

Ce qu'il faut retenir :

Lorsque le dispositif d'enregistrement vidéo fait appel à des moyens informatiques (ex : surveillance vidéo IP, stockage des images sur support numérique, etc.) il est nécessaire de déclarer le dispositif à la CNIL.

Lorsque le système s'accompagne d'un dispositif biométrique (ex : reconnaissance faciale, analyse comportementale), Il doit faire l'objet d'une demande d'autorisation auprès de la CNIL puisqu'il fait appel à une technique biométrique (voir fiche n° 12).

2. La nécessité d'une analyse préalable des risques

Une réflexion préalable à l'installation d'un système de vidéosurveillance, basée sur une analyse précise des risques doit être menée afin d'identifier des solutions alternatives (une sécurisation des accès au moyen de badges magnétiques peut par exemple constituer la réponse efficace et adaptée à un objectif particulier de sécurisation).

3. La nécessité de respecter le principe de proportionnalité

La mise en œuvre d'un système de vidéosurveillance des employés doit nécessairement respecter le principe de proportionnalité. Elle doit donc s'effectuer de façon **adéquate, pertinente, non excessive et strictement nécessaire à l'objectif poursuivi**.

Si le déploiement de tels dispositifs sur un lieu de travail répond généralement à un objectif sécuritaire (contrôle des accès aux locaux, surveillance de zones de travail à risques), il ne peut ainsi avoir pour seul objectif la mise sous surveillance spécifique d'un employé déterminé ou d'un groupe particulier d'employés.

Le nombre, l'emplacement, l'orientation, les fonctionnalités et les périodes de fonctionnement des caméras, ou la nature des tâches accomplies par les personnes devant être soumises à la vidéosurveillance, sont autant d'éléments à prendre en compte lors de l'installation du système.

L'enregistrement du son associé aux images rend le système encore plus intrusif. Dès lors, ce type d'enregistrements est disproportionné, sauf justification particulière.

Exemples de systèmes de vidéosurveillance susceptibles de présenter un caractère illégal : installation de caméras dans les vestiaires, les douches, les toilettes ; installation d'un dispositif à l'insu des employés ou de façon non visible (caméra miniaturisée) ; système permettant d'enregistrer de façon spécifique les allées et venues des personnes se rendant dans un local syndical.

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

> L'information des salariés et visiteurs

Les personnes concernées (employés ou visiteurs) doivent être informées, au moyen d'un panneau affiché de façon visible dans les locaux sous vidéosurveillance, 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 (voir modèle proposé en annexe).

> une consultation des représentants du personnel

Les instances représentatives du personnel doivent être consultées avant toute mise en œuvre d'un système de vidéosurveillance et précisément informées des fonctionnalités envisagées (article L2323-32 du code du travail, textes relatifs aux trois fonctions publiques, lois n° 84-16 du 11 janvier 1984, n° 84-53 du 26 janvier 1984 et n° 86-33 du 9 janvier 1986).

■ 5. Une visualisation des images restreinte aux seuls destinataires habilités

Les images enregistrées ne peuvent être visionnées que par les seules personnes habilitées à cet effet, dans le cadre de leurs fonctions (par exemple : le responsable de la sécurité de l'organisme). Ces personnes doivent être particulièrement formées et sensibilisées aux règles encadrant la mise en œuvre d'un système de vidéosurveillance.

■ 6. Une durée de conservation des images limitée

Les images ne devraient pas être conservées plus de quelques jours : en effet, en cas d'incident, la visualisation des images s'effectue généralement rapidement. Leur durée de conservation ne doit en tout état de cause s'étendre au-delà **d'un mois**.

Lorsque c'est techniquement possible, une durée maximale de conservation des images doit être paramétrée dans le système. Elle ne doit pas être fixée en fonction de la capacité technique de stockage de l'enregistreur.

■ 7. Comment déclarer ?

