'article 51 de la loi informatique et libertés réprime d'un an d'emprisonnement et de 15.000 € d'amende le fait d'entraver l'action de la CNIL :

- en s'opposant à l'exercice des missions confiées à ses membres ou aux agents habilités lorsque la visite a été autorisée par un juge ;
- en refusant de communiquer à ses membres ou aux agents habilités les renseignements et documents utiles à leur mission, en dissimulant lesdits documents ou renseignements, ou en les faisant disparaître ;
- en communiquant des informations qui ne sont pas conformes au contenu des enregistrements tel qu'il était au moment où la demande a été formulée ou qui ne présentent pas ce contenu sous une forme directement accessible.

L'avocat peut accompagner son client tout au long de cette procédure de contrôle sur place, en l'informant des pouvoirs de la CNIL, des possibilités qui lui sont offertes pour réagir à ces contrôles et des suites qui peuvent être données. Il peut ainsi définir un dispositif de crise pour gérer un contrôle de la CNIL.

Le concours d'un avocat peut également être utile en cas de contrôle sur pièces, notamment lors de l'envoi des pièces sollicitées, et ce, afin de respecter les délais, la forme et le contenu des documents demandés. Il peut aussi proposer une analyse des éléments déclencheurs du contrôle afin de remédier à la non-conformité.

C. Le droit de s'opposer à un contrôle

L'article 44-II de la loi du 6 janvier 1978 modifiée prévoit que le responsable des locaux visités doit être informé de son droit à s'opposer au contrôle.

Si ce droit est exercé, la visite peut néanmoins se dérouler après une autorisation du juge des libertés et de la détention compétent.

Lorsque l'urgence, la gravité des faits, le risque de destruction ou de dissimulation de documents le justifie, un contrôle peut se dérouler sans information préalable du responsable des locaux, sur autorisation préalable du juge des libertés et de la détention. Dans ce cas, le responsable ne peut s'opposer à la visite.

D. L'opposabilité du secret professionnel

Lors d'un contrôle, le secret professionnel peut être utilement avancé pour interdire à la délégation de la CNIL d'accéder aux fichiers qui en relèvent (article 69 du décret n°2005-1309 du 20 octobre 2005 pris pour l'application de la loi informatique et libertés).

Le responsable des locaux visités doit cependant préciser les dispositions législatives et réglementaires auxquelles il se réfère, ainsi que la nature des données qu'il estime couvertes par ces dispositions.

Ces éléments (c'est-à-dire la mention de l'opposition, son fondement textuel et la nature des données couvertes) sont mentionnés sur le procès verbal établi par les membres de la CNIL.

Le secret professionnel ne peut concerner que les seuls fichiers comportant des éléments confidentiels.

L'invocation injustifiée du secret professionnel constitue une entrave passible des peines prévues par l'article 51 de la loi informatique et libertés (1 an d'emprisonnement et 15.000 € d'amende).

En 2005, la Commission a ainsi prononcée une sanction pécuniaire de 5.000 € à l'encontre d'une étude d'huissiers ayant détourné le secret professionnel de son objet.

A savoir : Les fichiers des avocats, au même titre que ceux de tous les responsables de traitements de données à caractère personnel, peuvent être contrôlés par une délégation de la CNIL. Cette dernière peut se voir opposer le secret professionnel.

Fiche n° 8 : Le rôle de l'avocat en cas de procédure de sanction

A. La procédure de sanction suite à la réforme du 30 mars 2011

Le Conseil d'Etat a considéré par une ordonnance du 19 février 2008 que la CNIL, en raison de ses missions et de sa composition, était un « Tribunal » au sens de l'article 6-1 de la Convention de sauvegarde des droits de l'homme et des libertés fondamentales.

Cette décision a entrainé un profond remaniement de l'organisation et du fonctionnement de la « formation restreinte » de la Commission.

Les lois organique et ordinaire relatives au Défenseur des droits, publiées le 30 mars 2011 au Journal Officiel, ont ainsi redistribué les pouvoirs de poursuite, d'instruction et de jugement au sein de la Commission pour répondre aux exigences de la Cour européenne des droits de l'homme.

Désormais, les membres du bureau de la Commission (le Président et les deux vices Présidents) ne sont plus éligibles à la « formation restreinte » alors que le Président de la Commission est seul compétent pour diligenter des missions de contrôle sur place, adresser des mises en demeure et procéder à la désignation des rapporteurs. En application de ces dispositions, une nouvelle « formation restreinte » a été élue le 5 mai 2011.

Pour rappel, depuis la réforme du 6 août 2004, la CNIL dispose d'un large éventail de mesures coercitives à l'encontre des responsables de traitement.

Hormis l'avertissement, la CNIL peut, après une mise en demeure restée infructueuse et à l'issue d'une procédure contradictoire, prononcer une sanction pécuniaire allant jusqu'à 300.000 € (à l'exception des traitements mis en œuvre par l'État), prononcer une injonction de cesser le traitement ou encore retirer une autorisation préalablement accordée.

