FIEEC

FEDERATION DES INDUSTRIES ELECTRIQUES, ELECTRONIQUES ET DE COMMUNICATION

JUILLET 2016

Guide Pratique

Organisations professionnelles

Gestion des données personnelles dans l'entreprise

FÉDÉRATION DES INDUSTRIES ELECTRIQUES, ELECTRONIQUES ET DE COMMUNICATION

Edito

La gestion des données personnelles est désormais au cœur du quotidien de l'entreprise. Et cela ne vaut pas seulement pour les groupes spécialisés dans les technologies de la communication, loin de là. Avec l'essor du numérique, toutes les entreprises – de la PME à la multinationale – sont conduites à traiter de plus en plus de données à caractère personnel dans le cadre de leurs activités quotidiennes. Gestion du recrutement et du fichier client, de l'annuaire du personnel, utilisation de badges, vidéosurveillance ou encore géolocalisation : toutes ces pratiques impliquent le maniement de données personnelles.

Pour les entreprises, l'enjeu relatif à ces usages croissants de données n'est pas seulement de nature juridique. Il va plus loin que la seule conformité à la loi Informatique et Libertés. Il influence aussi la qualité de la relation avec leurs clients, les échanges avec leurs écosystèmes d'innovation, l'éthique interne des salariés. En un mot, l'entreprise est-elle digne de confiance vis-à-vis de l'ensemble des parties prenantes qui travaillent avec elle ? C'est particulièrement vrai depuis quelques années, alors que les individus sont de plus en plus sensibles aux risques liés au maniement de leurs données. Dans ce contexte, la conformité peut aussi devenir un argument concurrentiel pour l'entreprise soucieuse d'attirer et de retenir consommateurs et talents.

La Commission Nationale de l'Informatique et des Libertés s'est particulièrement attachée ces dernières années à accompagner les entreprises dans cette direction. Elle l'a fait en répondant à des demandes de conseil toujours plus nombreuses. Elle l'a fait également en développant de nouveaux outils : labels, packs de conformité élaborés en concertation avec différents secteurs ou encore mise en place du Correspondant Informatique et Libertés. Ces nouveaux outils de régulation participent d'un même objectif : diffuser toujours mieux la culture Informatique et Libertés au sein des entreprises et préciser dans une perspective opérationnelle les contours des obligations auxquelles celles-ci sont soumises.

Ces nouveaux outils portent en eux-mêmes une certaine idée de la régulation : une régulation co-construite, dans laquelle le régulateur et le régulé agissent de concert en jouant de leur complémentarité. Je salue donc l'initiative prise par la FIEEC de s'approprier les recommandations de la CNIL pour élaborer les fiches pratiques rassemblées dans le présent guide. Elle illustre une nouvelle fois la fécondité du partenariat noué depuis plusieurs années entre nos deux institutions.

Isabelle Falque-Pierrotin

Présidente de la CNiL

Introduction

Au quotidien, les entreprises sont amenées à collecter de nombreuses informations à caractère personnel sur leurs salariés par le biais de solutions informatiques facilitant de plus en plus la gestion des données. C'est le cas, par exemple, du traitement de données par le service des ressources humaines dans le cadre des recrutements, de la gestion des carrières et des compétences, du suivi du temps de travail, etc. En parallèle, certaines entreprises mettent également en place des dispositifs de contrôle comme la vidéosurveillance, la cybersurveillance, la géolocalisation, etc.

Dans la mesure où toute divulgation ou mauvaise utilisation des données est susceptible de porter atteinte aux droits et libertés des personnes, ou à leur vie privée, il est essentiel de veiller au respect des règles de protection des données à caractère personnel. A ce titre, la loi Informatique et Libertés du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée par la loi du 6 août 2004, fixe un cadre à la collecte et au traitement des données afin de protéger les salariés.

Elle met en avant 5 principes à respecter en cas de collecte, de traitement et de conservation des données à caractère privé :

- La finalité du traitement,
- La proportionnalité et la pertinence des données collectées,
- La durée de conservation des données,
- La sécurité et la confidentialité des données,
- Le respect des droits des personnes.

Ainsi, une entreprise devra respecter ces principes et, la plupart du temps, informer la Commission de Nationale de l'Informatique et des Libertés (CNIL) de la collecte et du traitement de ce type de données.

Ce guide a pour objectif de sensibiliser tout employeur sur les obligations qui lui incombent en cas de traitement de données à caractère personnel sur ses salariés, et de les informer sur les mesures à mettre en œuvre pour se conformer à la loi.

SOMMAIRE

Fiche 1 - Les obligations de l'employeur en cas de traitement de données à caractère personnel 9

Fiche 2 - Les opérations de recrutement 14

Fiche 3 - Les annuaires du personnel 19

Fiche 4 - L'accès au dossier professionnel 21

Fiche 5 - Les réseaux sociaux externes 23

Fiche 6 - Les réseaux sociaux d'entreprises 30

Fiche 7 - Le contrôle de l'utilisation d'internet et de la messagerie 34

Fiche 8 - Les administrateurs réseaux 40

Fiche 9 - La vidéosurveillance sur les lieux de travail 42

Fiche 10 - La gestion de la téléphonie 48

Fiche 11 - Les dispositifs de géolocalisation des véhicules 51

Fiche 12 - L'utilisation de badges ou de dispositifs biométriques sur le lieu de travail 54

Annexes 57

Les obligations de l'employeur en cas de traitement de données à caractère personnel 1

Tout traitement de données personnelles par un employeur est soumis à des **obligations destinées à protéger la vie privée de ses salariés et leurs libertés individuelles** : recueillir l'accord des salariés, les informer de leur droit d'accès, de modification et de suppression des informations collectées, veiller à la sécurité des systèmes d'information, assurer la confidentialité des données, indiquer une durée de conservation des données.

Ces obligations varient selon la **nature du fichier et la finalité des informations recueillies.**

L'obligation de déclaration à la CNIL[1]

Principe

Tout fichier ou traitement automatisé contenant des informations à caractère personnel doit être déclaré avant sa création, en ligne ou par courrier adressé à la Commission nationale de l'informatique et des libertés (CNIL) sous forme d'une déclaration normale ou simplifiée.

Qu'est-ce qu'une donnée à caractère personnel ?

Il s'agit de *« 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 »*[2]*. Par exemple, sont des données à caractère personnel : le nom, le prénom, l'adresse, le numéro de téléphone, l'année et le lieu de naissance, la nationalité, la profession, l'état de santé, les opinions religieuses, l'appartenance syndicale, les origines raciales…*

1 Pour aller plus loin : vous pouvez consulter le site de la CNIL : http://www.cnil.fr/vos-obligations/declarer-a-la-cnil/ ou encore, vous reportez à la Fiche FIEEC « Les obligations de déclaration à la CNIL ».
2 Article 2 de la Loi« Informatique et libertés » du 6 janvier 1978, modifiée par la loi du 6 Août 2004

Que faut-il entendre par « traitement de données » ?

Cela recouvre *« 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 »*[3].

Dispense de déclaration à la CNIL

Il existe des cas où vous n'avez pas à accomplir cette déclaration[4] :

- **Les traitements** ayant pour seul objet la tenue d'un registre qui, en vertu de dispositions législatives ou réglementaires, est **destiné exclusivement à l'information du public et est ouvert à la consultation de celui-ci ou de toute personne justifiant d'un intérêt légitime[5] ;**
- **Les fichiers associatifs**[6], à certaines conditions ;
- **En cas de désignation d'un « correspondant à la protection des données »**[7] ;
- **Les traitements dont la finalité se limite à assurer la conservation à long terme de documents d'archives**[8] ;
- **Lorsque les traitements sont mis en œuvre pour l'exercice d'activités exclusivement personnelles**[9] ;
- **En cas de copies temporaires dans le cadre d'une activité technique de transmission et de fourniture d'accès à un réseau numérique[10] ;**
- **Certains traitements courants dont la mise en œuvre n'est pas susceptible de porter atteinte à la vie privée et aux libertés[11].**

3 Article 2 de ladite loi
4 Articles 12 et 22 de la Loi
5 Article 22, II, 1° de la Loi
6 Article 22, II, 2° et article 8, II, 3° de la Loi
7 Article 22, III de la Loi
8 Article 36 de la Loi
9 Article 2 de la Loi
10 Article 4 de la Loi
11 Article 24 de la Loi

Les sanctions en cas de non-respect de l'obligation de déclaration

Outre les sanctions pénales (amende, emprisonnement), la CNIL peut prononcer :

- **un avertissement,**
- **une amende,**
- **le verrouillage des données pendant 3 mois,**
- **une injonction d'arrêter le traitement des données,**
- **un retrait de l'autorisation de la Cnil.**

L'obligation d'information

L'employeur doit recueillir l'accord des salariés avant de collecter des données à caractère personnel les concernant. De plus, l'objectif de la collecte d'informations doit être précis et les données recueillies en accord avec cette finalité.

Dès lors que l'employeur détient des données personnelles relatif à ses salariés, il doit informer la personne concernée de :

- **l'identité du responsable du fichier,**
- **la finalité du traitement des données,**
- **le caractère obligatoire ou facultatif des réponses,**
- **les droits d'accès, de rectification, d'interrogation et d'opposition,**
- **les transmissions des données.**

Ainsi, en plus d'obtenir l'accord de ses salariés et de veiller à ce que les données collectées soient bien en conformité avec la finalité du traitement, l'employeur doit informer ses salariés de leur droit d'accès, de modification et de suppression des informations collectées.

Si l'employeur ne respecte pas ces obligations, il encourt **une amende de 1 500 € par infraction et de 3 000 € en cas de récidive.**

Exemples de notes d'informations :

(Ces exemples doivent être adaptés par l'employeur)

- **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)*.

- **Mention d'information à porter sur les formulaires de collecte**

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)*.

L'obligation de sécurité et de confidentialité

L'employeur, en tant que responsable du traitement, doit mettre en œuvre les **mesures de sécurité des locaux et des systèmes d'information,** pour empêcher que les fichiers soient déformés, endommagés ou que des tiers non autorisés y aient accès.

