

FICHE CONSEIL NUMÉRO 4

LES DECLARATIONS DE FICHIERS A LA CNIL



POURQUOI FAIRE UNE DECLARATION

Pourquoi déclarer les fichiers de données à caractère personnel ? C'est tout simplement une obligation légale issue de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés visant à la protection de l'individu. Cette obligation de déclaration est d'ailleurs assortie de sanctions pénales pour les contrevenants. Vous risquez 300 000 € d'amende et 5 ans d'emprisonnement pour oubli ou fausse déclaration (le plus souvent, suite à des plaintes).

Au-delà des sanctions pénales encourues, l'absence de déclaration peut avoir d'autres conséquences. Citons l'exemple de cette société dont le fichier de la badgeuse n'était pas déclaré à la Cnil et qui, en plus de l'amende, a dû réintégrer les salariés licenciés au motif de retard ou d'absentéisme.

La Commission Nationale Informatique et Libertés (CNIL) est une autorité administrative indépendante qui a pour mission de veiller au respect des dispositions de la loi informatique et libertés. A ce titre elle est chargée d'instruire les dossiers de déclaration ou dans certains cas d'autoriser les traitements. Dans le cadre de son instruction elle veille particulièrement à la légitimité du fichier et/ou du traitement, aux modalités d'accès à l'information les concernant par les individus (voir chapitre « mentions légales ») et à la durée de conservation des données (voir chapitre « quoi déclarer »).

D'un point de vue plus positif, la déclaration à la Cnil et son affichage participe à jouer la transparence et donner une bonne image.

QUOI DECLARER

1. Les types de fichiers exonérés :

Beaucoup de fichiers ou de traitements contenant des données à caractère personnel sont purement et simplement dispensés de formalités déclaratives, le plus souvent parce qu'ils ne portent pas atteinte à la vie privée ou aux libertés.

Vous n'avez pas à déclarer à la CNIL dans les cas suivants :

- **Vous êtes un particulier**, vous ne déclarez pas les fichiers qui concernent votre vie privée ou familiale comme votre carnet d'adresses ou votre site perso si l'accès est réservé à un nombre limité de personnes.
- **Vous êtes une église, un parti politique, un syndicat, un organisme ou une association à caractère religieux, politique, philosophique ou syndical**, vous ne déclarez pas votre fichier de membres, d'adhérents ou de personnes qui sont en contact régulier avec vous.
- **Vous exercez une activité professionnelle dans le domaine artistique (écrivain, cinéaste, éditeur...)**, vous ne déclarez pas les traitements de données personnelles utilisés dans le cadre de cette activité (livres, films, TV...).
- Vous êtes responsable d'un traitement mais vous êtes domicilié dans un autre état membre de la Communauté européenne.
- Vous êtes responsable d'un traitement, établi en dehors de la Communauté européenne et les données personnelles que vous gérez ne font que transiter par la France.
- Les traitements ayant fait l'objet d'une décision de dispense de déclaration par la CNIL (notamment les fichiers paye, les fichiers fournisseurs)



2. Les fichiers devant faire l'objet d'une déclaration :

Vous avez l'obligation de déclarer à la CNIL tout fichier ou traitement de données à caractère personnel

Les plus courants :

- Fichiers clients et/ou prospects
- Sites internet avec recueil d'information on-line
- Jeux concours
- Questionnaires et enquêtes
- Certaines fichiers relatifs au personnel (badgeuse, autocommutateur...) sauf la paye

A savoir

Vos fichiers clients et prospects peuvent faire l'objet d'une seule déclaration, en prévoyant une finalité assez large.



QU'EST-CE QU'UNE DONNÉE A CARACTERE PERSONNEL ?

Ce que dit la loi :

« Constitue une donnée à caractère personnel toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres. Pour déterminer si une personne est identifiable, il convient de considérer l'ensemble des moyens en vue de permettre son identification dont dispose ou auxquels peut avoir accès le responsable du traitement ou toute autre personne. » (art. 2)

« La personne concernée par un traitement de données à caractère personnel est celle à laquelle se rapportent les données qui font l'objet du traitement. » (art. 2)

Le principe

Les données sont considérées comme à caractère personnel dès lors qu'elles concernent des personnes physiques identifiées directement ou indirectement.

Une personne est identifiée lorsque par exemple son nom apparaît dans un fichier.

Une personne est identifiable lorsqu'un fichier comporte des informations permettant indirectement son identification (ex. : n° d'immatriculation, adresse IP, n° de téléphone, photographie...).