En outre, la formation restreinte peut engager des procédures d'urgence : l'interruption du traitement, l'avertissement, le verrouillage des données et l'information du Premier ministre pour certains traitements sensibles mis en œuvre par l'Etat.

En cas d'atteinte grave et immédiate aux droits et libertés garantis par la loi du 6 janvier 1978 modifiée, le Président peut demander par la voie du référé à la juridiction compétente d'ordonner, le cas échéant sous astreinte, toute mesure de sécurité nécessaire à la sauvegarde de ces droits et libertés. Il peut également, au nom de la Commission, dénoncer au Procureur de la République les violations de la loi dont il a connaissance.

Enfin, la formation restreinte peut décider de rendre publique les sanctions qu'elle prononce.

B. L'avocat et la procédure de sanction

L'avocat trouve naturellement sa place comme représentant des intérêts de son client à l'occasion d'une procédure de sanction administrative diligentée par la CNIL. Tel est le cas, notamment, lorsque l'avocat assiste ou représente un client devant la « formation restreinte » de la Commission.

La procédure de sanction mise en œuvre au sein de la « formation restreinte » de la CNIL est écrite.

Le Président de la CNIL commence par désigner un rapporteur chargé de rédiger un rapport caractérisant, en fait et en droit, les manquements reprochés à l'organisme mis en cause.

Le rapport est notifié à l'organisme au minimum un mois avant la séance de la « formation restreinte ».

A compter de cette notification, l'avocat, en sa qualité de conseil de l'organisme mis en cause, peut avoir accès au dossier en venant le consulter au siège de la CNIL. Il dispose également de la possibilité d'obtenir une copie de ce dossier.

Les écritures en défense doivent être communiquées à la CNIL dans un délai raisonnable avant la séance. A cet égard, un projet de décret qui devrait être adopté prochainement impose un délai incompressible de communication des observations en défense de trois jours avant la séance.

Le jour de la séance, le rapporteur prend la parole en premier, suivi de l'organisme mis en cause et, le cas échéant, de son conseil. La « formation restreinte » peut entendre toute personne dont l'audition lui parait utile et demander au rapporteur, si elle s'estime insuffisamment éclairée, de poursuivre ses diligences. L'organisme et son conseil ont la parole en dernier.

Les observations orales de l'avocat ne peuvent être développées qu'à l'appui de ses conclusions écrites. Le décret précité formalisera également ce principe inhérent au caractère écrit de la procédure.

A la fin de la séance, la formation restreinte se retire pour délibérer. La décision de sanction, ou de relaxe, est notifiée à l'organisme avec indication des voies et délais de recours.

A noter : Depuis la publication des lois organique et ordinaire relatives au Défenseur des droits en date du 30 mars 2011, la « formation restreinte » peut rendre publique toutes les sanctions qu'elle prononce sans devoir établir la mauvaise foi de l'organisme mis en cause.

III. ANNEXES

A. Conseils pour assurer un niveau de sécurité satisfaisant

La loi informatique et libertés impose que les organismes mettant en œuvre des traitements ou disposant de fichiers de données à caractère personnel en garantissent la sécurité.

Par sécurité des données, on entend l'ensemble des précautions utiles, au regard de la nature des données et des risques présentés par le traitement pour, notamment, empêcher que les données soient déformées, endommagées, ou que des tiers non autorisés y aient accès. (Art.34 de la loi informatique et libertés). Cette sécurité se conçoit pour l'ensemble des processus relatifs à ces données, qu'il s'agisse de leur création, leur utilisation, leur sauvegarde, leur archivage ou leur destruction et concerne leur confidentialité, leur intégrité, leur authenticité et leur disponibilité.

Rappel : Les avocats, au même titre que les éventuels prestataires spécialisés dans l'hébergement et la gestion de documents, sont tenus de présenter des garanties suffisantes pour assurer la sécurité et la confidentialité des données auxquelles ils accèdent, en application de l'article 35 de la loi informatique et libertés.

1. Authentifiez les utilisateurs

- définissez un identifiant (*login*) unique à chaque utilisateur
- adoptez une politique de mot de passe utilisateur rigoureuse
- obligez l'utilisateur à changer son mot de passe après réinitialisation

2. Gérez les habilitations et sensibilisez les utilisateurs

- définissez des profils d'habilitation
- supprimez les permissions d'accès obsolètes
- documentez les procédures d'exploitation
- rédigez une charte informatique et annexez-la au règlement intérieur

3. Sécurisez les postes de travail

- limitez le nombre de tentatives d'accès à un compte
- installez un « pare-feu » (*firewall*) logiciel
- utilisez des antivirus régulièrement mis à jour
- prévoyez une procédure de verrouillage automatique de session