L'**accès aux données est réservé uniquement aux personnes désignées,** habilitées en raison de leur fonction, ou à des tiers qui détiennent une autorisation spéciale et ponctuelle (service des impôts, police, inspection du travail etc.).

L'employeur a également pour obligation de fixer une **durée raisonnable de conservation des informations personnelles, en fonction de la finalité du fichier.**

S'il ne respecte pas ces obligations, il encourt **5 ans d'emprisonnement et 300 000 € d'amende.**

L'obligation d'obtenir une autorisation préalable de la CNIL pour certains fichiers

L'employeur doit solliciter une autorisation de la CNIL, pour les fichiers qui présentent des risques particuliers d'atteinte aux droits et aux libertés. Il s'agit :

- des **données enregistrées portant sur des informations sensibles** (origine, opinions politiques, religieuses, syndicales, ...), **biométriques ou génétiques,**
- **des fichiers ayant une finalité particulière** (études statistiques de l'Insee, traitements de recherche médicale, ...),
- des **transferts de données hors de l'Union européenne.**

La demande d'autorisation fait l'objet d'un **examen approfondi de la part de la CNIL,** qui a 2 mois pour se prononcer. Une fois la délibération prise, la CNIL doit la notifier dans les 8 jours au responsable de traitement.

Si l'employeur n'effectue par les déclarations auprès de la CNIL, il peut être condamné à **5 ans d'emprisonnement et 300 000 € d'amende.**

Recommandations

Il n'est pas toujours évident, pour une entreprise, de s'assurer de sa parfaite conformité aux obligations de déclarations vis-à-vis de la CNIL. Ainsi, il apparaît nécessaire de mettre en place des actions permettant d'identifier les traitements de données personnelles au sein de l'entreprise, afin d'effectuer les démarches adaptées auprès de l'administration. Il est donc conseillé de :

1. **Etablir la liste de vos traitements de données personnelles** (par exemple : accès au site web avec logs, badgeuse, paye...).
2. **Vérifiez la conformité de ces derniers aux obligations de sécurité** visant à garantir des données non déformées, non endommagées, et qui ne soient pas accessibles à des tiers non autorisés.
3. **Assurez-vous d'être à jour de vos déclarations.**
4. **Imposez-vous des délais maximum de conservation des données.** Ces délais sont précisés lors de la mise en œuvre du traitement.

2 Les opérations de recrutement

Quelles sont les données qui peuvent être collectées?

Les informations demandées au candidat lors du recrutement ont pour finalité d'apprécier la capacité de celui-ci à occuper l'emploi proposé (formations, expériences etc). Ces informations doivent, par conséquent, présenter un lien direct avec l'offre d'emploi ou avec l'évaluation des qualités et compétences professionnelles du candidat.

Des informations complémentaires pourront être collectées pour la bonne gestion administrative du personnelle (personne à contacter en cas d'urgence, permis de conduire etc.) ou l'organisation du travail (photographie de l'employé pour l'annuaire interne), par exemple.

En revanche, la **collecte des informations suivantes est considérée comme interdite,** sauf cas particuliers justifiés par la nature très spécifique du poste à pourvoir ou par une obligation légale :

- date d'entrée en France ;
- date de naturalisation ;
- modalités d'acquisition de la nationalité française ;
- nationalité d'origine ;
- numéro de sécurité sociale ;
- détail de la situation militaire : sous la forme « objecteur de conscience, ajourné, réformé, motifs d'exemption ou de réformation, arme, grade » ;
- adresse précédente ;
- entourage familial du candidat (nom, prénom, nationalité, profession et employeur du conjoint ainsi que nom, prénom, nationalité, profession, employeur, des parents, des beaux-parents, des frères et soeurs et des enfants) ;
- état de santé, taille, poids, vue ;
- conditions de logement (propriétaire ou locataire) ;

- vie associative ;
- domiciliation bancaire, emprunts souscrits, défauts de paiement ;
- origines raciales ou ethniques ;
- opinions politiques, philosophiques ou religieuses ou appartenances syndicales ;
- informations relatives à la santé ou à la vie sexuelle des personnes.

Dans tous les cas, l'accord exprès du salarié recueilli par écrit ne saurait, à lui seul, justifier la collecte de telles données si ces dernières sont dépourvues de lien direct et nécessaire avec l'emploi proposé.

Le recueil de références auprès de l'environnement professionnel du candidat (supérieurs hiérarchiques, collègues, maîtres de stages, clients, fournisseurs…) est permis dès lors que le candidat en a été préalablement informé.

Attention

Les « zones commentaires » destinées à enregistrer des informations de gestion, telles que des résumés d'entretien, doivent, comme toute donnée à caractère personnel enregistrée dans un traitement, être pertinentes, adéquates et non excessives au regard de la finalité du traitement. De plus, le salarié peut y avoir accès à tout moment.

La CNIL veille au respect de ces principes et a, par exemple, prononcé une sanction pécuniaire d'un montant de 40 000 euros à l'encontre d'une entreprise pour des commentaires particulièrement subjectifs sur des personnes ayant déjà été employées par une société mais qui n'ont pas donné satisfaction (Délibération n° 2007-374 du 11 décembre 2007).

L'accès aux données

Les informations recueillies sur les candidats ou employés sont uniquement accessibles aux personnes intervenant dans le processus de recrutement et chargées de la gestion du personnel. Les supérieurs hiérarchiques peuvent accéder aux informations nécessaires à l'exercice de leurs fonctions comme, par exemple, les données d'évaluations, de rémunération etc.

Les délégués du personnel ont accès aux données figurant dans le registre unique du personnel (nom, nationalité, fonction occupée, date d'entrée dans l'organisme, etc.).

Enfin, il est possible de donner accès à d'autres instances comme le comité d'entreprise ou les délégués syndicaux, afin de leur permettre d'exercer leurs missions.

L'information des candidats

L'employeur ne pourra mettre en place un dispositif de collecte tant que le candidat (ou l'employé) n'aura pas été préalablement informé.

Les instances représentatives du personnel doivent également être informées avant toute utilisation de fichiers de gestion du personnel, ou d'aide au recrutement.

Lors de la collecte des données, les candidats au poste proposé, comme les employés doivent être informés :

- de l'**identité du responsable du traitement** (ex : cabinet de recrutement X ; service des ressources humaines de la société Y) ;
- **des finalités du traitement** (ex : gestion des candidatures) ;
- **du caractère obligatoire ou facultatif des réponses,** (ex : le recueil d'informations sur les loisirs est facultatif) ;
- **des éventuelles conséquences à leur égard d'un défaut de réponse ;**
- **des personnes physiques ou morales destinataires des informations** (ex : autres cabinets de recrutements) ;
- **des conditions d'exercice de leur droit d'accès et de rectification ainsi que de leur droit d'opposition** (ex : indication du service auprès duquel ces droits peuvent être exercés).

Recommandations de la CNIL

- Informer, dans des délais raisonnables, les candidats au sujet du processus de recrutement, et notamment sur:
  - les suites données à sa candidature ;
  - la durée de conservation des informations le concernant ainsi que de la possibilité d'en demander la restitution ou la destruction ;
  - une éventuelle cession d'informations à d'autres organismes de recrutement et de la possibilité de s'y opposer ;
  - les méthodes et techniques d'aide au recrutement utilisées à son égard (de préférence dispensée préalablement par écrit, de manière collective ou individuelle).

A noter : les résultats obtenus doivent rester confidentiels.

- Recueillir préalablement l'accord du candidat sur la transmission de son CV à l'employeur, lorsque l'identité de celui-ci n'a pas été précisée lors de l'offre de poste.
- Informer le candidat à l'emploi, de la forme (nominative ou non), sous laquelle les informations le concernant seront éventuellement diffusées en ligne ou transmises aux employeurs, dans le cas de sites de recrutements en ligne.

Les droits des candidats

Tout candidat ou employé doit pouvoir obtenir sur demande et dans un délai raisonnable toutes les informations le concernant y compris les résultats des analyses et des tests (psychologiques, graphologiques...) ou évaluations professionnelles éventuellement pratiqués.

Le droit d'accès s'applique aux informations collectées directement auprès du candidat, aux informations éventuellement collectées auprès de tiers ainsi qu'aux informations issues des méthodes et techniques d'aide au recrutement.

Combien de temps peut-on conserver les données relatives à un candidat?

La CNIL recommande que la durée de conservation des informations (sur support informatique et papier) n'excède pas deux ans après le dernier contact avec la personne concernée, à mois d'un accord explicite et formel du candidat pour une conservation plus longue.

S'agissant des données relatives à un employé, elles seront conservées le temps de sa présence dans l'organisme.

Comment déclarer?

Doivent faire l'objet d'une déclaration à la CNIL : les outils informatiques d'aide au recrutement (déclaration normale) et ceux relatifs à la gestion du personnel (déclaration simplifiée ou déclaration normale). En cas de désignation d'un correspondant informatique et libertés, l'entreprise est dispensée de déclaration.

Exemple de notice d'information en matière de recrutement (à remettre au candidat)

…….. (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 de 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 :

Les annuaires du personnel 3

De nombreuses entreprises mettent en place un annuaire du personnel sur support informatisé comprenant des informations personnelles sur les salariés telles que : leur identité, fonction, coordonnées professionnelles et le cas échéant leur photographie.

Lorsque l'annuaire est interne, il est accessible aux seuls membres du personnel et diffusé sur intranet ou sur format papier. L'annuaire peut être externe ; il est alors accessible à d'autres personnes que le personnel de l'organisme (ex : annuaire publié sur internet).

Qu'il soit interne ou externe, l'annuaire constitue un traitement de données personnelles soumis aux dispositions de la loi du 6 janvier 1978 modifiée en 2004.

L'employeur doit donc respecter certaines obligations : information des salariés sur leurs droits, recueillir l'accord de ces derniers etc.

Dans tous les cas, les annuaires du personnel ne doivent pas être utilisés à des fins commerciales ou politiques.