Un système de vidéosurveillance numérique mis en place sur un lieu de travail ne peut être installé 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 déclaration à la CNIL ne peut être opposé aux employés.



■ 3. Les droits spécifiques des employés protégés

Toute utilisation des informations issues de l'utilisation des services de téléphonie pour un contrôle des appels émis et reçus par les représentants du personnel et les représentants syndicaux dans le cadre de leur mandat est **interdite**.

Depuis un arrêt de la Cour de Cassation du 6 avril 2004, les employés investis d'un mandat électif ou syndical doivent pouvoir 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).

■ 4. Comment déclarer ?

Concernant les fichiers mis en œuvre dans le cadre de l'utilisation de service de téléphonie fixe et mobile, l'employeur a la possibilité d'effectuer une déclaration de conformité à la norme simplifiée n°47.

Si toutefois, le dispositif mis en place dépasse le cadre prévu par cette norme, l'employeur doit faire une déclaration normale sauf en cas de désignation d'un correspondant informatique et libertés (dispense de déclaration).



Fiche n° 10 – les dispositifs de géolocalisation gsm/gps

Certains employeurs équipent leurs véhicules professionnels de dispositifs de géolocalisation GPS/GSM. Compte tenu des risques d'atteinte aux droits et libertés des personnes que comporte l'utilisation de ces dispositifs, la CNIL a estimé nécessaire de préciser, dans une recommandation du 16 mars 2006, les conditions dans lesquelles ils pouvaient être utilisés.

■ 1. Pourquoi géolocaliser les véhicules des employés ?

Un dispositif de géolocalisation peut être mis en place pour les finalités suivantes à savoir :

- la contribution à la sécurité des personnes ou des marchandises transportées ;
- une meilleure gestion des moyens en personnel et véhicules (prestations à accomplir en des lieux dispersés) ;
- le suivi et la facturation d'une prestation ;
- le suivi du temps de travail des employés, lorsque ce suivi ne peut être réalisé par d'autres moyens.

En revanche, le recours à la géolocalisation n'est pas justifié lorsqu'un employé dispose d'une liberté dans l'organisation de ses déplacements (visiteurs médicaux, VRP, etc.).

L'utilisation d'un dispositif de géolocalisation ne doit pas conduire à un contrôle permanent de l'employé concerné. Ainsi, la CNIL recommande la désactivation du système embarqué dans les véhicules de fonction des employés en dehors des horaires de travail.

■ 2. À quelles conditions ?

La mise en œuvre d'un traitement de géolocalisation :

- ne doit pas permettre la collecte d'informations concernant les éventuels dépassements des limitations de vitesse ;
- doit nécessairement s'accompagner de mesures de sécurité limitant l'accès aux données de géolocalisation aux personnes habilitées ;
- nécessite de fixer une durée de conservation adéquate de ces données (généralement 2 mois) ;
- implique au préalable la consultation des instances représentatives du personnel et l'information individuelle des employés concernés relative à la finalité du traitement, les données traitées, leur durée de conservation, les destinataires des données, leurs droits d'accès, de rectification et d'opposition (voir modèle proposé en annexe) ;
- ne doit pas s'appliquer aux employés investis d'un mandat électif ou syndical lorsqu'ils agissent dans le cadre de leur mandat.



3. Comment déclarer?

Si le dispositif de géolocalisation des véhicules des employés est en tout point conforme aux prescriptions de la norme simplifiée n° 51 du 16 mars 2006, le responsable du traitement peut procéder en ligne à une déclaration de conformité à cette norme. Dans les autres cas, il lui appartiendra d'adresser une déclaration normale à la CNIL, sauf désignation d'un Correspondant informatique et libertés (dispense de déclaration).



Fiche n° 11 – utilisation de badges sur le lieu de travail

Sur le lieu de travail, les badges électroniques (cartes magnétiques ou à puce) servent notamment au contrôle des accès aux locaux, à la gestion des temps de travail, ainsi qu'à la gestion de la restauration d'entreprise.