4. Sécurisez l'informatique mobile

- prévoyez des moyens de chiffrement pour les ordinateurs portables et les unités de stockage amovibles (clés USB, CD, DVD…)

5. Sauvegardez et prévoyez la continuité d'activité

- effectuez des sauvegardes régulières
- stockez les supports de sauvegarde dans un endroit sûr
- prévoyez des moyens de sécurité pour le convoyage des sauvegardes
- prévoyez et testez régulièrement la continuité d'activité
- chiffrez les sauvegardes

6. Encadrez la maintenance

- enregistrez les interventions de maintenance dans une main courante
- effacez les données de tout matériel avant sa mise au rebut
- recueillez l'accord de l'utilisateur avant toute intervention sur son poste
- prévoyez de rendre impossible l'accès au contenu des bases de données aux prestataires techniques

7. Tracez les accès et gérez les incidents

- prévoyez un système de journalisation
- informez les utilisateurs de la mise en place du système de journalisation
- protégez les équipements de journalisation et les informations journalisées
- notifiez aux personnes concernées des accès frauduleux à leurs données

8. Protégez les locaux

- restreignez les accès aux locaux au moyen de portes verrouillées
- installez des alarmes anti-intrusion et vérifiez-les périodiquement

9. Protégez le réseau informatique interne

- limitez les flux réseau au strict nécessaire
- sécurisez les accès distants des appareils informatiques nomades par VPN
- utilisez le protocole SSL avec une clé de 128 bits pour les services web
- mettez en œuvre le protocole WPA - AES/CCMP pour les réseaux WiFi

10. Sécurisez les serveurs et les applications

- adoptez une politique de mot de passe administrateur rigoureuse
- installez sans délai les mises à jour critiques
- assurez une disponibilité des données

11. Gérez la sous-traitance

- prévoyez une clause spécifique dans les contrats des sous-traitants

- assurez-vous de l'effectivité des garanties prévues (audits de sécurité, visites...)
- prévoyez les conditions de restitution et de destruction des données

12. Archivez

- mettez en œuvre des modalités d'accès spécifiques aux données archivées
- détruisez les archives obsolètes de manière sécurisée

13. Sécurisez les échanges avec d'autres organismes

- chiffrez les données avant leur envoi
- assurez-vous qu'il s'agit du bon destinataire
- transmettez le secret lors d'un envoi distinct et via un canal différent

B. Tableaux récapitulatifs : quelle formalité simplifiée pour quel fichier ?

1. Dispenses de déclaration pouvant concerner les cabinets d'avocat

Référence de la délibération	Numéro de la dispense	Domaine couvert par la dispense
Délibération n° 2004-097 du 9 décembre 2004	Dispense n° 2	Gestion des **rémunérations** (y compris l'intéressement, la participation et les déclarations fiscales et sociales), tenue des registres obligatoires
Délibération n° 2005-005 du 18 janvier 2005	Dispense n° 4	Gestion des fichiers de **fournisseurs** comportant une personne physique
Délibération n° 2006-138 du 9 mai 2006	Dispense n° 7	Traitements constitués à des fins d'information ou de **communication externe** ne pouvant s'apparenter à une sollicitation commerciale
Délibération n° 2006-186 du 6 juillet 2006	Dispense n° 9	Traitements automatisés de données personnelles ayant pour finalité la tenue, l'utilisation et la communication des **listes d'initiés**
Délibération n° 2006-230 du 17 octobre 2006	Dispense n° 10	Traitements mis en œuvre par les comités d'entreprises ou d'établissements, les comités centraux d'entreprises, les comités de groupe ou les comités interentreprises ou les délégués du personnel pour la **gestion des activités sociales et culturelles**

Délibération n° 2009-476 du 10 septembre 2009	Dispense n° 14	Traitements de données à caractère personnel mis en œuvre dans le cadre de plans de continuité d'activité relatifs à une **pandémie grippale**
Délibération n° 80-34 du 21 octobre 1980		Traitements automatisés de **comptabilité générale**

2. Normes simplifiées pouvant concerner les cabinets d'avocats :

Référence de la délibération	Numéro de la norme simplifiée	Domaine couvert par la norme simplifiée
Délibération n° 03-067 du 18 décembre 2003	Norme simplifiée n° 21	Gestion et la négociation des **biens immobiliers**
Délibération n° 02-001 du 8 janvier 2002	Norme simplifiée n° 42	Traitements automatisés d'informations nominatives mis en œuvre sur les lieux de travail pour la gestion des **contrôles d'accès aux locaux, des horaires et de la restauration**
Délibération n° 2005-002 du 13 janvier 2005	Norme simplifiée n° 46	**Gestion des ressources humaines** (gestion administrative du personnel, mise à disposition des outils informatiques, organisation du travail, gestion des carrières et mobilité, formation)
Délibération n° 2005-019 du 3 février 2005	Norme simplifiée n° 47	Traitements automatisés de données à caractère personnel mis en œuvre dans le cadre de **l'utilisation de services de téléphonie fixe et mobile** sur les lieux de travail
Délibération n° 2005-112 du 7 juin 2005	Norme simplifiée n° 48	Traitements automatisés de données à caractère personnel relatifs à la **gestion des fichiers de clients et de prospects**
Délibération n° 2006-067 du 16 mars 2006	Norme simplifiée n° 51	Traitements automatisés de données à caractère personnel mis en œuvre par les organismes publics ou privés destinés à **géolocaliser les véhicules utilisés par leurs employés**

