

# Gérez vos fichiers dans les règles de l'art !

## Déclarer ses fichiers

### Quels fichiers déclarer ?

Les entreprises qui détiennent et gèrent des fichiers dans lesquels figurent des informations personnelles sont tenues, en principe, de les déclarer à la Commission nationale de l'informatique et des libertés (Cnil).

Précision : pour la loi, les informations « à caractère personnel » sont celles « qui sont relatives à une personne identifiée ou pouvant être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres » (nom, prénoms, date de naissance, photo, numéro de téléphone, adresse courriel, numéro d'immatriculation, etc.). Une définition large qui a donc vocation à s'appliquer à un grand nombre de données...

Étant précisé que l'obligation de déclaration ne concerne que les fichiers permettant d'identifier des personnes physiques. Les fichiers contenant exclusivement des données relatives à des personnes morales (sociétés, associations...) n'ont pas à être déclarés à la Cnil.

#### Déclaration ou autorisation

Selon le contenu des fichiers et la finalité des traitements dont ils font l'objet, la déclaration à produire peut relever de plusieurs procédures.

– La procédure simplifiée concerne les fichiers qui ne portent pas atteinte à la vie privée et aux libertés individuelles. La Cnil a ainsi établi et publié des normes qui précisent les finalités des traitements pouvant faire l'objet d'une déclaration simplifiée, les données à caractère personnel traitées, la catégorie de personnes concernées, les destinataires auxquels ces données sont communiquées et la durée de conservation de celles-ci.

Les dirigeants d'entreprise peuvent être rassurés : pour les cas les plus courants, ils n'ont à remplir qu'une déclaration simplifiée. Tel est, en effet, le cas des traitements des fichiers clients et prospects de l'entreprise, des fichiers de gestion des horaires des salariés, de la restauration d'entreprise, ou encore des fichiers courants des ressources humaines (gestion des carrières, formation professionnelle des salariés...).

– Pour les traitements qui ne sont pas expressément visés par une norme simplifiée, une déclaration ordinaire s'impose, dans laquelle un certain nombre d'informations complémentaires doivent être données. Il en est ainsi, par exemple, d'un traitement de recrutement des salariés (base de données de CV ou de candidats) ou d'un traitement permettant un contrôle de l'activité professionnelle des salariés.

**Attention** : simplifiée ou ordinaire, la déclaration doit être souscrite avant la mise en œuvre du traitement. Un retard dans l'accomplissement des formalités est susceptible d'être sanctionné au même titre qu'un défaut de déclaration.

– Les traitements les plus sensibles – ceux qui intègrent des données telles que l'origine raciale, les opinions politiques ou religieuses, l'appartenance à un syndicat, la santé, la vie sexuelle, des données génétiques ou biométriques, faisant état de condamnations en justice, etc. – requièrent, quant à eux, une autorisation préalable de la Cnil. C'est le cas par exemple lorsqu'une entreprise décide de fichier ses clients

mauvais payeurs dans une « liste noire » ou lorsqu'elle entend créer un fichier permettant le fonctionnement d'un dispositif d'accès aux locaux par reconnaissance de l'empreinte digitale des salariés.

### Dispense de déclaration

Certains traitements de données très courants, qui ne soulèvent aucune difficulté particulière, sont totalement dispensés de déclaration. Les traitements informatisés de la comptabilité de l'entreprise, de la paie du personnel (rémunérations, tenue des registres obligatoires, déclarations sociales) et de la gestion des fournisseurs peuvent ainsi être mis en œuvre sans aucune formalité à accomplir auprès de la Cnil.

Attention là encore, la dispense de déclaration est subordonnée au respect des conditions posées par la Cnil. Ainsi, par exemple, les fichiers paie sont dispensés de déclaration sous réserve que les traitements de ces données aient pour seules finalités celles indiquées par la Cnil (calcul et paiement des rémunérations...), que les données collectées soient uniquement celles énumérées par la Cnil (identité, situation familiale et matrimoniale, nombre d'enfants à charge...) et que leurs destinataires soient seulement ceux définis par la Cnil (service chargé de l'administration et de la paie du personnel, organismes gérant les différents systèmes d'assurances sociales...).

## **Comment déclarer ?**

Les entreprises peuvent déclarer leurs fichiers à la Cnil par courrier ou, plus simplement, par Internet sur le site [www.cnil.fr](http://www.cnil.fr). Plusieurs types de formulaires peuvent ainsi être remplis selon qu'il s'agit d'une déclaration normale ou simplifiée. Et quelques jours après la déclaration, l'entreprise reçoit un récépissé qui lui permet alors de mettre en œuvre le traitement projeté en toute légalité.

Les demandes d'autorisation nécessitent, quant à elles, un examen plus approfondi par la Cnil. Pouvant également être transmises en ligne, elles doivent faire l'objet d'un dossier complet comprenant un certain nombre d'informations très précises. La réponse de la Cnil intervenant, cette fois, dans un délai de deux mois environ.

À noter que toutes ces formalités sont gratuites.