Ces différents types de dispositifs, qui comportent des données permettant l'identification des employés, sont soumis à la loi « informatique et libertés » et, ainsi que la Cour de cassation l'a rappelé dans son arrêt du 6 avril 2004, doivent être préalablement déclarés auprès de la CNIL, sauf désignation d'un correspondant informatique et libertés.

■ 1. 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 notamment susceptibles de « tracer » les déplacements des salariés à des fins de surveillance de leur activité.

Par ailleurs, les enregistrements réalisés peuvent parfois permettre à l'employeur d'accéder à des informations privées (consommations de ses personnels au sein du restaurant d'entreprise).

Des garanties particulières doivent donc être apportées par l'employeur pour éviter de tels détournements de finalité. Il doit notamment préciser :

- la finalité du dispositif (ex : contrôle des accès, gestion des temps de présence...);
- les informations qui seront collectées;
- les services destinataires des données;
- les modalités d'exercice du droit d'accès à ces données.

Les personnels et leurs représentants doivent être parfaitement informés de ces modalités, préalablement à la mise en œuvre du système de badges (voir modèle proposé en annexe).

■ 2. Comment déclarer ?

Si le dispositif envisagé respecte en tout point le cadre fixé par la norme simplifiée n° 42, l'employeur privé ou public peut effectuer une déclaration simplifiée sauf s'il a désigné un correspondant informatique et libertés auquel cas il est dispensé de déclaration.

Dans le cas contraire - notamment en cas de recours à des dispositifs biométriques -, des formalités de déclaration particulières voire de demande d'autorisation devront être accomplies auprès de la CNIL (cf. fiche n°12).

Fiche n° 12 – 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 sont donc soumis à un contrôle particulier de la CNIL.

Ainsi, ces dispositifs ne peuvent être mis en œuvre sans autorisation préalable de la CNIL.

La biométrie, qu'est-ce que c'est ?

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...). Elles se rapprochent ainsi de ce qui pourrait être défini comme un « identificateur unique universel », permettant de fait le traçage des individus.

1. Le cadre juridique

Tous les dispositifs de reconnaissance biométrique sont soumis à autorisation préalable de la CNIL quel que soit le procédé technique retenu (contour ou forme de la main, empreinte digitale...). Il appartient à chaque organisme d'adresser une demande d'autorisation à la CNIL. Sauf trois cas de figure précisés ci-après, chaque application fait l'objet d'un examen au cas par cas, en fonction notamment de la caractéristique biométrique utilisée.

Attention

La CNIL n'agrée pas et ne labellise pas les dispositifs biométriques. Les sociétés qui commercialisent ce type de dispositifs ne peuvent donc en aucune façon se prévaloir d'un quelconque agrément de la CNIL sur leur produit.

2. Des formalités allégées pour certains dispositifs biométriques

Afin de faciliter les formalités, la Commission a défini un cadre, appelé autorisation unique, applicable à certains dispositifs biométriques. Le principe est le suivant : lorsque, par exemple, un employeur souhaite mettre en œuvre un dispositif biométrique qui répond aux conditions définies dans ce cadre, il peut bénéficier d'une procédure simplifiée. Il lui suffit alors d'adresser à la CNIL une simple déclaration de conformité.



Cette procédure d'autorisation unique s'applique à trois types de dispositifs reposant sur la reconnaissance :

- du contour de la main pour assurer le contrôle d'accès au restaurant scolaire (autorisation n°AU-009);
- 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 n°AU-008);
- de l'empreinte digitale exclusivement enregistrée sur un support individuel détenu par la personne concernée pour contrôler l'accès aux locaux professionnels (autorisation n°AU-007).