3. Autorisations uniques pouvant être utilisées par les Cabinets d'avocats :

Référence de la délibération	Numéro de l'autorisation unique	Domaine couvert par l'autorisation unique
Délibération n°2005-305 du 8 décembre 2005	Autorisation unique AU-004	Traitements automatisés de données à caractère personnel mis en œuvre dans le cadre de dispositifs d'**alerte professionnelle**
Délibération n°2006-101 du 27 avril 2006	Autorisation unique AU-007	Mise en œuvre de **dispositifs biométriques** reposant sur la reconnaissance du **contour de la main** et ayant pour finalités le **contrôle d'accès ainsi que la gestion des horaires et de la restauration** sur les lieux de travail
Délibération n°2006-102 du 27 avril 2006	Autorisation unique AU-008	Mise en œuvre de **dispositifs biométriques** reposant sur la reconnaissance de **l'empreinte digitale** exclusivement enregistrée sur un support individuel détenu par la personne concernée et ayant pour finalité le **contrôle de l'accès aux locaux** sur les lieux de travail
Délibération n°2009-316 du 7 mai 2009	Autorisation unique AU-019	Mise en œuvre de **dispositifs biométriques** reposant sur la reconnaissance du **réseau veineux** des doigts de la main et ayant pour finalité le **contrôle de l'accès aux locaux** sur les lieux de travail
Délibération n°2011-074 du 10 mars 2011	Autorisation unique AU-027	Mise en œuvre de **dispositifs biométriques** reposant sur la reconnaissance de **l'empreinte digitale** et ayant pour finalité le **contrôle de l'accès aux postes informatiques portables**

4. Recommandations de la CNIL pouvant faciliter la mise aux normes des traitements informatisés généralement utilisés par les cabinets d'avocat :

Référence de la délibération	Domaine de la recommandation
Délibération n°2009-474 du 23 juillet 2009	Transferts de données à caractère personnel dans le cadre de procédures judiciaires américaines dite de **« Discovery »**
Délibération n°2006-066 du 16 mars 2006	Dispositifs destinés à **géolocaliser les véhicules** automobiles utilisés par les employés d'un organisme privé ou public
Délibération n°2005-213 du 11 octobre 2005	Modalités **d'archivage électronique** dans le secteur privé
Délibération n°02-017 du 21 mars 2002	Collecte et traitement d'informations nominatives lors d'opérations de **recrutement**
Délibération n°01-057 du 29 novembre 2001	Diffusion de données personnelles sur internet par les **banques de données de jurisprudence**
Délibération n° 94-056 du 21 juin 1994	Dispositifs de **vidéosurveillance** mis en œuvre dans les lieux publics et les lieux recevant du public
Délibération n° 84-031 du 18 septembre 1984	Usage des **autocommutateurs téléphoniques**
Délibération n° 81-094 du 21 juillet 1981	Mesures générales de **sécurité des systèmes informatiques**
Délibération n° 80-010 du 1er avril 1980	Mise en œuvre du **droit individuel d'accès** aux fichiers automatisés

C. Modèles de mentions informatives

1. Formulaire de collecte de données à caractère personnel

..... *(Indiquez l'identité du responsable du traitement)*

« Les informations recueillies font l'objet d'un traitement informatique destiné à ..... *(Précisez la finalité).*

Les destinataires des données sont :..... *(Précisez).*

Conformément à la loi « informatique et libertés » du 6 janvier 1978 modifiée, vous bénéficiez d'un droit d'accès et de rectification aux informations qui vous concernent, que vous pouvez exercer en vous adressant à ..... *(Précisez le service et l'adresse).*

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

2. Note d'information à afficher

Le(s) service(s)…… *(Veuillez citer le nom du ou des services responsables du traitement)* dispose(nt) de moyens informatiques destinés à gérer plus facilement …… *(Veuillez indiquer la finalité du traitement)*.

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

Conformément aux articles 39 et suivants de la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés, toute personne peut obtenir communication et, le cas échéant, rectification ou suppression des informations la concernant, en s'adressant au service…… *(Veuillez citer le nom du service ou des services concernés)*.

3. Panneau d'information concernant la vidéoprotection

Établissement sous vidéoprotection *(représentation graphique d'une caméra)*

Nous vous informons que cet établissement est placé sous vidéoprotection pour des raisons de …… *(Indiquez les finalités poursuivies)*.