En ce sens, constituent également des données à caractère personnel toutes les informations dont le recoupement permet d'identifier une personne précise. (ex. : une empreinte digitale, l'ADN, une date de naissance associée à une commune de résidence ...).

Les technologies de l'information et de la communication génèrent de nombreuses données personnelles (un paiement par carte bancaire, un appel passé par un téléphone portable, une connexion à internet) et aussi des "traces informatiques" facilement exploitables grâce aux progrès des logiciels, notamment les moteurs de recherche.

QU'EST-CE QU'UN TRAITEMENT DE DONNEES ?

Ce que dit la loi :

« Constitue un traitement de données à caractère personnel toute opération ou tout ensemble d'opérations portant sur de telles données, quel que soit le procédé utilisé, et notamment la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction. » (art. 2)

« Constitue un fichier de données à caractère personnel tout ensemble structuré et stable de données à caractère personnel accessibles selon des critères déterminés. » (art. 2)

Exemples de traitements :

Fichier clients, base contacts, autocommutateur, système d'enregistrement des conversations téléphoniques sur support numérique.

Mais également toute procédure de télétransmission de données personnelles, d'interconnexion, de consultation et ce quel que soit le moyen de télécommunication ainsi que toute application de cartes à puce.



A savoir :

Il convient de déterminer, au moment de la déclaration, la finalité du traitement. Celle-ci, tout en restant précise et explicite, pourra regrouper des sous finalités connexes. Le mieux est d'être le plus prévoyant possible de manière à ne pas refaire une déclaration à chaque traitement. Par exemple :

- **finalité** = « gestion d'un fichier clients/prospects »
- **fonctions d'application** = « extraction de la base selon différents critères », « envoi de messages commerciaux »...

Ce qui vous permettra de ne pas refaire une déclaration à chaque fois que vous enverrez un courrier à vos clients ou lorsque vous aurez à faire des tris de votre base par ordre alphabétique !

Recommandations pour la « Durée de conservation des données »

Soignez cette partie de la déclaration, elle est souvent à l'origine de difficultés. Ne vous enfermez pas dans un délai fixe.

Fichier de clients : plutôt qu'un nombre d'années fixe, prévoyez un délai après la dernière relation commerciale (par exemple 3 ans).

Fichier de prospect : la recommandation de la Cnil est de supprimer du fichier un prospect qui n'a répondu après 2 sollicitations commerciales, ce qui est bien sûr modulable selon les secteurs d'activité.

QUAND DECLARER

La déclaration doit être préalable à la mise en œuvre du traitement. Ainsi dès que vous constituez un fichier informatisé (même s'il ne s'agit que d'Excel ou d'un serveur de messagerie) vous devez faire une déclaration initiale. Le mieux est d'anticiper et de prévoir dès la première déclaration toutes les fonctions d'applications possibles afin de ne pas refaire de déclaration lors de l'ajout de nouvelles fonctionnalités.

A savoir

Les déclarations « normales » peuvent faire l'objet de rajouts, ce qui n'est pas le cas des déclarations « simplifiées ».

Attention, le fait de faire une déclaration ne vous dégage en rien de vos responsabilités. Et sachez que le récépissé de celle-ci ne vaut pas agrément du traitement par la CNIL. Il faut compter actuellement près de 2 mois de délais pour obtenir une réponse. Alors si vous devez réaliser une enquête par exemple, et que vous devez soumettre le questionnaire, vous devrez anticiper...

MENTIONS LEGALES

Vos obligations légales ne se limitent pas à la déclaration de vos fichiers informatisés, vous devez également faire apparaître des mentions légales sur vos documents de collecte quel que soit le moyen. L'affichage de celles-ci fait partie des éléments vérifiés en priorité par la Cnil (en particulier, l'accès aux informations).

MODÈLE DE NOTE D'INFORMATION A PORTER SUR LES FORMULAIRES DE COLLECTE

_____ (indication de l'identité du responsable du traitement)
 « Les informations recueillies font l'objet d'un traitement informatique destiné à ... (préciser la finalité). Les destinataires des données sont : _____ (précisez). Conformément à la loi « informatique et libertés » du 6 janvier 1978, vous bénéficiez d'un droit d'accès et de rectification aux informations qui vous concernent. Si vous souhaitez exercer ce droit et obtenir communication des informations vous concernant, veuillez vous adresser à _____ (préciser le service). [vous pouvez également, pour des motifs légitimes, vous opposer au traitement des données vous concernant] » à ne pas faire figurer si le traitement présente un caractère obligatoire.