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 le 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. En outre, et conformément au Code du travail et à la législation applicable à la fonction publique territoriale, les instances représentatives du personnel doivent, le cas échéant, être consultées et informées avant la mise en œuvre des dispositifs.

voir modèle proposé en annexe

4. Le cas particulier des dispositifs reposant sur l'enregistrement des empreintes digitales dans une base de données

Dans une communication destinée à mieux informer les salariés sur leurs droits et permettre aux entreprises et administrations de se poser les bonnes questions « informatique et libertés » la CNIL rappelle que :

- **l'empreinte digitale est une biométrie à « trace »**. Chacun laisse des traces de ses empreintes digitales, plus ou moins facilement exploitables, dans beaucoup de circonstances de la vie courante (sur un verre ou une poignée de porte etc.) ;

- ces « traces » peuvent être capturées à l'insu des personnes et être utilisées notamment pour usurper leur identité.

Par conséquent, ces dispositifs ne sont justifiés que s'ils sont fondés sur un fort impératif de sécurité et satisfont aux quatre exigences suivantes :

- **la finalité du dispositif** : elle doit être limitée au contrôle de l'accès d'un nombre limité de personnes à une zone bien déterminée, représentant ou contenant un enjeu majeur dépassant l'intérêt strict de l'organisme tel que la protection de l'intégrité physique des personnes, de celle des biens et des installations ou encore de celles de certaines informations (ex : accès à une centrale nucléaire, à une cellule de production de vaccins ou à un site Seveso II) ;
- **la proportionnalité** : le système proposé est-il bien adapté à la finalité préalablement définie eu égard aux risques qu'il comporte en matière de protection des données à caractère personnel ?
- **la sécurité** : le dispositif doit permettre à la fois une authentification et/ou une identification fiable des personnes et comporter toutes garanties de sécurité pour éviter la divulgation des données ;
- **l'information des personnes concernées** : elle doit être réalisée dans le respect de la loi « informatique et libertés » et, le cas échéant, du Code du travail.

5. Comment déclarer ?

Si le dispositif biométrique est conforme à l'une de ces trois autorisations uniques, il suffit d'adresser à la CNIL une simple déclaration de conformité qui peut s'effectuer en ligne sur www.cnil.fr.

Les traitements ne relevant pas de l'une de ces autorisations uniques doivent faire l'objet d'une demande d'autorisation. Cette demande est constituée du formulaire de déclaration, complété et signé par le responsable du traitement ou son représentant, accompagné des annexes « sécurité » (également disponibles sur le site web de la CNIL), ainsi que de tout élément justifiant la mise en place du dispositif de reconnaissance biométrique envisagé.



prévues par la loi (en ce qui concerne la finalité du fichier, sécurité et confidentialité, les droits des personnes...).

4. Les formalités particulières

Certains traitements peuvent relever d'un **régime d'autorisation** ou de **demande d'avis**. Il s'agit de régimes plus protecteurs, qui s'appliquent aux fichiers considérés comme « sensibles » ou comportant des risques pour la vie privée ou les libertés.

> **La procédure d'autorisation (art. 25)** concerne :

- les traitements qui comportent des données sensibles énumérées à l'article 8 de la loi ;
- les traitements qui comportent des données relatives aux infractions ou condamnations ;
- les traitements qui comportent le numéro de sécurité sociale (NIR) ou qui nécessitent une interrogation du répertoire national d'identification des personnes physiques (RNIPP) ;
- les traitements qui procèdent à l'interconnexion de fichiers dont les finalités principales sont différentes ;
- les traitements de données comportant des appréciations sur les difficultés sociales des personnes ;
- les traitements qui utilisent des données biométriques.

Le traitement devra respecter en tout point le cadre fixé par l'autorisation délivrée par la CNIL.

> **La procédure de demande d'avis (art. 27)** concerne principalement les administrations ou les entreprises gérant un service public pour les fichiers comportant le numéro de sécurité sociale (NIR) ou nécessitant une interrogation du répertoire national d'identification des personnes physiques (RNIPP), et les téléservices de l'administration électronique comportant un identifiant des personnes physiques.