Pour tout renseignement, s'adresser à ……*(identifiez la personne ou le service compétent),* auprès duquel vous pouvez également exercer votre droit d'accès, conformément à la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés.

4. Mention générale pour formulaire :

…… *(Veuillez indiquer l'identité du responsable du traitement)*

« Les informations recueillies font l'objet d'un traitement informatique destiné à ……. *(Veuillez préciser la finalité)*.

Les destinataires des données sont :…… *(Précisez)*.

Conformément à la loi « informatique et libertés » du 6 janvier 1978 modifiée, vous bénéficiez d'un droit d'accès et de rectification aux informations qui vous concernent, que vous pouvez exercer en vous adressant à …… *(Veuillez préciser le service et l'adresse)*.

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

5. Annuaire diffusé sur internet

Madame, Monsieur,

Nous envisageons de diffuser prochainement sur notre site Internet ……. *(Indiquez ici le nom de domaine de votre site)* des informations vous

concernant dans le cadre de *(à compléter : Exemples : site internet d'une administration, d'une association, d'un groupement professionnel, d'une entreprise, etc.)*.

Ces informations sont les suivantes : *(Indiquez ici les informations que vous allez diffuser. Exemples : nom, prénom, diplôme, etc.).*

Compte tenu des caractéristiques du réseau internet que sont la libre captation des informations diffusées et la difficulté, voire l'impossibilité, de contrôler l'utilisation qui pourrait en être faite par des tiers, vous pouvez vous opposer à une telle diffusion.

Pour que nous puissions prendre en compte votre refus, contactez-nous *(Précisez comment).*

6. Enregistrement de conversations téléphoniques

Nous vous informons que votre conversation téléphonique est susceptible d'être enregistrée pour des raisons de ……. *(Veuillez indiquer les finalités poursuivies)*.

Vous pouvez vous opposer à cet enregistrement de la manière suivante : *(Veuillez préciser la procédure à suivre, appui sur une touche téléphonique, demande à formuler à l'opérateur…)*

En cas d'enregistrement des conversations, ceux-ci son conservés pour une durée de *(Veuillez préciser la durée).*

Seules les personnes habilitées du service …… *(Veuillez préciser le service – par exemple le service clientèle)* auront accès à cet enregistrement.

Conformément à la loi « informatique et libertés » du 6 janvier 1978 modifiée, vous pouvez accéder et rectifier les informations qui vous concernent en vous adressant à …… *(Veuillez préciser le service et l'adresse).*

7. Notice d'information en matière de recrutement

…….. *(Indication de l'identité du responsable du traitement)*

Nous vous prions de bien vouloir compléter soigneusement ce formulaire. Les réponses aux cases munies d'un astérisque sont facultatives et sans conséquence pour l'examen du dossier ; dans les autres cas, le défaut réponse est susceptible de compromettre le bon suivi de votre candidature.

Conformément au Code du travail, nous vous informons que la procédure de recrutement utilisée par notre société comprend : *(à préciser, par exemple des entretiens, éventuellement une analyse graphologique et/ou des tests psychotechniques). Dans ce dernier cas il convient d'ajouter :* Les résultats de ces tests vous seront restitués sur demande, ils ne seront conservés dans votre dossier qu'en cas d'embauche.

Nous vous informons que les données vous concernant sont (ou ne sont pas) informatisées, elles seront traitées de façon confidentielle. Vos données sont conservées pour une durée de *(à préciser, au maximum 24 mois à compter du dernier contact avec le candidat).*

Seules les personnes habilitées de notre société pourront accéder à vos données à des fins strictement internes.

Option pour les groupes internationaux : J'autorise la société à communiquer les informations me concernant aux filiales du groupe situées en dehors de l'Union Européenne : Oui Non

Option pour les cabinets de recrutement : J'autorise la société à communiquer les informations me concernant à toute entreprise cliente : Oui Non

Option pour les « cvthèques » en ligne : J'autorise la société à :

- communiquer les informations me concernant à toute entreprise cliente qui en ferait la demande : Oui Non
- diffuser en ligne les informations me concernant sans les rendre anonymes : Oui Non

Vous pouvez accéder aux informations vous concernant, les rectifier ou les supprimer pour ce faire il suffit de vous adresser auprès du service suivant : (à préciser).

Fait le : ..... à .....

Signature :

8. Mention d'information en cas de transfert de donnés en dehors de l'Union européenne

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

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

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

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

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

- Le pays du ou des destinataire(s) offre un niveau de protection adéquat par décision de la Commission européenne : ..... *(Précisez laquelle);*
- Le ou les destinataire(s) sont adhérent(s) aux principes du Safe Harbour;
- Le transfert de données a été autorisé par la CNIL et est encadré par les clauses contractuelles types établies par la Commission européenne *(précisez le numéro de la délibération autorisant le transfert);*
- Le transfert de données a été autorisé par la CNIL et est encadré par des règles internes validées par la CNIL;
- La société bénéficie d'une des exceptions mentionnées à l'article 69 de la loi du 6 janvier 1978 modifiée : ..... *(Précisez laquelle).*

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

9. Contrôle d'accès biométrique

..... *(Indication de l'identité du responsable du traitement)*

Un dispositif biométrique destiné au contrôle de l'accès ..... *(Veuillez préciser ici la finalité, par exemple contrôle d'accès à un bâtiment ou à une zone en particulier, contrôle d'accès à un poste informatique ou à une application)* a été mis en place.