COMMENT DECLARER

Qui doit déclarer

C'est le responsable du traitement qui doit procéder à la déclaration préalablement à sa mise en oeuvre. **Le prestataire qui réalise le traitement peut tout à fait se charger de la déclaration pour son client** mais ne peut pas le signer. Le responsable reste celui du fichier.

Pour effectuer une déclaration à la CNIL, deux voies vous sont offertes :



La déclaration simplifiée

Vous pouvez effectuer une déclaration simplifiée dès lors que votre fichier ou traitement de données personnelles est strictement conforme à des normes que la CNIL a établies pour les traitements les plus courants, c'est-à-dire ceux dont la mise en oeuvre n'est pas susceptible de porter atteinte à la vie privée ou aux libertés. Il faut vous assurer de la totale conformité d'un traitement à une norme (cf www.cnil.fr.)

Si votre traitement est conforme à une norme, vous pouvez réaliser votre déclaration simplifiée en téléprocédure directement sur le site de la CNIL.

Exemples de normes courantes :

- N°48 : gestion des fichiers de clients et prospects (en cours de publication, anciennement N°11)
- N°46 : badgeuse/ contrôle d'accès
- N°47 : autocommutateurs
- N°15 : traitements automatisés d'informations nominatives relatifs aux listes d'adresses ayant pour objet l'envoi d'informations

La déclaration normale

Si votre traitement ne correspond à aucune norme, vous devez effectuer une déclaration normale et compléter des annexes.

Vous pouvez effectuer votre déclaration en remplissant le formulaire « Déclaration normale » et les annexes.

A savoir

Une nouvelle norme pour les fichiers clients et/ou prospects est en cours de publication (norme 48) car la norme simplifiée actuelle (norme 11) ne prévoit pas la collecte de l'e-mail ! Autant dire que cette norme simplifiée n'était pas très utile de nos jours. En attendant, vous devez donc établir une déclaration normale.

Une fois le formulaire rempli

- Si vous avez effectué une télédéclaration, vous recevez immédiatement après envoi un accusé de réception électronique ;
- Si vous avez utilisé un formulaire papier, veuillez adresser à la CNIL votre dossier de déclaration :
 - soit par envoi recommandé avec demande d'avis de réception postal à :
CNIL, 21, rue Saint-Guillaume 75340 Paris Cedex 07
 - soit par dépôt auprès de la CNIL contre reçu.

La CNIL délivre ensuite par voie postale un récépissé de déclaration qui indique le numéro sous lequel un traitement déclaré est enregistré.



AVERTISSEMENT

Formulaires particuliers

Pour déclarer un site internet avec des données personnelles, vous devez effectuer votre déclaration en téléprocédure directement sur le site de la CNIL ou télécharger le guide « Déclarer un site internet ».

Pour déclarer un fichier de recherche médicale, vous devez compléter le formulaire CERFA n° 10769*01 disponible sur simple demande à la CNIL.

Formalités particulières

Pour des fichiers sensibles ou à risques, comportant par exemple des données biométriques ou génétiques ou encore le NIR ..., la loi a prévu des formalités particulières. Toutefois, dans un souci de simplification, la CNIL se charge de prendre contact avec les responsables des traitements concernés pour compléter et instruire leur dossier.



A savoir :

- **Cas des questionnaires** : vérifier que la fonction d'application « réalisation d'enquêtes » a bien été prévue lors de la déclaration du fichier. Sinon, il faut procéder à une déclaration supplémentaire. Dans tous les cas, le questionnaire peut être envoyé à part, pour une validation.
- **Cas des jeux-concours** avec récupération de données dans un but de prospection : de même que ci-dessus, il faut vérifier que ces fonctions d'applications avaient bien été prévues. La Cnil recommande dans ce cas de procéder à deux déclarations différentes même si ces deux applications ont un lien, en précisant que les données récupérées lors du jeu peuvent être utilisées à des fins de prospection.
- **Cas du data-mining** : la fonction d'application à prévoir est « extraction selon différents critères ». Attention cependant à certains traitements sensibles, par exemple, des statistiques sur l'origine des clients en se basant sur la consonance des noms de famille sont interdites.

CAS DES SITES INTERNET



Vous devez déclarer auprès de la Commission Nationale Informatique et Libertés (CNIL) tout système participant à un traitement automatisé d'informations nominatives. Ainsi, doivent faire l'objet d'une déclaration les sites web, listes de diffusion ou de discussion, forums ou chambres de discussion (*chat room*) qui enregistrent, reproduisent ou exploitent des informations nominatives. Toutefois, les traitements effectués à titre totalement privé, comme la constitution d'un agenda électronique personnel ou d'une liste de contacts sur votre logiciel de courrier électronique, échappent à cette obligation.