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

5. Une fois le dossier complété

Dans le cas d'une **déclaration en ligne**, la CNIL adresse immédiatement après envoi un accusé de réception électronique.

La CNIL délivre ensuite par voie postale ou électronique un **récépissé de déclaration** indiquant le numéro sous lequel le traitement déclaré est enregistré.

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.



Tableau récapitulatif : quelle déclaration pour quel fichier ?

FINALITÉ DU FICHIER	FORMALITÉS DÉCLARATIVES	CONDITIONS PARTICULIÈRES
<p>Paie</p> <p>Déclarations fiscales et sociales obligatoires (déclarations aux organismes de protection sociale, de retraite et de prévoyance, DADS, DUE, travailleurs handicapés...), y compris celles réalisées à partir de www.net-entreprises.fr</p> <p>Tenue des registres obligatoires (registre unique du personnel...)</p> <p>Tenue des comptes individuels relatifs à l'intéressement et à la participation</p> <p>Statistiques non nominatives liées à l'activité salariée dans l'entreprise</p>	AUCUNE	<p>Respecter les termes de la dispense n° 1 (employeurs publics) ou la dispense n° 2 (employeurs privés) du 9 décembre 2004</p> <p>Attention : Les transferts de données vers un pays tiers à l'Union Européenne ne sont pas dispensés.</p>
Tenue d'une liste d'initiés dans les conditions fixées par le Code des marchés financiers	AUCUNE	Respecter les termes de la dispense n°9 du 6 juillet 2006
Comptabilité générale	AUCUNE	Respecter les termes de la dispense n° 80-34 du 21 octobre 1980
Traitements mis en œuvre par les CE, ou les délégués du personnel pour la gestion de leurs activités sociales et culturelles	AUCUNE	Respecter les termes de la dispense n° 10 du 17 octobre 2006
<ul style="list-style-type: none"> • Gestion des contrôles d'accès aux locaux, • Gestion des horaires, • Gestion de la restauration d'entreprise 	<p>DÉCLARATION SIMPLIFIÉE</p> <p>Si désignation d'un correspondant informatique et libertés : AUCUNE</p>	<p>Respecter la norme simplifiée n° 42.</p> <p>Cette norme ne concerne pas les traitements recourant à un procédé de reconnaissance biométrique, qui sont soumis à une procédure d'autorisation</p>

<p>Fichiers courants de gestion des ressources humaines :</p> <ul style="list-style-type: none"> • gestion administrative (dossiers professionnels, annuaires, élections professionnelles, convocations) • mise à disposition d'outils informatiques (suivi et maintenance, annuaires informatiques, messagerie électronique, Intranet) • organisation du travail (agenda professionnel, gestion des tâches) • gestion des carrières (évaluation, validation des acquis, mobilité...) • gestion de la formation 	<p>DÉCLARATION SIMPLIFIÉE</p> <p>Si désignation d'un correspondant informatique et libertés : AUCUNE</p>	<p>Respecter la norme simplifiée n° 46.</p> <p>Cette norme exclut notamment :</p> <ul style="list-style-type: none"> • les traitements permettant le contrôle individuel de l'activité des employés • les dispositifs ayant pour objet l'établissement du profil psychologique des employés • les transferts de données vers un pays tiers à l'union européenne
<p>Mise en œuvre de services de téléphonie fixe et mobile sur les lieux de travail</p> <p>Gestion des communications (annuaire interne, gestion des dotations, messagerie téléphonique interne, maîtrise des dépenses liées à l'utilisation des services de téléphonie...)</p>	<p>DÉCLARATION SIMPLIFIÉE</p> <p>Si désignation d'un correspondant informatique et libertés : AUCUNE</p>	<p>Respecter la norme simplifiée n° 47.</p> <p>Cette norme exclut expressément :</p> <ul style="list-style-type: none"> • les finalités relatives à l'écoute ou à l'enregistrement de conversations téléphoniques • la localisation d'un employé à partir de son téléphone portable
<p>Mise en œuvre de services destinés à géolocaliser les véhicules utilisés par les employés</p>	<p>DÉCLARATION SIMPLIFIÉE</p> <p>Si désignation d'un correspondant informatique et libertés : AUCUNE</p>	<p>Respecter la norme simplifiée n° 51.</p>