Les données vous concernant sont conservées au maximum *(précisez)*.

Au-delà, toutes les données sont détruites. Seules les personnes habilitées du service ..... *(Veuillez préciser le service – par exemple le service informatique)* auront accès à vos données biométriques.

Conformément à la loi « informatique et libertés » du 6 janvier 1978 modifiée, vous pouvez avoir accès et rectifier les informations qui vous concernent en vous adressant à ..... *(Veuillez préciser le service et l'adresse)*

D. Lexique informatique et libertés

Alertes professionnelles (*Whistleblowing*)

C'est un outil mis à la disposition des salariés. Il peut s'agir par exemple d'un numéro de téléphone « ***ligne éthique*** » ou d'une adresse électronique particulière. Ce dispositif leur permet de signaler des problèmes pouvant sérieusement affecter l'activité d'une entreprise ou engager gravement sa responsabilité. Les alertes recueillies sont ensuite vérifiées, dans un cadre confidentiel, et permettent à l'employeur de décider, en connaissance de cause, des mesures correctives à prendre. Compte tenu de la multiplicité des voies d'alertes déjà disponibles dans les entreprises (voie hiérarchique, commissaires aux comptes, fonctions de l'audit ou de la conformité interne, représentants du personnel, inspection du travail, etc.), le dispositif d'alerte professionnelle ne peut être que facultatif. Un salarié ne peut pas être sanctionné s'il ne souhaite pas l'utiliser.

BCR

Le sigle BCR signifie *Binding Corporates Rules* ou règles d'entreprise contraignantes. Ces règles internes applicables à l'ensemble des entités du groupe contiennent les principes-clés permettant d'encadrer les transferts de données personnelles, de salariés ou de clients et prospects, hors de l'Union européenne. Les BCR sont une alternative au Safe Harbor (qui ne vise que les transferts vers les États-Unis) ou aux Clauses contractuelles types adoptées par la Commission européenne. Elles garantissent qu'une protection équivalente à celle octroyée par la directive européenne de 1995 s'applique aux données personnelles transférées hors de l'Union européenne.

Biométrie

La biométrie regroupe l'ensemble des techniques informatiques permettant de reconnaître automatiquement un individu à partir de ses caractéristiques physiques, biologiques, voire comportementales. Les données biométriques sont des données à caractère personnel car elles permettent d'identifier une personne. Elles ont, pour la plupart, la particularité d'être uniques et permanentes (ADN, empreintes digitales...).

Biométrie sans trace ou avec trace ?

Parmi toutes les données biométriques utilisées aujourd'hui, certaines présentent la particularité de pouvoir être capturées et utilisées à l'insu des personnes concernées. C'est le cas, par exemple, des empreintes génétiques puisque chacun laisse involontairement derrière soi des traces, même infimes, de son corps, dont on peut extraire l'ADN. C'est également le cas des empreintes digitales, dont on laisse aussi des traces, plus ou moins facilement exploitables, dans beaucoup d'actes de la vie courante. D'autres données biométriques ne présentent pas, du moins dans l'état actuel de la technique, cette particularité : c'est le cas, par exemple, du réseau veineux du doigt ou du contour de la main, car ces données biométriques laissent peu de trace au quotidien, voire aucune. La biométrie avec trace impose donc une vigilance toute particulière de la part des personnes concernées.

Clauses Contractuelles Types

Il s'agit de modèles de clauses contractuelles adoptés par la Commission européenne permettant d'encadrer les transferts de données personnelles effectués par des responsables de traitement vers des destinataires situés hors de l'Union européenne. Elles ont pour but de faciliter la tâche des responsables de traitement dans la mise en œuvre de contrats de transfert.

On distingue les transferts de responsable de traitement à responsable de traitement et les transferts de responsable de traitement à sous-traitant. Il existe donc deux types de clauses afin d'encadrer chacun des transferts.

Cloud computing

Le Cloud Computing (en français, « informatique dans les nuages ») fait référence à l'utilisation de la mémoire et des capacités de calcul des ordinateurs et des serveurs répartis dans le monde entier et liés par un réseau. Les applications et les données ne se trouvent plus sur un ordinateur déterminé mais dans un nuage (Cloud) composé de nombreux serveurs distants interconnectés. D'un point de vue « Informatique et Libertés », ce concept soulève des problématiques de sécurité, de qualification des parties, de droit applicable, d'exercice effectif des droits et d'encadrement des transferts internationaux de données personnelles.