La nécessité d'informer les intéressés

Préalablement à la mise en place d'un annuaire, l'employeur doit informer ses salariés de leurs droits d'accès, de rectification et d'opposition sur les données récoltées. Cette information s'effectue par la remise d'un document écrit ou par voie électronique.

Si l'employeur souhaite rendre accessible sur internet les données à caractère personnel concernant ses salariés, (ex annuaire externe avec diffusion des nom, prénom, coordonnées professionnelles, etc.) il ne pourra en maitriser leur utilisation par des tiers. Aussi, le salarié doit pouvoir s'opposer simplement et à tout moment à une telle diffusion.

Concernant la diffusion de la photographie des salariés, la CNIL recommande qu'elle soit subordonnée à l'accord préalable de l'employé, en particulier lorsque cette photographie est destinée à être publiée ou mise en ligne sur internet.

Exemple de courrier d'information pour un 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).

Comment déclarer?

Les annuaires professionnels internes doivent faire l'objet d'une déclaration de conformité en référence à la norme n° 46 relative à la gestion des personnels des organismes publics et privés, sauf si un Correspondant Informatique et Libertés (CIL) a été désigné au sein de l'organisme (dispense de déclaration).

Les annuaires autres que les annuaires internes doivent faire l'objet d'une déclaration normale préalablement à leur mise en oeuvre, sauf si un CIL a été désigné au sein de l'organisme (dispense de déclaration).

L'accès au dossier professionnel 4

Tout salarié ou ancien salarié bénéficie d'un droit d'accès à son dossier. L'intéressé qui souhaite effectuer cette demande auprès du service du personnel devra simplement justifier de son identité.

Les données accessibles

L'ensemble des données concernant le salarié peuvent lui être communiquées sur simple demande, qu'elles soient conservées sur support informatique ou dans un dossier papier.

C'est le cas notamment des données relatives :

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

Limites au droit d'accès

Certaines données ne sont, en revanche, pas accessibles au salarié ou à l'ancien salarié, quand bien même il en ferait la demande. Il s'agit :

- des données relatives à la situation personnelle d'un tiers (ex : un autre salarié) ;
- des données prévisionnelles de carrière (potentiel de carrière, classement), sauf si ces dernières ont été prises en compte pour décider de son affectation, de son augmentation de salaire, de sa promotion etc.

Un salarié peut donc accéder, sur simple demande, à l'ensemble des données de gestion des ressources humaines qui ont servi à prendre une décision qui le concerne.

L'employeur a le droit de s'opposer aux demandes manifestement abusives. Mais en cas de contestation par le salarié, il devra établir le caractère abusif de la demande du salarié.

Comment s'exerce le droit d'accès?

Le salarié ou ancien salarié peut exercer son droit d'accès en se rendant sur place ou en adressant un écrit, avec un justificatif d'identité.

L'employeur doit répondre immédiatement si la demande est effectuée sur place (et s'il est possible de rendre immédiatement accessible les éléments demandé), ou dans un délai maximal de 2 mois si la demande est écrite (ou lorsqu'un laps de temps est nécessaire pour répondre à la demande effectuée sur place).

Une copie des données est alors délivrée à l'intéressé (le simple 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.

En cas de refus de l'employeur d'y répondre favorablement, le refus doit être écrit, motivé et doit mentionner les voies et délais de recours à disposition du salarié.

Les réseaux sociaux externes

5

Un réseau social est une **plate-forme « en ligne » qui permet à des personnes ou à des organisations d'être regroupées autour de centres d'intérêts communs et d'échanger un certain nombre d'informations[12] .**

Depuis les années 2003-2004, les réseaux sociaux occupent une place croissante dans notre quotidien, qu'il s'agisse des réseaux sociaux externes ou internes. **Les réseaux sociaux externes** sont accessibles par tous (tels que Facebook, LinkedIn, Viadeo, Twitter…). Alors que les **réseaux sociaux internes** ou réseau sociaux d'entreprise ont un accès restreint (intranet ou extranet).

Identification des risques liés à l'utilisation des réseaux sociaux externes

La publication d'informations sur les réseaux sociaux peut, dans certains cas, se révéler s**ource de risques pour l'entreprise**. Ces risques existent, que le contenu soit publié par un salarié sous le contrôle ou hors du contrôle de l'entreprise. Ils peuvent, notamment, se traduire par :

- **la responsabilité de l'entreprise et de ses salariés** : Elle peut être engagée du fait, par exemple, de publications volontaires ou involontaires portant atteinte à une tierce personne ;
- **une atteinte à l'image et à la réputation** : L'entreprise peut se voir affectée par le dénigrement, la diffamation ou encore des injures à l'encontre de l'entreprise ou de ses dirigeants par des employés ;
- **la divulgation d'informations confidentielles :** Les salariés peuvent être amenés à échanger sur des situations rencontrées dans l'exercice de leur activité professionnelle. Lorsque cet échange à lieu sur des réseaux sociaux, il peut entrainer la divulgation volontaire, ou involontaire, d'informations confidentielles pour l'entreprise (secrets d'affaires, secrets de fabrique, savoir-faire…) ;

12 Guide MEDEF « Réseaux sociaux et entreprises : quels enjeux juridiques ? »

- **une atteinte à la sécurité du système d'information de l'entreprise** : L'utilisation de réseaux sociaux, et plus généralement d'internet, peut parfois conduire à l'installation de logiciels malveillants, ou à être confronté à l'ingénierie sociale (forme d'acquisition déloyale d'information qui consiste à extirper frauduleusement, par manipulation, de l'information à l'insu de son interlocuteur) ;
- **une atteinte aux droits de la propriété intellectuelle** : Il peut s'agir de la reproduction de textes protégés par le droit d'auteur, ou encore du logo d'une entreprise sans autorisation et de manière illicite ;
- **une usurpation d'identité :** Cela peut se traduire, par exemple, par la création de fausses pages ou de faux comptes sur un réseau social.

Compte tenu des enjeux juridiques liés à l'utilisation des réseaux sociaux externes, l'employeur a tout intérêt à informer et sensibiliser ses salariés sur ce sujet.

Accompagnement et sensibilisation des salariés dans l'utilisation des réseaux sociaux

Un salarié correctement informé, sensibilisé et responsabilisé sur les enjeux soulevés par l'utilisation des réseaux sociaux, participera de ce fait à la protection de l'entreprise contre la mise en cause éventuelle de sa responsabilité juridique.

Il est donc fortement conseillé de mettre en place des **mesures d'accompagnement des salariés au sein de l'entreprise** comme, par exemple :

- la signature d'une charte d'entreprise qui informe et engage moralement le salarié,
- la mise à disposition de notes ou guides de sensibilisation sur l'utilisation des réseaux sociaux, voir le contrôle ou la limitation de l'utilisation des réseaux sociaux,
- la mise en place d'une politique de communication,
- l'organisation de session d'information et/ou de formation.

L'adoption d'une charte d'entreprise relative à l'utilisation des réseaux sociaux

C'est un document qui définit les conditions et règles d'utilisation des technologies de l'information et de la communication dans l'entreprise.

Il n'est pas rare de voir déjà établie, dans une entreprise, une charte pour l'utilisation d'internet et du système d'information. La charte d'entreprise sur l'utilisation des réseaux sociaux peut y être intégrée ou faire l'objet d'un document à part entière.

- **Valeur juridique de la charte vis-à-vis du salarié**

  Les documents ou « chartes » intégrés ou annexés au règlement intérieur ont une **valeur contraignante** pour les salariés. Il en est de même pour les règles incluses directement dans le contrat de travail du salarié.

  A l'inverse, les documents ou « chartes » autonomes n'auront qu'une **valeur informative ou pédagogique.**

- **Intérêt pour l'entreprise**

  Il est important de souligner que la mise en place d'une charte **nécessitera la conduite collective de travaux au sein de l'entreprise** en vue de sa rédaction, son adoption, et ses éventuelles modifications à venir. Elle constitue à ce titre un outil intéressant pour mobiliser et impliquer les salariés dans le cadre de ces réflexions.

Son contenu permettra d'informer l'ensemble des salariés sur, notamment :

- les risques liés à l'utilisation des réseaux sociaux,
- la politique de communication de l'entreprise sur les réseaux sociaux,
- les éventuels moyens mis en place pour contrôler l'utilisation par les salariés des réseaux sociaux, via les moyens informatiques fournis par l'entreprise.

Aucun texte légal ou réglementaire n'impose aux entreprises la mise en place de telles mesures. Ces chartes ne sont pas **obligatoires pour l'entreprise,** mais sont néanmoins recommandées.

Si elles ne peuvent pas empêcher la publication de contenus sur les réseaux sociaux par les salariés qui restent libres de les utiliser à partir de leurs équipements personnels et/ou hors de leur temps de travail, elles constituent toutefois un **instrument efficace de sécurisation de l'entreprise, de prévention, de sensibilisation et de responsabilisation des salariés.**

Le contrôle ou la limitation de l'utilisation des réseaux sociaux

De manière générale, l'utilisation des outils informatiques à des fins personnelles par le salarié est tolérée dans la mesure où elle demeure raisonnable et n'affecte pas le bon fonctionnement de l'entreprise. L'employeur pourra néanmoins décider, en vertu de son pouvoir de direction, de **filtrer ou non certains sites internet** (tels que les réseaux sociaux).

Lorsque l'employeur décide limiter l'utilisation des réseaux sociaux par les salariés et/ou d'en contrôler l'activité, un certain nombre de règles doivent être respectées :

- les instances représentatives du personnelles devront être informées et consultées préalablement à la décision de mise en œuvre, dans l'entreprise, de dispositifs permettant un contrôle de l'activité des salariés (article L. 2323-32 du Code du travail) ;
- les salariés devront également être informés de l'existence, des modalités, de la finalité du dispositif de contrôle, de la durée de conservation ou de sauvegarde des données de connexion et des conséquences éventuelles (article L. 1222-4 du Code du travail et la loi relative aux fichiers, à l'informatique et aux libertés du 6 janvier 1978 modifiée) ;
- les mesures de limitation ou de contrôle devront être proportionnées au but recherché du point de vue des droits des personnes et des libertés individuelles (article L. 1121-1 du Code du travail) ;
- les formalités préalables nécessaires devront être réalisées, au titre de la loi du 6 janvier 1978 modifiée relative aux fichiers, à l'informatique et aux libertés.