A l'heure actuelle, de nombreux sites exploitant des informations nominatives ne sont toujours pas enregistrés auprès de la CNIL. L'exemple n'est pas à suivre car le défaut de déclaration est sanctionné par trois ans d'emprisonnement et 45 000 euros d'amende. La CNIL propose maintenant un formulaire de déclaration en ligne que l'entreprise ou le particulier pourra remplir très facilement en moins de vingt minutes.

Quelles informations faire figurer ?

La loi du 21 juin 2004 pour la confiance dans l'économie numérique fait obligation aux personnes qui éditent un site web de tenir à la disposition du public, sur leur propre site :

- S'il s'agit de personnes physiques ou morales agissant à titre professionnel :

- le nom du directeur ou du codirecteur de la publication et, le cas échéant, celui du responsable de la rédaction ;

- le nom, la dénomination ou la raison sociale et l'adresse et le numéro de téléphone de l'hébergeur.

- pour les personnes physiques : leurs nom, prénoms, domicile et numéro de téléphone et, si elles sont assujetties aux formalités d'inscription au RCS ou au répertoire des métiers, le numéro de leur inscription ;

- pour les personnes morales : leur dénomination ou leur raison sociale et leur siège social, leur numéro de téléphone et, s'il s'agit d'entreprises assujetties aux formalités d'inscription au RCS ou au répertoire des métiers, le numéro de leur inscription, leur capital social, l'adresse de leur siège social ;

- S'il s'agit de personnes physiques ou morales n'agissant pas à titre professionnel :

La loi prévoit une exception pour les particuliers non-professionnels qui, pour préserver leur anonymat, peuvent ne dévoiler que le nom, la dénomination ou la raison sociale et l'adresse de leur hébergeur, sous réserve toutefois qu'ils lui aient communiqué leurs éléments d'identification personnelle. Cette communication est normalement automatique lorsque vous hébergez vos pages dans l'espace mis à votre disposition par votre fournisseur d'accès à l'internet.

Le défaut de mise à disposition du public de ces informations est passible de sanctions pénales.

Si votre site procède à la collecte d'informations nominatives, vous devez par ailleurs informer les personnes concernées de l'existence et des modalités d'exercice du droit d'accès aux informations qui les concernent et du droit de les faire modifier (changement de nom, d'adresse, de fonction, etc...), rectifier en cas d'erreur ou supprimer (article 34 de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés).

En cas d'utilisation de procédés particuliers permettant la collecte invisible de données nominatives, tels que les "cookies" ou les applets java, la CNIL recommande d'informer les visiteurs de leur objet et de la faculté dont ils disposent pour s'y opposer.

ANNEXE : LOI INFORMATIQUE ET LIBERTES

La loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés

Les principes :

■ **Loyauté de la collecte de données** : tout moyen de collecte frauduleux, déloyal ou illicite est interdit (article 226-18 du code pénal : 5 ans d'emprisonnement, 300.000 € d'amende).

■ **Finalité des fichiers** : les traitements informatiques doivent poursuivre une finalité explicite ; c'est au regard de cette finalité que sont appréciés le caractère pertinent, adéquat et non excessif des données enregistrées, les catégories de personnes ou d'organismes qui peuvent être destinataires de ces données et la durée pendant laquelle les données collectées peuvent être conservées (articles 226-21 et 226-20 du code pénal : utiliser des données personnelles à des fins étrangères à celles qui ont justifié leur collecte, ou les conserver au-delà de ce que justifie la finalité du traitement est puni, respectivement, de 5 ans d'emprisonnement et de 300.000 € d'amende et de 5 ans d'emprisonnement et de 45.000 € d'amende).

■ **Information des personnes** : les personnes auprès desquelles sont recueillies des données personnelles doivent être informées de l'identité du responsable du traitement, de la finalité poursuivie par le traitement, du caractère obligatoire ou facultatif des réponses, des conséquences d'un défaut de réponse, des destinataires des données, de leur droit d'accès et de rectification ainsi que de leur droit, sous certaines conditions, de refuser le traitement.



■ **Protection renforcée des données sensibles** : les informations qui font apparaître directement ou indirectement les origines raciales ou ethniques, les opinions politiques, philosophiques ou religieuses, les appartenances syndicales ou les données relatives à la santé ou à la vie sexuelle des personnes ne peuvent être collectées et enregistrées que dans les conditions définies par la loi (article 8). Par exemple, de telles données peuvent être collectées, pour des motifs d'intérêt public, sur autorisation délivrée soit par la CNIL soit par un décret en Conseil d'Etat pris après avis de la CNIL (tel peut être le cas pour certains fichiers de police). L'article 226-19 du code pénal punit toute infraction à ces dispositions de 5 ans d'emprisonnement et de 300.000 € d'amende.