CNIL

Autorité administrative indépendante, composée d'un collège pluraliste de 17 commissaires, provenant d'horizons divers : 4 parlementaires, 2 membres du Conseil économique et social, 6 représentants des hautes juridictions, 5 personnalités qualifiées désignées par le Président de l'Assemblée nationale (1), par le Président du Sénat (1), par le Conseil des ministres (3). Le mandat de ses membres est de 5 ans.

Conférence mondiale des commissaires à la protection des données et à la vie privée

Cette conférence se tient chaque année à l'automne. Elle réunit l'ensemble des 81 autorités et commissaires à la protection des données et à la vie privée de tous les continents. Elle est ouverte aux intervenants et participants du monde économique, des autorités publiques, et de la société civile. Une partie de la Conférence est réservée aux représentants des autorités accréditées par la Conférence, durant laquelle sont adoptées les résolutions et déclarations.

Correspondant « Informatique et Libertés »

Créé en 2004, le correspondant « Informatique et Libertés » (CIL) est chargé d'assurer de manière indépendante le respect des obligations prévues par la loi du 6 janvier 1978 ; en contrepartie de sa désignation, les traitements de données personnelles les plus courants sont exonérés de déclarations auprès de la CNIL.

Déclarant

Personne physique ou morale responsable d'un traitement ou d'un fichier contenant des données personnelles qu'il doit déclarer à la CNIL sous peine

de sanctions.

Destinataire

Personne habilitée à obtenir communication de données enregistrées dans un fichier ou un traitement en raison de ses fonctions.

Discovery

Discovery est le nom donné à la procédure américaine permettant, dans le cadre de la recherche de preuves pouvant être utilisées dans un procès, de demander à une partie tous les éléments d'information (faits, actes, documents...) pertinents pour le règlement du litige dont elle dispose quand bien même ces éléments lui seraient défavorables.

Donnée biométrique

Caractéristique physique ou biologique permettant d'identifier une personne (ADN, contour de la main, empreintes digitales...).

Donnée personnelle

Toute information identifiant directement ou indirectement une personne physique (ex. nom, no d'immatriculation, no de téléphone, photographie, date de naissance, commune de résidence, empreinte digitale...).

Donnée sensible

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.

Droit à la protection des données personnelles

Le droit à la protection des données à caractère personnel est inscrit dans la charte des droits fondamentaux de l'Union européenne au titre des libertés fondamentales telles que la liberté de pensée, de conscience et de religion, la liberté d'expression et d'information ou le respect de la vie privée et familiale, etc.

Droit à l'information

Toute personne a un droit de regard sur ses propres données ; par conséquent, quiconque met en œuvre un fichier ou un traitement de données personnelles est obligé d'informer les personnes fichées de son identité, de l'objectif de la collecte d'informations et de son caractère obligatoire ou facultatif, des destinataires des informations, des droits reconnus à la personne, des éventuels transferts de données vers un pays hors de l'Union européenne.

Droit d'accès direct

Toute personne peut prendre connaissance de l'intégralité des données la concernant dans un fichier en s'adressant directement à ceux qui les détiennent, et en obtenir une copie dont le coût ne peut dépasser celui de la reproduction.

Droit d'accès indirect

Toute personne peut demander que la CNIL vérifie les renseignements qui peuvent la concerner dans les fichiers intéressant la sûreté de l'État, la Défense et la Sécurité publique.

Droit d'opposition

Toute personne a la possibilité de s'opposer, pour des motifs légitimes, à figurer dans un fichier, et peut refuser sans avoir à se justifier, que les données qui la concernent soient utilisées à des fins de prospection commerciale.

Droit de rectification

Toute personne peut faire rectifier, compléter, actualiser, verrouiller ou effacer des informations la concernant lorsqu'ont été décelées des erreurs, des inexactitudes ou la présence de données dont la collecte, l'utilisation, la communication ou la conservation est interdite.

Finalité d'un traitement

Objectif principal d'une application informatique de données personnelles. Exemples de finalité : gestion des recrutements, gestion des clients, enquête de satisfaction, surveillance des locaux, etc.

Formalités préalables

Ensemble des formalités déclaratives à effectuer auprès de la CNIL avant la mise en œuvre d'un traitement de données personnelles ; selon les cas, il peut s'agir d'une déclaration ou d'une demande d'autorisation.

Formation restreinte

Pour prendre des mesures à l'encontre des responsables de traitement qui ne respectent pas la loi « Informatique et Libertés », la CNIL siège dans une formation spécifique, composée de six membres appelée « formation restreinte ». À l'issue d'une procédure contradictoire, cette formation peut notamment décider de prononcer des sanctions pécuniaires pouvant atteindre 300 000 €.