A noter : les personnes exerçant une fonction de contrôle (inspection, audit, conformité, etc.) peuvent exploiter des données concernant un salarié, récoltées sur les réseaux sociaux professionnels, sous réserve de respecter les règles suivantes :

- demeurer dans le cadre de leurs missions de contrôle et dans les limites posées par les conditions de ce contrôle : proportionnalité, transparence, respect des formalités préalables éventuelles (CNIL, etc.),
- exploiter des données directement liées à l'activité professionnelle du salarié ou qui créent, au minimum, un trouble caractérisé au sein de l'entreprise,
- récolter des données rendues accessibles à un large public ou au minimum à un cercle plus élargi que des individus reliés par une communauté d'intérêts,
- rapporter la preuve de l'imputabilité du salarié dans l'hypothèse où des propos ou des actes lui seraient reprochés.

La mise en place d'une politique de publication

Il est dans l'intérêt de l'entreprise d'**encadrer précisément les publications de contenus effectuées par les salariés au nom et pour le compte de celle-ci**. Ainsi, l'élaboration de règles précises, établies en association avec les salariés de l'entreprise, contribue à sensibiliser ces derniers.

Ces règles peuvent, notamment, viser à :

- informer les salariés sur la réglementation applicable en matière de publication de contenus (droit à l'image, droit d'auteur…) et la responsabilité encourue tant par le salarié que par l'entreprise,
- identifier les réseaux sociaux sur lesquels l'entreprise souhaite être présente,
- s'assurer du respect des conditions d'utilisation des réseaux sociaux sur lesquels l'entreprise a décidé de créer un compte/une page,
- définir et mettre en place une ligne éditoriale ou réfléchir à une politique de publication.

Les voies d'actions en cas de publication d'un contenu litigieux par un salarié sur un réseau social

Les salariés jouissent dans l'entreprise de leur **liberté d'expression**. Elle permet aux salariés de **tenir des propos sur l'organisation et le fonctionnement de l'entreprise**. Toutefois, cette liberté d'expression connait des limites en cas d'abus, notamment si les termes utilisés sont injurieux, diffamatoires ou excessifs, ou que les informations divulguées étaient confidentielles.

De manière générale, un salarié ne peut pas être sanctionné en raison de faits relevant de sa vie personnelle. Il en est autrement si son comportement entraine un trouble caractérisé pour l'entreprise. En effet, des sanctions disciplinaires peuvent être prises à l'encontre du salarié dans le cas où un fait relevant de sa vie personnelle se rattache à sa vie professionnelle et porte atteinte à l'entreprise, ou entraine un manquement à une obligation contractuelle.

Ce sont les juges du fond qui apprécient souverainement le caractère privé ou public des réseaux sociaux selon les situations rencontrées.

- **La preuve de la publication litigieuse**

  En cas de contenu litigieux publié sur un réseau social concernant l'entreprise, il est essentiel, dans un premier temps, de rapporter la preuve de cette publication par tout moyen loyal.

- **Les moyens d'action de l'entreprise**

  Il sera toujours possible, pour l'entreprise visée par une publication litigieuse, d'exercer un **droit de réponse** prévu par la **loi pour la confiance dans l'économie numérique** (LCEN) du 21 Juin 2004, directement sur le réseau social ou par courrier recommandé avec accusé de réception au directeur de la publication du site concerné.

  Ce dernier devra communiquer sa réponse sur les suites données à la publication litigieuse dans un délai de 3 jours à compter de la réception.

L'entreprise peut également **demander la suppression du contenu à l'auteur du contenu ou à la plate-forme du réseau social.** Certains réseaux sociaux ont mis en place une procédure de signalement permettant de dénoncer un contenu qui serait en violation avec le règlement ou les conditions du réseau. La LCEN prévoit, en outre, une procédure de notification à l'hébergeur de contenus « manifestement illicites »[13] par leur nature et de tout autre contenu illégal.

Si l'entreprise décide d'intenter une **action judiciaire**, il lui faudra déterminer les fondements juridiques applicables en fonction du contenu publié.

A titre d'exemples :

- violation des conditions d'utilisation du réseau social concerné (article 1147 du Code civil),
- dénigrement des produits ou des services (article 1382 du Code civil),
- usurpation d'identité (article 226-4-1 du Code pénal),
- atteinte à la vie privée/atteinte au droit à l'image/atteinte au droit au nom (article 9 du Code civil),
- …

13 Article 6-I-7 alinéa 3 de la LCEN

Recommandations

Pour limiter les risques potentiels liés à l'utilisation des réseaux sociaux, il apparait nécessaire de mettre en place une organisation interne spécifique, ainsi que des mesures préventives, telles que :

- identifier les **enjeux généraux et spécifiques pour l'entreprise concernant l'utilisation des réseaux sociaux,**
- assurer une **veille régulière des contenus publiés sur les réseaux sociaux relatifs à l'entreprise,**
- définir et mettre en place une **politique de sensibilisation, d'information et d'accompagnement des salariés dans l'utilisation des réseaux sociaux,**
- encadrer les usages en mettant en place **un document définissant précisément les droits et les devoirs des salariés,** ainsi que la **politique de communication de l'entreprise sur les réseaux sociaux.**

Pour aller plus loin, vous pouvez consulter le **site de la CNIL** : www.cnil.fr et prendre connaissance du document **Questions/Réponses publié par le MEDEF** sur les « **Réseaux sociaux et entreprises : quels enjeux juridiques ?** ».

6 Les réseaux sociaux d'entreprises

En parallèle des réseaux sociaux externes connus (Facebook, Twitter, Linkedin, Viadéo…) et parfois accessible par les salariés sur leur lieu de travail, l'entreprise peut choisir de mettre en place un réseau social interne dont l'accès est limité aux seuls salariés de l'entreprise.

La mise en place d'un réseau social d'entreprise (RSE) présente plusieurs avantages en termes de performance, d'innovation et en matière de ressources humaines.

En effet, l'utilisation d'un tel réseau par les salariés contribue à décloisonner les échanges et faciliter le travail transversal. Elle permet de réduire les flux d'e-mails et le temps de réunion en rendant plus fluide la communication et le partage d'information.

En termes d'innovation, elle semble faciliter le développement des initiatives. Enfin, sur le plan humain, elle favorise le partage de compétence interservices et contribue à améliorer le bien-être au travail.

Néanmoins, certaines précautions devront être prises par l'employeur pour, notamment :

- sensibiliser les utilisateurs sur les règles à respecter,
- les informer des moyens de contrôles associés à cet outil.

L'encadrement de l'utilisation des réseaux sociaux internes

Afin d'**éviter que des informations confidentielles ou particulièrement protégées soient accessibles à un public plus large** que celui prévu, un certain nombre d'actions peuvent être menées en amont ou lors de la mise en place d'un RSE :

- **Elaboration d'un règlement intérieur et d'une charte d'utilisation des technologies de communication.**

  Il apparaît essentiel de **revoir le règlement intérieur**, notamment le paragraphe et/ou l'annexe traitant de l'utilisation des moyens informatiques

de l'entreprise, afin de le rafraîchir, de le compléter ou de l'adapter à l'utilisation des nouveaux moyens de diffusion et d'échange de l'information.

Il est également nécessaire de **rediffuser ce règlement intérieur, accompagné éventuellement d'une brochure ou d'une charte**, pour rappeler aux utilisateurs leurs droits et leurs devoirs, notamment en matière de discrétion, de sécurité des informations et de respect du droit des personnes et de la vie privée.

- **Conditions générales d'utilisation et guide d'utilisation**

  Les conditions générales d'utilisation (CGU) doivent comporter :

  - les règles générales du bon usage du réseau social d'entreprise ;
  - l'organisation permettant de faire respecter ces règles générales ;
  - les restrictions qu'un utilisateur se verra appliquer en cas de non-respect de ces règles générales ;
  - les règles s'appliquant à la publication des informations en fonction de leur degré de confidentialité ;
  - les licences d'utilisation s'appliquant à la publication des contenus sur le réseau social d'entreprise ;
  - les informations relatives à la collecte des éléments d'authentification et relatives aux contenus publiés.

La diffusion d'un guide d'utilisation rappelant de manière simple les CGU est un bon moyen d'inciter les utilisateurs à en prendre connaissance et à se les approprier.

Le contrôle et l'exploitation des informations présentes sur les réseaux sociaux internes par l'entreprise

Les collaborateurs exerçant une fonction de contrôle (inspection, audit, conformité, etc.) peuvent, de façon beaucoup plus large que pour les réseaux externes, exploiter des données concernant le salarié, récoltées sur les réseaux sociaux internes.

Cependant, **ils devront demeurer dans le cadre de leurs missions de contrôle et dans les limites posées par les conditions de ce contrôle** (respect du principe de proportionnalité, de transparence et des formalités préalables éventuelles).

Ainsi, l'entreprise devra veiller au respect des règles suivantes :

- avoir préalablement informé les salariés et les instances représentatives du personnel de l'existence, des modalités, de la finalité des contrôles effectués et des conséquences éventuelles pouvant en résulter pour l'utilisateur ;

- exercer un contrôle proportionné au but recherché, de l'activité des salariés par le réseau social au regard de l'éventuelle atteinte à la vie privée du salarié ou à ses droits ;
- s'assurer que l'ensemble des formalités juridiques encadrant le réseau social d'entreprise a bien été réalisé, c'est à dire :
  - le respect des formalités concernant le traitement des données à caractère personnel,
  - le respect des formalités prévues dans le Code de travail concernant le contrôle de l'activité du salarié doivent être respectées (consultation des instances représentatives du personnel,...).