<p>Tout autre traitement automatisé, dès lors qu'il n'est pas conforme aux normes élaborées par la Commission, notamment :</p> <p>Annuaire du personnel sur internet Traitements informatiques permettant un contrôle de l'activité professionnelle des salariés (surveillance des connexions internet ou de la messagerie électronique, géolocalisation) Traitements de vidéosurveillance Traitements de recrutement (base de données de CV ou de candidats)</p> <p>Traitements comportant un transfert de données vers un pays tiers à l'Union européenne</p>	<p>DÉCLARATION NORMALE</p> <p>Si désignation d'un correspondant informatique et libertés :</p> <p>AUCUNE</p> <p>AUTORISATION</p>	<p>Utiliser le formulaire de déclaration normale (téléchargeable sur le site de la CNIL www.cnil.fr, rubrique déclarer, mode d'emploi)</p> <p>Pour les fichiers de recrutement : se référer à la recommandation n° 02-017 du 21 mars 2002</p>
<p>Dispositifs biométriques : 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</p>	<p>AUTORISATION UNIQUE</p>	<p>Respecter les termes de l'autorisation unique AU-008</p>
<p>Dispositifs biométriques : reconnaissance de l'empreinte digitale exclusivement enregistrée sur un support individuel détenu par la personne concernée pour contrôler l'accès aux locaux professionnels</p>	<p>AUTORISATION UNIQUE</p>	<p>Respecter les termes de l'autorisation unique AU-007</p>
<p>Dispositifs d'alerte professionnelle (lignes éthiques) dans le domaine financier, comptable, bancaire et de la lutte contre la corruption.</p>	<p>AUTORISATION UNIQUE</p>	<p>Respecter les termes de l'autorisation unique AU-004</p>

Autres dispositifs biométriques	AUTORISATION	Un système recourant, par exemple, à un procédé de reconnaissance des empreintes digitales avec base centrale ne peut être mis en œuvre sans l'autorisation préalable de la CNIL
Autres dispositifs d'alertes professionnelles	AUTORISATION	Un dispositif permettant de signaler des violations autres que comptables ou financières (ex : harcèlement, atteinte aux droits de propriété intellectuelle, violation d'un code de bonne conduite...)

Dans tous les cas, la déclaration doit être effectuée avant la mise en œuvre du traitement. Cette mise en œuvre ne peut intervenir qu'à réception du récépissé de déclaration (pour les déclarations simplifiées et normales) ou de l'autorisation de la CNIL (pour les demandes d'autorisation).

Droit à l'information

Conformément aux dispositions du code du travail (L2323-32) et aux textes relatifs aux trois fonctions publiques (lois n°84-16 du 11 janvier 1984, n°84-53 du 26 janvier 1984 et n°86-33 du 9 janvier 1986), les instances représentatives du personnel doivent être consultées et précisément informées des fonctionnalités envisagées dans le cas de mise en œuvre de traitements qui ont une incidence sur le personnel.

De plus, le code du travail prévoit qu'aucune information concernant directement un salarié ne peut être collectée par un dispositif qui n'a pas été porté préalablement à sa connaissance (L1221-9 et L1222-4).

Les employés doivent, **dans tous les cas de figure**, être informés **individuellement** de l'existence des traitements contenant des données personnelles les concernant par note, affichage, publication dans le journal interne, courrier électronique...

En application de la loi du 6 janvier 1978 modifiée, les personnels concernés doivent être informés de la ou des finalité(s) et fonctionnalités précises de chaque traitement automatisé mis en œuvre par l'employeur, des conséquences individuelles qui pourront en résulter (par exemple un contrôle), des destinataires des données enregistrées et de leur droit d'accès, d'opposition et de rectification à ces données.