G29

L'article 29 de la directive du 24 octobre 1995 sur la protection des données et la libre circulation de celles-ci a institué un groupe de travail rassemblant les représentants de chaque autorité indépendante de protection des données nationale. Cette organisation réunissant l'ensemble des CNIL européennes a pour mission de contribuer à l'élaboration des normes européennes en adoptant des recommandations, de rendre des avis sur le niveau de protection dans les pays tiers et de conseiller la Commission européenne sur tout projet

ayant une incidence sur les droits et libertés des personnes physiques à l'égard des traitements de données personnelles. Le G29 se réunit à Bruxelles en séance plénière tous les deux mois environ.

Listes d'opposition

Les listes d'opposition recensent les personnes qui ont fait connaître leur opposition à être prospectées dans le cadre d'opérations de marketing.

NIR (Numéro d'inscription au Répertoire)

Le NIR ou numéro de sécurité sociale est attribué à chaque personne à sa naissance sur la base d'éléments d'état civil transmis par les mairies à l'INSEE.

Reconnaissance faciale

En s'appuyant sur une base de photographies préenregistrées reliée à un système de vidéoprotection et à un dispositif de reconnaissance automatique des visages, il est désormais techniquement possible d'identifier un individu dans une foule. Si cette technologie n'en est qu'à ses balbutiements, il importe de comprendre que son caractère intrusif est croissant puisque la liberté d'aller et venir anonymement pourrait être remise en cause.

Responsable de données

Personne qui décide de la création d'un fichier ou d'un traitement de données personnelles, qui détermine à quoi il va servir et selon quelles modalités.

RFID (*Radio Frequency Identification*)

Les puces RFID permettent d'identifier et de localiser des objets ou des personnes. Elles sont composées d'une micropuce (également dénommée étiquette ou tag) et d'une antenne qui dialoguent par ondes radio avec un lecteur, sur des distances pouvant aller de quelques centimètres à plusieurs dizaines de mètres. Pour les applications dans la grande distribution, leur coût est d'environ 5 centimes d'euros. D'autres puces communicantes, plus intelligentes ou plus petites font leur apparition avec l'avènement de l'internet des objets. Certains prototypes sont quasi invisibles (0,15 millimètre de côté et 7,5 micromètres d'épaisseur) alors que d'autres, d'une taille de 2 mm^2, possèdent une capacité de stockage de 512 Ko (kilo-octets) et échangent des données à 10Mbps (méga bits par seconde).

Safe Harbor

Il s'agit d'un ensemble de principes de protection des données personnelles, publiés par le Département du Commerce américain, auxquels des entreprises établies aux Etats-Unis adhèrent afin de pouvoir recevoir des données en provenance de l'Union européenne.

Ces principes, négociés entre les autorités américaines et la Commission européenne en 2001, sont essentiellement basés sur ceux de la Directive 95/46 du 24 octobre 1995 :

- information des personnes,

- possibilité accordée à la personne concernée de s'opposer à un transfert à des tiers ou à une utilisation des données pour des finalités différentes,
- consentement explicite pour les données sensibles,
- droit d'accès, de rectification,
- sécurité.

Le Safe Harbor permet donc d'assurer une protection adéquate pour les transferts de données en provenance de l'Union européenne vers des entreprises établies aux Etats-Unis.

Séance plénière

C'est la formation qui réunit les 17 membres de la CNIL pour se prononcer sur des traitements ou des fichiers et examiner des projets de loi ou de décrets soumis pour avis par le Gouvernement.

Traitement de données

Collecte, enregistrement, utilisation, transmission ou communication d'informations personnelles, ainsi que toute exploitation de fichiers ou bases de données, notamment des interconnexions.

Transfert de données

Toute communication, copie ou déplacement de données personnelles ayant vocation à être traitées dans un pays tiers à l'Union européenne.

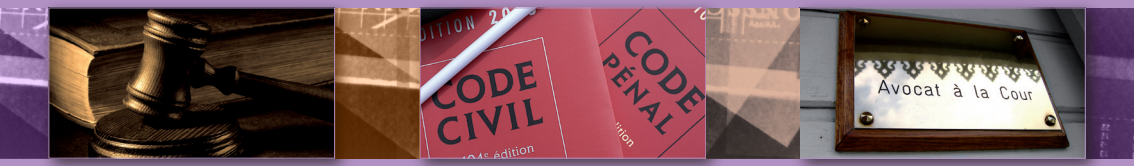
Document Imprimé sur papier 100% recyclé

Une difficulté ? Une hésitation ?

Plus d'informations sur **www.cnil.fr,**

Une permanence de renseignements juridiques
par téléphone est assurée tous les jours
de 10h à 12h et de 14h à 16h
au **01 53 73 22 22**

Vous pouvez adresser toute demande
par télécopie au **01 53 73 22 00**



www.cnil.fr

8 rue Vivienne - CS 30223
75083 Paris cedex 02
Tél : 01 53 73 22 22
Fax : 01 53 73 22 00