Le cas d'un réseau social d'entreprise constituant un traitement de données à caractère personnel

Si le **réseau social d'entreprise collecte et traite des données permettant d'identifier directement** (nom, prénom, profil, photographie, CV…) ou **indirectement des personnes** (n° d'identifiant personnel…), il constitue un traitement de données à caractère personnel, selon la loi « Informatique et Libertés ».

A ce titre, il devra respecter certains principes et faire l'objet de formalités déclaratives préalables à sa mise en œuvre. Les manquements aux principes de la loi Informatique et Libertés peuvent faire l'objet de sanctions (sanctions pénales, administratives, financières de la part de la CNIL, ...).

Les principes à respecter

- **Principe de finalité** : le RSE devra avoir une finalité bien déterminée ;
- **Principe de proportionnalité** : seules les informations pertinentes et en lien avec la finalité et les objectifs du RSE pourront être collectées ;
- **Principe d'une durée limitée de conservation des informations** : les informations doivent être effacées au-delà d'une certaine durée ;
- **Principe de sécurité et de confidentialité** : le responsable de traitement doit prendre toutes précautions utiles pour préserver la sécurité et la confidentialité des données et notamment empêcher qu'elles ne soient déformées, endommagées ou que des tiers non autorisés n'y aient accès ;

- **Principe de transparence à l'égard des personnes concernées :** toute personne concernée par le traitement de ses données doit être informée des finalités du RSE, des destinataires des informations et des modalités d'exercice de ses droits d'accès, de rectification et d'opposition.
- **Principe de droit d'accès, de rectification et d'opposition :** toute personne doit disposer d'un droit d'accès, de rectification et d'opposition aux données le concernant.

Les formalités déclaratives

Elles varient en fonction de la finalité et du périmètre du réseau social d'entreprise :

- soit une **déclaration ordinaire à la CNIL,**
- soit une **inscription au registre du Correspondant Informatique et Libertés** pour les organismes qui en sont dotés,
- soit une **demande d'autorisation à la CNIL**. Il s'agit des cas où le RSE est accessible à des utilisateurs ou destinataires situés hors de l'Union Européenne ou encore s'il comporte des informations sensibles (telles que les informations concernant l'origine raciale ou ethnique, les opinions politiques, philosophiques ou religieuses, l'appartenance syndicale, la santé...).

7 Le contrôle de l'utilisation d'internet et de la messagerie

La plupart du temps, l'employeur met à disposition du salarié un poste de travail informatique doté d'une messagerie électronique et d'un accès à internet, pour le bon exercice de son activité professionnelle. Si l'utilisation de ces outils informatiques 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 de l'entreprise ou de l'administration concernée.

Le contrôle de l'utilisation d'internet

L'employeur peut déterminer les conditions et limites de l'utilisation d'internet par ses salariés, en mettant en place, par exemple :

- des dispositifs de filtrage de sites non autorisés (sites à caractère pornographique, pédophile, d'incitation à la haine raciale, révisionniste, etc.),
- des limites dictées par l'exigence de sécurité de l'organisme, telles que l'interdiction de télécharger des logiciels, l'interdiction de se connecter à un forum ou d'utiliser le « chat », l'interdiction d'accéder à une boîte aux lettres personnelle par internet compte tenu des risques de virus qu'un tel accès est susceptible de présenter, etc.

Ces mesures ne constituent pas, en soi, des atteintes à la vie privée des salariés.

En revanche, les « *keyloggers* », qui permettent d'enregistrer à distance toutes les actions accomplies sur un ordinateur, constituent un mode de surveillance illicite, sauf circonstance exceptionnelle liée à un fort impératif de sécurité.

A noter : les logs de connexion ne doivent pas être conservés plus de 6 mois.

Comment déclarer?

- **Déclaration normale**
  L'entreprise ou l'administration qui met en place un **dispositif de contrôle individuel des salariés (relevé des connexions ou des sites visités), poste par poste,** doit déclarer le traitement à la CNIL (déclaration normale).

  C'est le cas, par exemple, d'un logiciel de contrôle de l'utilisation d'internet permettant d'analyser les données de connexion de chaque salarié ou de calculer le temps passé sur internet par un salarié déterminé.

  Toutefois, si un Correspondant Informatique et Libertés (CIL) a été désigné, aucune déclaration n'est nécessaire.

- **Déclaration simplifiée**

  Lorsque l'entreprise ou l'administration met en place un dispositif qui ne permet pas de contrôler individuellement l'activité des salariés, le traitement mis en oeuvre peut faire l'objet d'une déclaration de conformité en référence à la norme simplifiée n° 46 (gestion des personnels des organismes publics et privés).

  Par exemple : logiciel permettant seulement de réaliser des statistiques sur l'utilisation d'internet au niveau de l'ensemble des salariés de l'entreprise ou au niveau d'un service déterminé.

Le contrôle de l'utilisation de la messagerie

Les entreprises ou les administrations peuvent choisir de mettre en place des outils de contrôle de la messagerie pour répondre à des exigences de sécurité, de prévention ou de contrôle de l'encombrement du réseau. C'est le cas, par exemple, des outils de mesure de la fréquence, de la taille des messages électroniques, ou encore des outils d'analyse des pièces jointes (détection des virus, filtres « anti-spam » destinés à réduire les messages non-sollicités, etc.).

Comment déclarer?

- **Déclaration normale**
  Si un **dispositif de contrôle individuel de la messagerie** est mis en place, il doit être déclaré à la CNIL sauf désignation d'un CIL.

Par exemple : logiciel d'analyse du contenu des messages électroniques entrant ou sortants destinés au contrôle de l'activité des salariés.

- **Déclaration simplifiée**
  La messagerie professionnelle doit faire l'objet d'une **déclaration de conformité en référence à la norme n° 46** (gestion des personnels des organismes publics et privés).

Les conditions d'accès aux messages électroniques d'un salarié

L'employeur peut accéder librement aux courriels qui sont présumés être professionnels, c'est-à-dire ceux qui n'ont pas été identifiés comme étant « personnels » ou « privés ».

En effet, la Cour de cassation considère qu'un message envoyé ou reçu depuis le poste de travail mis à disposition par l'employeur est **présumé avoir un caractère professionnel, sauf s'il est identifié comme étant « personnel »**, dans l'objet du message par exemple (Cour de cassation, 30 mai 2007).

Il appartient à l'employé d'identifier les messages qui sont personnels. À défaut d'une telle identification, les messages sont présumés être professionnels.

La nature personnelle/privée d'un message peut figurer dans l'objet du message ou dans le nom du répertoire dans lequel il est stocké.

Le respect du secret des correspondances privées par l'employeur

- **Principe**
  Une communication électronique émise ou reçue par un employé peut donc, compte tenu de ce qui précède, avoir le caractère d'une correspondance privée. La violation du secret des correspondances est une infraction pénalement sanctionnée par les articles 226-15 et 432-9 du Code pénal.

  La Cour de cassation a affirmé, dans un arrêt du 2 octobre 2001 (arrêt « Nikon »), qu'un employeur ne saurait prendre connaissance de messages personnels d'un employé sans porter atteinte à la vie privée de celui-ci (article 9 du code civil) et au principe du secret des correspondances, quand bien même une utilisation à des fins privées aurait été proscrite par l'employeur.

- **Limites**

  Pour autant, le principe du secret des correspondances connaît des limites dans la sphère professionnelle. Il peut être levé dans le cadre d'une instruction pénale ou par une décision de justice.

  C'est le cas, par exemple, d'une ordonnance délivrée par un juge désignant un huissier pour accéder aux messages (Cour de cassation, chambre sociale, arrêt du 10 juin 2008).

  Par ailleurs, un employé ne doit pas transformer des messages de nature professionnelle en correspondance « privée » à des fins illégales. Par exemple, un employé ne doit pas communiquer des documents confidentiels à un concurrent en identifiant ses messages comme étant « personnels ».

  Une telle identification serait contraire au principe de bonne foi prévu à l'article L1222-1 du Code du travail.

  La Cour de cassation a ainsi admis, après avoir constaté que l'employeur avait des motifs légitimes de suspecter des actes de concurrence déloyale, qu'un employeur puisse être autorisé par le juge à mandater un huissier de justice pour prendre connaissance et enregistrer des messages électroniques échangés entre le salarié et deux personnes étrangères à l'entreprise (Cour de cassation, 23 mai 2007).

L'accès aux dossiers contenus dans le poste informatique

Le cas des fichiers et des répertoires créés par un employé

Il a été jugé que les fichiers créés par un salarié grâce à l'outil informatique mis à sa disposition pour l'exécution de son travail sont présumés, sauf si le salarié les identifie comme étant personnels, avoir un caractère professionnel (Cour de cassation, 18 octobre 2006).

Tout fichier qui n'est pas identifié comme « personnel » est réputé être professionnel de sorte que l'employeur peut y accéder hors la présence du salarié. Par ailleurs, il a été précisé que l'identification d'un dossier par les initiales du salarié ne permet pas de le considérer comme étant personnel (Cour de cassation, 21 octobre 2009).

En revanche, 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.

Par exemple : il a été jugé que la découverte de photos érotiques dans le tiroir d'un salarié ne constituait pas un risque ou un événement particulier justifiant que l'employeur accède au répertoire intitulé « perso » hors la présence du salarié ou sans que celui-ci en soit informé (Cour de cassation, chambre sociale, arrêt du 17 mai 2005).

L'employé est-il tenu de communiquer ses mots de passe?

Les mots de passe constituent des mesures de sécurité visant à protéger les données figurant dans les postes informatiques par les salariés. Ils doivent être fréquemment modifiés et ne peuvent être portés à la connaissance de tiers que dans certaines conditions bien particulières.

Ainsi, si un employé est absent, l'employeur peut lui demander de communiquer son mot de passe lorsque les informations détenues par cet employé sont nécessaires à la poursuite de l'activité de l'entreprise (Cour de cassation, 18 mars 2003). L'employeur ne doit pas accéder au contenu personnel de l'intéressé.

Comment organiser la fermeture du compte utilisateur lors du départ de l'employé?