À cet égard, la déclaration adressée à la CNIL doit préciser les mesures relatives à l'information individuelle des salariés.

Toute personne peut obtenir communication de la liste des traitements déclarés au sein d'un organisme sur simple demande écrite (article 31 de la loi du 6 janvier 1978 modifiée). Le contenu d'un dossier de déclaration peut être communiqué au titre de la loi dite « CADA » du 17 juillet 1978.



Exemples de notes d'informations

(Ces exemples doivent être adaptés par le responsable du traitement)

■ Mention d'information à 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 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 (préciser le service et l'adresse).
(vous pouvez également, pour des motifs légitimes, vous opposer au traitement des données vous concernant).

■ Note d'information susceptible d'être affichée

Le(s) service(s).....(citer le nom du ou des services responsables du traitement) dispose(nt) de moyens informatiques destinés à gérer plus facilement(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 : (préciser les destinataires).

Conformément aux articles 39 et suivants de la loi n° 78-17 du 6 janvier 1978 modifiée en 2004 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.....(citer le nom du service ou des services concernés).

■ Courrier d'information (annuaire diffusé sur internet)

Madame, Monsieur,

Nous envisageons de diffuser prochainement sur notre site Internet (indiquez ici le nom de domaine de votre site. Exemple : *www.monsite.fr*) des informations vous concernant dans le cadre de (A 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.

Attention!

En l'absence de réponse de votre part dans un délai d'un mois à compter de la réception de ce courrier, votre accord sera réputé acquis. Vous pourrez toutefois nous faire part ultérieurement, à tout moment, de votre souhait que la diffusion de vos données sur Internet cesse.

Nous vous rappelons que vous disposez d'un droit d'accès, de modification, de rectification et de suppression des données qui vous concernent. Pour exercer ce droit, adressez-vous à :

(indiquez ici l'adresse où les personnes peuvent exercer leur droit d'accès et de rectification)

Panneau d'information (vidéosurveillance)

(ce panneau doit être situé à l'entrée de l'établissement et visible par les salariés et les personnes extérieures)

Établissement sous vidéosurveillance
(représentation graphique d'une caméra)

Nous vous informons que cet établissement est placé sous vidéosurveillance pour des raisons de ... *(indiquer les finalités poursuivies)*. Pour tout renseignement, s'adresser au service ... ou à ... *(identifier 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 relative à l'informatique, aux fichiers et aux libertés, modifiée par la loi du 6 août 2004.

Note d'information adressée au personnel (géolocalisation)

..... *(indication de l'identité du responsable du traitement)* Nous avons installé, dans les véhicules, un système permettant de les localiser en temps réel.

Ce nouveau service va nous servir *(précisez ici la finalité, par exemple, repérer le véhicule le plus proche à la demande d'un client)*. Nous aurons connaissance de l'itinéraire que vous suivez ainsi que des arrêts que vous effectuez.

Les données relatives à vos déplacements sont conservées au maximum *(précisez)*. Au-delà, toutes les données sont rendues anonymes et ont pour seul objet la réalisation de statistiques.

Seuls les services suivants sont destinataires de ces informations *(précisez, par exemple direction des ressources humaines, responsables opérationnels...)*.

Conformément à la loi « informatique et libertés » du 6 janvier 1978 modifiée en 2004, vous pouvez avoir accès et rectifier les informations qui vous concernent en vous adressant à *(préciser le service et l'adresse)*.



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 :



Une difficulté ? Une hésitation ?

Pour plus d'informations, vous trouverez sur le site de la CNIL www.cnil.fr, rubrique « Déclarer » :

- un scénario en ligne d'aide à la déclaration
- tous renseignements utiles pour la désignation d'un CIL

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

Vous pouvez en outre adresser toute demande par télécopie au **01 53 73 22 00**
(réponse sous 15 jours en moyenne)





www.cnil.fr

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