Aucune décision produisant des effets juridiques à l'égard d'une personne ne peut être prise sur le seul fondement d'un traitement informatique destiné à définir le "profil" de l'intéressé ou à évaluer certains aspects de sa personnalité (article 10 de la loi).

Les droits "informatique et libertés" :

Toute personne peut s'adresser directement à un organisme pour savoir si elle est fichée ou pas.

Toute personne peut, gratuitement, sur simple demande adressée à l'organisme considéré, avoir accès à l'intégralité des informations la concernant sous une forme accessible (les codes doivent être explicités) et en obtenir copie moyennant le paiement, le cas échéant, des frais de reproduction.

Toute personne peut demander directement à un organisme détenant des informations sur elle qu'elles soient rectifiées (si elles sont inexacts), complétées ou clarifiées (si elles sont incomplètes ou équivoques), mises à jour (si elles sont périmées) ou effacées (si ces informations ne pouvaient pas être régulièrement collectées).

Toute personne peut s'opposer à ce qu'il soit fait un usage des informations la concernant à des fins publicitaires ou de prospection commerciale ou que les informations la concernant soient cédées à des tiers à de telles fins. Les personnes concernées doivent être mises en mesure d'exercer leur droit d'opposition à la cession de leurs données à des tiers dès la collecte des données. L'utilisation d'automates d'appels téléphoniques ou de fax à des fins publicitaires est interdite si les personnes n'y ont pas préalablement consenti.

Toute personne peut demander à la CNIL de procéder à des vérifications des informations la concernant éventuellement enregistrées dans des fichiers intéressant la sûreté de l'Etat, la défense ou la sécurité publique (droit d'accès indirect). La CNIL vérifie la pertinence, l'exactitude et la mise à jour de ces informations et peut demander leur rectification ou leur suppression. Avec l'accord du responsable du traitement, les informations concernant une personne peuvent lui être communiquées.

Toute personne peut s'adresser à la CNIL pour être aidée dans l'exercice de ses droits (notamment si elle se heurte à un refus de droit d'accès).

Les obligations des responsables des fichiers :

■ Notifier la mise en oeuvre du fichier et ses caractéristiques à la CNIL, sauf cas de dispense prévus par la loi ou par la CNIL.

■ Mettre les personnes concernées en mesure d'exercer leurs droits en les informant et en donnant suite à leurs demandes dans un délai raisonnable.

■ Assurer la sécurité et la confidentialité des informations afin qu'elles ne soient pas déformées ou communiquées à des tiers non autorisés.

■ Se soumettre aux contrôles et vérifications sur place de la CNIL et répondre à toute demande de renseignements qu'elle formule dans le cadre de ses missions.

Les données à caractère personnel

Il peut s'agir évidemment d'informations associées au nom de la personne (par exemple "Benjamin Bernard a commis plusieurs impayés"). Mais il peut s'agir aussi d'informations qui ne sont pas associées au nom d'une personne mais qui permettent aisément de l'identifier (par exemple "le titulaire du numéro de ligne 0153732200 téléphone souvent au Sénégal" ou "le propriétaire du véhicule 3636AB75 est abonné à telle revue" ou encore "l'assuré social 1600530189196 va chez le médecin plus d'une fois par mois").

Constituent des données à caractère personnel, toutes les informations anonymes dont le recoupement permet d'identifier une personne précise (par exemple une empreinte digitale, l'ADN ou encore "le fils du médecin résidant au 11 boulevard Belleville à Montpellier est un mauvais élève").

Les technologies de l'information et de la communication génèrent des données nous concernant de plus en plus nombreuses et de plus en plus précises (un paiement par carte bancaire, un appel passé par un téléphone portable qui permet d'identifier à 400 m le lieu où nous nous trouvons, une connexion à internet).

Les données personnelles ont acquis, notamment avec le développement d'internet, une valeur marchande considérable et sont de ce fait de plus en plus convoitées (les fichiers s'achètent et se vendent, les groupes commerciaux peuvent être tentés d'identifier et de regrouper dans un même traitement les "bons clients" de chacune de leurs filiales ou au contraire les "mauvais clients").

Les "traces informatiques" liées aux technologies de l'information et de la communication peuvent être exploitées de plus en plus aisément grâce aux progrès des logiciels (ainsi de la technologie des moteurs de recherche sur internet ou des logiciels dits "de fouille" des données).