Les modalités de fermeture du compte sont à prévoir dans la charte informatique. Il est recommandé à l'employeur d'avertir le salarié de la date de fermeture de son compte afin que ce dernier puisse vider son espace privé.

Que faire en cas de difficulté?

En cas de contestation, il appartient aux juridictions compétentes d'apprécier la régularité et la proportionnalité de l'accès par l'employeur au poste informatique ou à la messagerie de l'employé.

L'indispensable information des salariés

L'employeur est tenu d'informer ses salariés des dispositifs mis en place et des modalités de contrôle de leur utilisation d'internet, de leur messagerie et de leurs dossiers enregistrés sur les serveurs.

Qui informer et quelles informations communiquer ?

L'employeur doit informer :

- ses salariés, individuellement, notamment de la finalité du dispositif de contrôle et de la durée pendant laquelle les données de connexion sont conservées ou sauvegardées ;
- le comité d'entreprise (ou, dans la fonction publique, le comité technique paritaire ou toute instance équivalente), qui doit également avoir été consulté (article L2323-32 du code du travail).

En cas d'archivage automatique des messages électroniques, les salariés doivent en outre être informés des modalités de l'archivage, de la durée de conservation des messages, et des modalités d'exercice de leur droit d'accès.

Une durée de conservation de l'ordre de six mois est suffisante, dans la plupart des cas, pour dissuader tout usage abusif d'internet.

Si des procédures disciplinaires sont susceptibles d'être engagées sur la base de ces fichiers, les salariés doivent en être explicitement informés.

Recommandations

- Portez à la connaissance des salariés le principe retenu pour différencier les e-mails professionnels des e-mails personnels (qualification par l'objet, création d'un répertoire spécifique dédié au contenu privé, etc.) ;
- Définissez préalablement, en concertation, les modalités d'accès de l'employeur aux données stockées sur l'environnement informatique d'un employé absent, et diffusez celles-ci auprès de l'ensemble des salariés susceptibles d'être concernés ;
- L'élaboration et la signature d'une charte peut utilement sensibiliser les salariés aux règles applicables en matière d'utilisation d'internet et de la messagerie au travail.

8 Les administrateurs réseaux

Les administrateurs réseaux sont chargés de la gestion des comptes et des machines du réseau informatique d'une organisation. Ils peuvent être également administrateurs système lorsqu'ils s'occupent des postes de travail et serveurs de l'entreprise.

Dans le cadre de leurs fonctions, les administrateurs sont amenés à avoir accès à des informations personnelles relatives aux utilisateurs (messagerie, historique des sites visités, fichiers « logs » ou de journalisation, etc.) y compris celles qui sont enregistrées sur le disque dur du poste de travail (fichiers temporaires, cookies…).

Accès aux données personnelles des utilisateurs

Les données enregistrées par les employés dans leur environnement informatique peuvent parfois être de nature personnelle. L'accès à ces données (personnelles ou non) ne peut être justifié que dans les cas où le bon fonctionnement des systèmes informatiques ne pourrait être assuré par d'autres moyens moins intrusifs.

Par ailleurs, les administrateurs de réseaux et systèmes sont soumis à une **obligation de confidentialité**, et ne doivent donc pas divulguer les informations qu'ils auraient été amenés à connaître dans le cadre de leurs fonctions. Cette obligation prend tout son sens pour les informations couvertes par le secret des correspondances ou qui relèvent de la vie privée des utilisateurs, et qui ne mettent pas en cause le bon fonctionnement technique des applications, ni leur sécurité, ni l'intérêt de l'entreprise. Enfin, sauf disposition législative particulière en ce sens, les administrateurs réseaux ou systèmes ne peuvent être contraints de divulguer ces informations.

L'obligation de confidentialité pesant sur les administrateurs informatiques doit ainsi être clairement rappelée dans leur contrat, ainsi que dans la charte d'utilisation des outils informatiques annexée au règlement intérieur de l'entreprise ou de l'administration.

L'utilisation des logiciels d'intervention à distance

Ces logiciels peuvent notamment permettre aux gestionnaires techniques d'accéder à distance à l'ensemble des données de n'importe quel poste de travail, en prenant le contrôle de l'ordinateur à distance, à des fins de maintenance informatique.

La CNIL a déjà pu constater que ces outils de télémaintenance ou de prise de main à distance sont également utilisés à des fins de contrôle, par l'employeur, de l'activité de ses employés sur leur poste informatique.

/! Une telle utilisation n'est ni conforme au principe de proportionnalité, ni respectueuse du principe de finalité posé par la loi « informatique et libertés ».

Dans l'hypothèse d'un recours à ces outils à des fins de maintenance informatique par un administrateur technique, leur utilisation doit s'entourer de précautions afin de garantir la transparence dans leur emploi et la confidentialité des données auxquelles le gestionnaire technique accédera par ce moyen, dans la stricte limite de ses besoins.

Les précautions à prendre sont les suivantes :

- **l'information préalable et le recueil de l'accord de l'utilisateur pour « donner la main » à l'administrateur informatique** avant l'intervention sur son poste (à titre d'illustration, l'accord peut être donné par simple validation d'un message d'information apparaissant sur son écran) ;
- **la traçabilité des opérations de maintenance** (par exemple, par la tenue d'un registre des interventions), ainsi que la précision dans les contrats des personnes assurant la maintenance - notamment en cas de recours à des prestataires extérieurs - de leur obligation de n'accéder qu'aux données informatiques nécessaires à l'accomplissement de leurs missions et d'en assurer la confidentialité.

A noter : l'utilisation de ces logiciels à des fins strictes de maintenance informatique n'est pas soumise à déclaration auprès de la CNIL.

9 La vidéosurveillance sur les lieux de travail

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).

Une fois cette analyse réalisée, l'employeur peut prendre la décision d'installer sur le lieu de travail des caméras pour plusieurs raisons : assurer la sécurité des biens et des personnes, dissuader ou identifier les auteurs des vols, de dégradations ou d'agressions.

Toutefois, le respect d'un certain nombre de règles est essentiel pour garantir une installation légale du dispositif de vidéo surveillance.

Les formalités à accomplir

Deux régimes juridiques sont applicables selon que les caméras sont installées dans un lieu public ou ouvert au public, ou dans un lieu privé.

Lieu public ou ouvert au public

Il s'agit de tout lieu du secteur public ou du secteur privé accessible au public. *Exemple : le guichet d'une mairie, rayons d'une grande surface, espace d'entrée et de sortie du public d'un centre d'affaires etc…*

Une autorisation préfectorale est nécessaire. Un formulaire, qui peut être retiré auprès des services de préfecture du département ou téléchargé sur le site du ministère de l'intérieur, doit donc être adressé au préfet du département avant toute installation du dispositif de vidéo surveillance. Le formulaire peut également être directement rempli en ligne, et est accessible à l'adresse suivante : www.televideoprotection.interieur.gouv.fr/gup/PhpVideo/TeleDeclaration/cnxAccueil.php

Lieu privé (lieu non ouvert au public)

Il s'agit de tout lieu du secteur public ou du secteur privé non accessible au public. *Exemple : la chaîne de montage d'une entreprise automobile, le parking réservé au personnel d'une entreprise, un lieu de stockage, ou des bureaux fermés au public etc.*

Une déclaration auprès de la CNIL est nécessaire. Par principe, chaque site ou établissement équipé doit faire l'objet d'une déclaration auprès de la CNIL. En effet, un système qui n'aurait pas fait l'objet d'une telle déclaration ne peut être opposé aux employés.

Toutefois, si l'organisme qui a mis en place des caméras a désigné un Correspondant Informatique et Liberté (CIL), ce dernier note simplement le dispositif dans son registre et aucune déclaration n'est nécessaire.

Par ailleurs, si le système de vidéosurveillance s'accompagne d'un dispositif biométrique (exemple reconnaissance faciale, analyse comportementale…, il doit faire l'objet d'une demande d'autorisation auprès de la CNIL (*Cf.* Fiche 12 du présent guide).

L'obligation d'information

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.

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

Exemple :

Etablissement sous surveillance *(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.

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 être précisément informées des fonctionnalités envisagées[14].

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. En effet, sur le lieu de travail comme ailleurs, les employés ont droit au respect de leur vie privée.

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.

Par exemple, les caméras peuvent :

- être installées au niveau des entrées et sorties des bâtiments, des issues de secours et des voies de circulation… ;
- filmer les zones où de la marchandise ou des biens de valeur sont entreposés.

Mais elles ne doivent, notamment, pas filmer :

- les employés sur leur poste de travail, sauf circonstances particulières (employé manipulant de l'argent par exemple, mais la caméra doit davantage filmer la caisse que le caissier ; entrepôt stockant des biens de valeurs au sein duquel travaillent des manutentionnaires) ;
- les zones de pause ou de repos des employés. Si des dégradations sont commises sur les distributeurs alimentaires par exemple, les caméras ne doivent filmer que les distributeurs et pas toute la pièce ;
- les locaux syndicaux ou des représentants du personnel, ni leur accès lorsqu'il ne mène qu'à ces seuls locaux.

14 (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)

Visualisation et conservation des images

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.

Les images ne devraient pas être conservées plus de quelques jours et, en tout état de cause, ne peuvent être conservées au-delà d'**un mois.**

En cas d'incident, la visualisation des images s'effectue généralement rapidement, et permet d'enclencher les procédures disciplinaires ou pénales appropriées. Le cas échéant, les images sont extraites et conservées pour la durée de la procédure.

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.

Contrôle et sanctions de la CNIL

La formation contentieuse de la CNIL a prononcé, entre 2013 et 2015, des sanctions d'un montant allant de 5000 à 10 000 euros à l'encontre de sociétés ne respectant pas les obligations d'information, la durée de conservation des données ou encore la proportionnalité du dispositif mis en place par rapport aux finalités recherchées.