Notre conseil : remplir correctement une déclaration, et a fortiori une demande d'autorisation, n'est pas simple. Aussi, est-il vivement conseillé de prendre contact avec la Cnil, qui vous informera de la nature et de l'étendue des éventuelles obligations à remplir à son égard et qui vous guidera dans l'accomplissement des formalités. Bien entendu, nous sommes à votre disposition pour vous assister dans vos démarches auprès de la Cnil.

## **Informez les personnes fichées**

Les personnes qui sont concernées par un fichier disposent de droits. Du droit de demander à prendre connaissance des informations les concernant contenues dans le fichier considéré (on parle de « droit d'accès »), du droit de faire procéder à la correction de ces informations (« droit de rectification »), et enfin, du droit de s'opposer, à condition toutefois de faire valoir une raison légitime, à ce que les données personnelles les concernant fassent l'objet d'un traitement et soient, par exemple, utilisées à des fins de prospection commerciale (« droit d'opposition »). Ces droits pouvant être exercés à tout moment.

L'entreprise qui détient des fichiers de données à caractère personnel et procède à des traitements est donc tenue, dès

leur collecte, d'informer les personnes concernées qu'elles disposent de ces droits. En pratique, une mention en ce sens doit être inscrite dans ses divers formulaires de collecte de données (bons de commande, formulaire de contact...) et sur son site Internet.

Bon à savoir : pour simplifier la tâche des entreprises, la Cnil propose sur son site Internet des modèles de mention, la formule générale étant la suivante :

« Les informations recueillies font l'objet d'un traitement informatique destiné à ... (veuillez préciser la finalité). Les destinataires des données sont : ..... (précisez). Conformément à la loi « informatique et libertés » du 6 janvier 1978 modifiée en 2004, vous bénéficiez d'un droit d'accès et de rectification aux informations qui vous concernent, que vous pouvez exercer en vous adressant à ..... (veuillez préciser le service et l'adresse). Vous pouvez également, pour des motifs légitimes, vous opposer au traitement des données vous concernant. »

## **Garantir la sécurité des fichiers**

L'entreprise est aussi garante de la confidentialité et de la sécurité des données à caractère personnel contenues dans ses fichiers. Aussi doit-elle impérativement s'assurer que ces informations ne soient pas divulguées à des personnes qui ne sont pas habilitées à les consulter. Un certain nombre de mesures doivent donc être prises à cette fin. L'entreprise doit notamment sécuriser l'accès aux locaux dans lesquels peuvent se trouver des fichiers de données sensibles et mettre ces derniers sous clé. Elle doit également veiller à ce que l'accès et l'utilisation de ces fichiers ne soient possibles qu'aux personnes habilitées et dotées de mots de passe qu'il sera prudent de changer régulièrement.

**À noter :** le transfert de ces fichiers sensibles vers un pays extérieur à l'Union européenne est en principe interdit.

## **Respecter la finalité des fichiers**

Il convient aussi impérativement de respecter la finalité des traitements ainsi déclarés ou autorisés. En effet, un fichier doit avoir un objectif précis et les informations qu'il contient doivent être cohérentes et utilisées par rapport à cet objectif. Quant à la durée de conservation des données, elle ne doit pas excéder le temps de réalisation de cet objectif.

## **Gare aux sanctions encourues en cas de non-respect des règles !**

Les entreprises qui procèdent ou font procéder, y compris par négligence, à des traitements de données à caractère personnel sans avoir respecté les formalités obligatoires préalables à leur mise en œuvre encourrent deux types de sanctions :

- des sanctions administratives, telles qu'un avertissement, une amende ou encore une injonction de cesser le traitement litigieux, prononcées par la Cnil après une procédure contradictoire au cours de laquelle l'entreprise aura eu la faculté d'apporter des explications et été invitée à se mettre en conformité avec la loi ;

- des sanctions pénales, qui peuvent aller jusqu'à 5 ans d'emprisonnement et 300 000 € d'amende, infligées par les

tribunaux (mais rarement prononcées en pratique). Ces sanctions pénales sont également encourues en cas de violation de l'obligation de garantir la sécurité et la confidentialité des données ou de non-respect de la durée de conservation des informations ou de la finalité d'un traitement.

## **Désignez un correspondant informatique et libertés !**

Une entreprise a tout intérêt à désigner en interne un « correspondant à la protection des données à caractère personnel », plus communément appelé « correspondant informatique et libertés » (Cil). En effet, ce Cil est chargé de veiller au bon respect dans l'entreprise des obligations imposées par la loi informatique et libertés. Et l'existence d'un Cil dispense l'entreprise des formalités de déclarations préalables obligatoires.

Cette fonction peut être assurée par n'importe quel salarié de l'entreprise dès lors qu'il possède un minimum de compétences juridiques et techniques. Pour des raisons d'indépendance et d'objectivité, il ne peut s'agir ni d'un dirigeant ni d'un associé de la société.

La nomination d'un Cil doit être portée à la connaissance des représentants du personnel et être notifiée à la Cnil.