A titre d'exemple, une société a fait installer trois caméras dans ses locaux afin de lutter contre le vol et les intrusions sans déclaration préalable à la CNIL, ni information suffisante auprès de ses salariés. Sur ce dernier point, la CNIL a rappelé que la mention « local placé sous vidéosurveillance » ne peut être regardée comme assurant une information suffisante des salariés quant à l'existence du traitement mis en œuvre, et des droits relatif à ce traitement.

10 La gestion de la téléphonie

L'écoute et l'enregistrement des conversations téléphoniques sur le lieu de travail

Par principe, l'écoute ou l'enregistrement des conversations du personnel d'une entreprise ou d'une administration ne peut être mis en œuvre de manière permanente, sauf législation ou réglementation particulière l'imposant.

Ces actions peuvent, par ailleurs, être réalisées en cas de **nécessité reconnue**. Il est donc possible de mettre en place l'écoute en temps réel et/ou l'enregistrement des appels sur le lieu de travail dans le cadre, par exemple, de :

- la formation de ses salariés,
- l'évaluation des salariés,
- l'amélioration de la qualité du service.

Les documents d'analyse rédigés sur la base des écoutes et enregistrement sont autorisés dès lors qu'ils s'inscrivent dans les objectifs précités.

Par ailleurs, l'écoute et l'enregistrement doivent être **proportionnés aux objectifs poursuivis**. *Par exemple, un enregistrement pour des besoins de formation ne pourra être réalisé que sur une brève période et en aucun cas de manière permanente.*

Ainsi, la collecte et le traitement de données dans ce cadre doit strictement répondre au but poursuivi.

Quelles garanties pour les salariés?

Information des salariés

Outre la consultation des instances représentatives du personnel, les salariés ainsi que leurs interlocuteurs, doivent être informés, préalablement à la mise en place du dispositif :

- des objectifs poursuivis par l'installation de ce système ;
- des conséquences individuelles qui pourront en résulter ;

- des destinataires des enregistrements ;
- des modalités d'exercice de leur droit d'accès.

Dans le cadre d'enregistrements ou d'écoutes à des fins de formation ou d'évaluation, les salariés doivent être informés des périodes pendant lesquelles leurs conversations sont susceptibles d'être enregistrées ou écoutées.

Par ailleurs, si des procédures disciplinaires sont susceptibles d'être engagées sur la base des enregistrements ou des comptes rendus, les salariés doivent en être explicitement informés.

L'information des interlocuteurs peut notamment être réalisée par la diffusion d'un message au début de l'appel, ou par l'insertion d'une mention particulière dans le document contractuel ou d'information relative au service téléphonique

Exemple : Information par message téléphonique

(enregistrement téléphonique)

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

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

En cas d'enregistrements des conversations, ceux-ci sont conservés pour une durée de (préciser la durée). Seules les personnes habilitées du service …… *(préciser le service – par exemple le service clientèle)* *auront accès à ces enregistrements.*

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

/! ces principes valent également en cas d'écoute des conversations téléphoniques sans enregistrement.

Enregistrements et vie privée

En cas d'enregistrement des communications téléphoniques, il convient que les employés disposent 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 (par exemple : possibilité d'utiliser une touche particulière avant de composer un numéro de téléphone pour neutraliser la fonction d'enregistrement). Ces fonctionnalités doivent être également offertes aux salariés protégés (représentants du personnel ou syndicaux) pour l'exercice de leur mandat.

Combien de temps l'employeur peut-il garder les enregistrements?

Lorsque les enregistrements sont réalisés à des fins de formation du personnel, la CNIL recommande une durée de conservation maximale de **6 mois.**

Lorsque les enregistrements sont réalisés à des fins de preuve en matière bancaire, la durée de conservation doit être conforme aux articles 313-51 et 313-52 du Règlement Général de l'Autorité des Marchés Financiers (cinq ans maximum).

En matière d'écoutes téléphoniques, la CNIL recommande que les comptes rendus des conversations téléphoniques et grilles d'analyse soient conservés pour une durée d'un an maximum.

Comment déclarer?

L'écoute ou l'enregistrement des conversations téléphoniques doit faire l'objet d'une déclaration auprès de la CNIL :

- déclaration simplifiée de conformité à la norme simplifiée n°57 ;
- déclaration normale si le dispositif n'est pas conforme à la norme précitée.

En cas de désignation d'un Correspondant Informatique et Libertés (CIL), aucune déclaration n'est nécessaire.

Lorsque l'enregistrement des conversations téléphoniques implique la collecte de données sensibles (ex : données de santé) liée aux missions de l'organisme, celui-ci doit effectuer une demande d'autorisation ou d'avis auprès de la CNIL.

L'utilisation du téléphone au travail

La possibilité d'un usage personnel du téléphone est tolérée à condition qu'une telle utilisation demeure raisonnable et ne soit pas préjudiciable à l'employeur. Il est ainsi légitime qu'un employeur s'assure du caractère non abusif de cette utilisation. Ce contrôle doit toutefois s'opérer dans des conditions propres à garantir le respect de la vie privée et des libertés des personnels sur leur lieu de travail.

La mise en place des autocommutateurs

Les autocommutateurs sont des standards téléphoniques permettant d'orienter l'ensemble des numéros de téléphone appelants et des numéros appelés. Ces appareils permettent même l'enregistrement des numéros de téléphone sortants, de sorte que ces dispositifs sont susceptibles d'être utilisés afin d'identifier les communications téléphoniques qui relèveraient d'un usage non professionnel.

Ils peuvent également servir à la comptabilisation statistique des flux entrants et sortants au niveau de l'organisation, d'un service ou d'un poste particulier. Reliés à des logiciels « de taxation », ils peuvent permettre d'imputer et de contrôler par service ou par poste les dépenses téléphoniques de l'organisation.

La gestion des relevés téléphoniques

Lorsque des relevés sont établis (ex : facturation détaillée des opérateurs de téléphone), les **quatre derniers chiffres de ces numéros doivent être occultés.**

Les supérieurs hiérarchiques ne doivent accéder aux numéros complets des relevés individuels que de façon exceptionnelle (par exemple en cas d'utilisation manifestement anormale du téléphone par un salarié).

Bien entendu, un salarié doit avoir la possibilité d'accéder aux numéros de téléphone complets composés depuis son poste téléphonique, notamment lorsqu'il lui est demandé le remboursement du coût des communications téléphoniques présumées personnelles.

La durée de conservation des données relatives à l'utilisation des services de téléphonie ne doit pas excéder un an.

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).

Comment déclarer ?

Concernant les fichiers mis en oeuvre 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).

Les dispositifs de géolocalisation des véhicules 11

Certains employeurs équipent leurs véhicules professionnels de dispositifs de géolocalisation GPS/GSM. Ces outils sont en plein essor dans le monde du travail. Toutefois, en raison des risques d'atteinte aux droits et libertés des personnes que comporte l'utilisation de ces dispositifs, la CNIL est venue préciser les conditions dans lesquelles ils pouvaient être utilisés.

Pourquoi mettre en place de tels dispositifs ?

La géolocalisation des véhicules peut être mis en place pour les finalités suivantes :

- Garantir la sécurité des employés, des marchandises transportées, ou des véhicules dont il a la charge ;
- Permettre une meilleure gestion des moyens en personnel et véhicules (prestations à accomplir en des lieux dispersés) ;
- Suivre et facturer une prestation de transport de personnes, de marchandises ou de prestation de service directement liée à l'utilisation du véhicule ;
- Suivre le temps de travail des employés, uniquement lorsque ce suivi ne peut être réalisé par d'autres moyens ;
- Respecter une obligation légale ou règlementaire imposant la mise en œuvre d'un dispositif de géolocalisation en raison du type de transport ou de la nature du bien transporté.

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

Quelles sont les conditions à respecter ?

La consultation des instances du personnelles

L'utilisation d'un dispositif de géolocalisation implique l'information et la consultation des instances représentatives du personnel avant toute installation dans les véhicules mis à la disposition des employés.

L'information des salariés

Les employés concernés doivent faire l'objet d'une information individuelle sur le dispositif, et plus précisément sur :

- la finalité poursuivie du traitement,
- les données traitées et les destinataires des données,
- leur durée de conservation,
- leurs droits d'accès, de rectification et d'opposition pour motif légitime.

Cette information peut être faite par le biais d'un avenant au contrat de travail ou d'une note de service, par exemple.

Exemple de message d'information

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).

Mesures de sécurité et durée de conservation des données

Il est impératif d'accompagner la géolocalisation des véhicules de mesures visant à limiter l'accès aux données de géolocalisation aux personnes habilitées (exemple : par le biais d'un identifiant et d'un mot de passe permettant aux personnes habilitées d'accéder au dispositif de suivi en temps réel sur un site internet). Ces mesures permettent de sécuriser le sytème en évitant que des personnes non autorisées accèdent aux données collectées.

Il est également essentiel de fixer une durée de conservation adéquate de ces données :

- en principe, les données obtenues ne doivent pas être conservées plus de 2 mois ;
- elles peuvent être conservées un an lorsqu'elles sont utilisées pour optimiser l'organisation des tournées ou à des fins de preuve des interventions effectuées (lorsqu'aucun autre moyen de preuve n'est possible) ;
- elles peuvent entre conservées cinq ans lorsque les données sont utilisées pour le suivi du temps de travail.

Ce qu'il faut éviter

Afin de garantir le respect de la vie privée des salariés et de conserver un caractère proportionné au but poursuivi, le dispositif de géolocalisation des véhicules 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 ;
- permettre la collecte d'informations concernant les éventuels dépassements des limitations de vitesse (interdiction de collecter des données relatives aux infractions, sauf législation particulière) ;
- s'appliquer aux employés investis d'un mandat électif ou syndical lorsqu'ils agissent dans le cadre de leur mandat.

Comment déclarer ?

Un dispositif de géolocalisation des véhicules des employés doit faire l'objet d'une déclaration auprès de la CNIL :

- déclaration simplifiée de conformité à la norme simplifiée n°51 ;
- déclaration normale si le dispositif n'est pas conforme à la norme précitée.

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

12 L'utilisation de badges ou de dispositifs biométriques sur le lieu de travail

Dans le cadre du contrôle des accès aux locaux, de la gestion du temps de travail, et de la gestion de la restauration d'entreprise, l'employeur peut avoir recours à plusieurs dispositifs comme le badge ou la 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…).

L'utilisation de ces dispositifs est **strictement encadrée** afin de préserver les droits et libertés des employés.

Quelles garanties prévoir ?

Chaque passage du badge dans un lecteur, ou l'utilisation de dispositifs biométriques, permet l'enregistrement de données relatives à son utilisateur. Ces données sont susceptibles d'être utilisées de manière détournée à des fins de surveillance de l'activité des salariés, puisqu'elles permettent de « tracer » les déplacements de ces derniers. Elles peuvent également donner à l'employeur des informations privées (exemple : consommations au restaurant d'entreprise).

Des garanties particulières doivent donc être apportées par l'employeur pour éviter de tels détournements de finalité.

La consultation des instances du personnelles

L'utilisation d'un dispositif contrôle des horaires ou d'accès aux locaux (badge ou dispositif biométrique) implique l'information et la consultation des instances représentatives du personnel avant toute installation.

La nécessaire information des salariés

Il est impératif pour l'employeur d'informer chaque employé sur :

- les finalités poursuivies par le dispositif (ex : contrôle des accès, gestion des temps de présence…) ;
- la nature des informations qui seront collectées ;
- les destinataires des données issues du dispositif ;
- les modalités d'exercice du droit d'accès, de rectification, et du droit d'opposition pour motif légitime.

Les personnes concernées par le dispositif biométrique doivent, en plus, être clairement informées de ses conditions d'utilisation et de son caractère obligatoire ou facultatif.

Exemple de dote d'information pour un dispositif de contrôle d'accès (badges, biométrie)

…… (indication de l'identité du responsable du traitement)

Un dispositif (biométrique) destiné au contrôle de l'accès …… (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 …… (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 en 2004, vous pouvez avoir accès et rectifier les informations qui vous concernent en vous adressant à …… (préciser le service et l'adresse).

Mesures de sécurité et durée de conservation des données

L'employeur doit prévoir des mesures pour assurer la sécurité des informations concernant ses salariés et éviter que des personnes ne puissent en prendre connaissance, alors même qu'elles n'ont pas la qualité pour y accéder.

Des habilitations doivent donc être prévues pour les accès informatiques, avec une traçabilité des actions effectuées.

Les données relatives aux accès doivent être supprimées **3 mois** après leur enregistrement. Celles utilisées pour le suivi du temps de travail, y compris les données relatives aux motifs des absences doivent être conservées pendant **5 ans maximum.**

Comment déclarer ?

Les **dispositifs de contrôle d'accès aux locaux et de contrôle des horaires** doivent faire l'objet d'une déclaration auprès de la CNIL :

- déclaration simplifiée de conformité à la **norme simplifiée n° 42**,
- déclaration normale si le dispositif n'est pas conforme à la norme précitée.

En cas de désignation d'un Correspondant Informatique et Libertés (CIL), aucune déclaration n'est nécessaire.

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…). Par principe, chaque application fait l'objet d'un examen au cas par cas, en fonction notamment de la caractéristique biométrique utilisée.

Cependant, afin de faciliter les formalités, la CNIL a défini un cadre, appelé autorisation unique, applicable à certains dispositifs biométriques. Il lui suffira alors d'adresser à la CNIL une simple déclaration de conformité à l'une des autorisations uniques suivantes :

- **autorisation n°AU-007** relative à 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 n°AU-008** relative à la reconnaissance 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-019** du réseau veineux des doigts de la main pour contrôler l'accès aux locaux sur les lieux de travail.

ANNEXES

Mode d'emploi : comment déclarer ?[15]

La déclaration est une obligation légale dont le non-respect est pénalement sanctionné[16]. Tout fichier ou traitement informatisé comportant des données personnelles doit donc être déclaré à la CNIL préalablement à sa mise en oeuvre, sauf s'il est expressément exonéré de déclaration. Cette formalité peut prendre plusieurs formes selon le fichier concerné (voir tableau récapitulatif à la fin du guide.).

Les déclarations peuvent être réalisées en ligne sur le site de la CNIL (www.cnil.fr rubrique « déclarer »). En cas de doute sur le régime dont relève le traitement, il suffit de réaliser une déclaration normale en ligne : la CNIL se chargera de qualifier le dossier et de contacter le déclarant.

Dans tous les cas, la désignation d'un Correspondant Informatique et Libertés (CIL) dispense l'organisme concerné de devoir accomplir les formalités relatives aux fichiers relevant de la déclaration simplifiée et de la déclaration normale. Le formulaire de désignation d'un CIL est accessible sur le site www.cnil.fr.

Les dispenses de déclaration

un certain nombre de traitements, décrits dans le tableau récapitulatif figurant ci-après, sont dispensés de déclaration par une décision de la CNIL (paie du personnel, comptabilité…).

Attention : Le fait d'être exonéré ne signifie pas pour autant que vous n'avez aucune obligation. Vous devez notamment garantir le droit d'information des personnes ainsi que la sécurité des données.

15 Guide CNIL pour les employeurs et salariés - 2010

16 Article 226-16 du code pénal : « 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 oeuvre prévues par la loi est puni de cinq ans d'emprisonnement et de 300 000 € d'amende ».

La déclaration simplifiée

La plupart des fichiers des entreprises ou administrations peuvent faire l'objet de **déclarations simplifiées**, qui se font en ligne sur le site de la CNIL (www.cnil.fr, rubrique « Déclarer »).

La déclaration normale

Le régime de droit commun est la **déclaration normale**, lorsque le fichier ne relève pas d'une procédure particulière (art. 22 de la loi du 6 janvier 1978 modifiée en 2004). Le traitement peut être mis en oeuvre dès réception du récépissé délivré par la CNIL.

Le récépissé atteste de l'accomplissement des formalités de déclaration, mais n'exonère pas le responsable du respect des autres obligations prévues par la loi (en ce qui concerne la finalité du fichier, sécurité et confidentialité, les droits des personnes…).

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 ;

- les traitements qui sont susceptibles 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.

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.

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
Paie 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 Tenue des registres obligatoires (registre unique du personnel…) Tenue des comptes individuels relatifs à l'intéressement et à la participation Remise dématérialisée du bulletin de paie (cf art L3243-2 du code du travail) Statistiques non nominatives liées à l'activité salariée dans l'entreprise	AUCUNE	Respecter les termes de la **dispense n° 1** (employeurs publics) ou la **dispense n° 2** (employeurs privés) du 9 décembre 2004 **Attention :** Les transferts de données vers un pays tiers à l'Union Européenne ne sont pas dispensés. **Attention :** le coffre-fort électronique ou l'archivage numérique ne sont pas dispensés.
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 oeuvre 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
• Gestion des contrôles d'accès aux locaux, • Gestion des horaires, • Gestion de la restauration d'entreprise	**DÉCLARATION SIMPLIFIÉE** Si désignation d'un correspondant informatique et libertés : AUCUNE	Respecter la **norme simplifiée n° 42**. Cette norme ne concerne pas les traitements recourant à un procédé de reconnaissance biométrique, qui sont soumis à une procédure d'autorisation

Fichiers courants de gestion des ressources humaines : • 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	**DÉCLARATION SIMPLIFIÉE** Si désignation d'un correspondant informatique et libertés : **AUCUNE**	Respecter la norme simplifiée n° 46. Cette norme exclut notamment : • les traitements permettant le contrôle individuel de l'activité des employés • les dispositifs ayant pour objet l'établissement du profil psychologique des employés
Mise en oeuvre de services de téléphonie fixe et mobile sur les lieux de travail Gestion des communications (annuaire interne, gestion des dotations, messagerie téléphonique interne, maîtrise des dépenses liées à l'utilisation des services de téléphonie…	**DÉCLARATION SIMPLIFIÉE** **Si désignation d'un correspondant informatique et libertés :** **AUCUNE**	Respecter la **norme simplifiée n° 47**. Cette norme exclut expressément : • les finalités relatives à l'écoute ou à l'enregistrement de conversations téléphoniques • la localisation d'un employé à partir de son téléphone portable
Mise en oeuvre de services destinés à géolocaliser les véhicules utilisés par les employés	**DÉCLARATION SIMPLIFIÉE** **Si désignation d'un correspondant informatique et libertés :** **AUCUNE**	Respecter la **norme simplifiée n° 51**.

FINALITÉ DU FICHIER	FORMALITÉS DÉCLARATIVES	CONDITIONS PARTICULIÈRES
Tout autre traitement automatisé, dès lors qu'il n'est pas conforme aux normes élaborées par la Commission, notamment : Annuaires 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) Traitements comportant un transfert de données vers un pays tiers à l'Union européenne	**DÉCLARATION NORMALE** **Si désignation d'un correspondant informatique et libertés :** **AUCUNE** **AUTORISATION**	Utiliser le formulaire de déclaration normale (téléchargeable sur le site de la CNIL www.cnil.fr, rubrique déclarer, mode d'emploi) Pour les fichiers de recrutement : se référer à la recommandation n° 02-017 du 21 mars 2002
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	**AUTORISATION UNIQUE**	Respecter les termes de l'autorisation unique AU-007
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	**AUTORISATION UNIQUE**	Respecter les termes de l'autorisation unique AU-008
Dispositifs biométriques : reconnaissance du réseau veineux des doigts de la main pour contrôler l'accès aux locaux sur les lieux de travail	**AUTORISATION UNIQUE**	Respecter les termes de l'autorisation unique AU-019
Dispositifs d'alerte professionnelle (lignes éthiques) dans le domaine financier, comptable, bancaire et de la lutte contre la corruption.	**AUTORISATION UNIQUE**	Respecter les termes de l'autorisation unique AU-004

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 oeuvre 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…)

**Fédération des Industries Electriques,
Electronique et de Communciation**

11-17 rue de l'Amiral Hamelin
75783 PARIS cedex 16

WWW.FIEEC.FR

@ FIEEC