RGPD : protégez les données de vos collaborateurs

Notre métier en RGPD et en CYBER : Auditer, Expertiser, Accompagner, Former et Informer					
		RGPD : Protégez les données de vos collaborateurs			

Protéger les données personnelles de vos collaborateurs sur leur lieu et pendant leur temps de travail c'est aussi un moyen de renforcer le lien de confiance nécessaire au bon fonctionnement de votre entreprise. Le développement de l'utilisation des nouvelles technologies au travail peut faire craindre surveillance systématique. La transparence sera alors le meilleur moyen de s'en prémunir.

La gestion de vos collaborateurs

De très nombreuses données personnelles relatives aux employés sont nécessaires pour la gestion de leur carrière au sein de votre entreprise.
Par exemple, vous avez besoin de beaucoup d'informations pour assurer :
• la rémunération et les déclarations sociales obligatoires ;
• la tenue du registre unique du personnel ;
• la gestion administrative du personnel (exemple : type de permis de conduire détenu ou coordonnées de personnes à prévenir en cas d'urgence) ;
• l'organisation du travail (exemple : photographie facultative de l'employé pour les annuaires internes et organigrammes) ;
• l'action sociale prise en charge par l'employeur (exemple : les informations concernant les ayants-droit de l'employé).

Ne demandez à vos employés que les informations utiles pour accomplir leurs missions, et évitez de traiter des données dites « sensibles » (activité syndicale, opinions politiques, religion, origine ethnique, santé). Si vous devez en traiter, des obligations particulières sont applicables.
Vous disposez forcément d'informations particulières (et donc à risque) sur vos employés (coordonnées bancaires pour la paie, numéro de sécurité sociale pour les déclarations sociales, etc.). **Assurez-vous d'en garantir la confidentialité et la sécurité. Ainsi, seules les personnes habilitées doivent en prendre connaissance**. Les actions sur les données effectuées par les personnes habilitées doivent être enregistrées (savoir qui se connecte à quoi, quand et pour faire quoi).

Informez vos collaborateurs à chaque fois que vous leur demandez des informations (exemple : mise à jour des données administratives, demande de formation, formulaire d'entretien d'évaluation, etc.).
Enfin, souvenez-vous toujours que vos salariés peuvent vous demander une copie de toutes les données les concernant que vous détenez : copie d'un bulletin de paie, état d'un compte épargne-temps, mais aussi les enregistrements téléphoniques, relevés des badgeuses, ou encore des messages envoyés via le mail professionnel – y compris lorsqu'un employé n'est plus en poste ou est en litige avec vous.

Le recrutement d'un nouveau collaborateur

Lorsque vous recrutez un nouveau collaborateur, vous ne pouvez pas demander tout et n'importe quoi aux candidats. **Seules les informations utiles au regard du poste à pourvoir peuvent être collectées**.
Exemple : des informations sur l'emploi occupé par les membres de sa famille n'ont pas de lien avec les compétences du candidat à occuper l'emploi proposé. Il est par ailleurs inutile, à ce stade, de demander aux candidats leur numéro de sécurité sociale.

Informez les candidats sur ce que vous allez faire des données qu'ils vous communiquent, qui va y avoir accès (service RH, un prestataire ?), combien de temps vous allez les conserver, comment ils peuvent exercer leurs droits sur leurs données.
Les candidats doivent notamment pouvoir accéder à leurs données, les faire rectifier ou supprimer.
Une fois le choix de votre nouvel employé effectué, supprimez les informations sur les candidats non retenus, sauf s'ils acceptent de rester dans votre « vivier » pour une durée limitée (2 ans).

Les limites au contrôle de l'activité de vos collaborateurs

Le code du travail vous permet de contrôler l'activité de vos employés. Les nouvelles technologies facilitent bien évidemment ce contrôle.
Mais tout n'est pas permis. Même sur son lieu de travail, un employé a droit au respect de sa vie privée et à la protection de ses données personnelles.

2 règles simples à retenir :
1. **N'abusez pas de votre pouvoir !**
    - la surveillance doit reposer sur un intérêt légitime pour l'entreprise (exemple : limiter les risques d'abus d'une utilisation trop personnelle d'internet ou de la messagerie pendant son temps de travail) ;
    - les employés ne doivent pas être mis sous une surveillance permanente (exemple : la sécurisation d'un local professionnel n'impose pas de filmer en permanence un employé sur son poste de travail) ;
    - un outil mis en place dans un but ne doit pas poursuivre un autre objectif caché (exemple : un outil de géolocalisation des véhicules opérant une tournée chaque matin chez des clients afin d'optimiser votre organisation ne doit pas servir à contrôler la vitesse de circulation en temps réel de votre employé).
2. **Soyez transparent !**
    - les instances représentatives du personnel doivent être consultées, lorsqu'elles existent ;
    - les employés doivent être informés de la mise en œuvre d'un dispositif de surveillance, selon les modalités les plus appropriées en fonction de l'organisation et du fonctionnement de l'entreprise (par exemple, charte d'utilisation des outils informatiques, note de service, avenant au contrat de travail, mention d'information sur un intranet, courrier d'information joint au bulletin de paye, etc.).
En fonction des technologies que vous utilisez pour exercer votre contrôle (vidéosurveillance, géolocalisation, écoutes et enregistrements téléphoniques, etc.) des règles particulières peuvent s'appliquer.
***Pour en savoir plus** : Fiches pratiques « Travail et protection des données »*

Sensibilisez et formez vos collaborateurs !

La protection des données personnelles de vos employés comme de vos clients n'est pas que l'affaire de juristes ou d'informaticiens.
*Tous vos employés doivent être sensibilisés à cette question. Ils sont concernés en tant que professionnels en relation avec vos clients, vos fournisseurs, vos prestataires, **et en tant que citoyens**.*
Des points d'attention assez simples peuvent facilement être mis en place :
• sensibilisez sur les droits des personnes concernées afin que les demandes reçues dans n'importe quel service soient clairement identifiées et qu'une procédure de traitement par le bon service soit connue et appliquée (exemple : le service client reçoit une demande d'opposition à recevoir de la publicité et la transmet au service en charge du marketing) ;
• sensibilisez largement sur les règles internes de gestion des données personnelles (on ne peut accéder qu'aux données dont on a besoin, on ne doit pas divulguer des données à des tiers non autorisés, les dossiers archivés ne sont accessibles qu'à certaines personnes, il faut effectuer des sauvegardes régulières de ses fichiers, etc.) ;
• sensibilisez aux règles élémentaires de sécurité (exemple : log-in, et mot de passe personnels complexes, poste de travail verrouillé dès que l'on s'absente, ne pas stocker des documents professionnels sur des outils personnels, etc.).

Profitez de la mise en place du RGPD pour sensibiliser l'ensemble de vos collaborateurs sur les règles à suivre en matière de protection des données et diffusez votre charte informatique.
Source : CNIL

Accompagnant depuis 2012 de nombreux établissements, Denis JACOPINI, Expert informatique diplômé en cybercriminalité, certifié en gestion des risques sur les systèmes d'information (ISO 27005) et formé par la CNIL depuis 2011 sur une trentaine de thèmes, est en mesure de vous accompagner dans votre démarche de mise en conformité RGPD.

Besoin d'un expert pour vous mettre en conformité avec le RGPD ?

Contactez-nous

Accompagné de son équipe d'auditeurs et de formateurs, notre Expert, Denis JACOPINI est spécialisé en cybercriminalité et en protection des Données à Caractère Personnel, formateur depuis 1998 et consultant depuis 1996. Avec bientôt une **expérience d'une dizaine d'années** dans la mise en conformité avec la réglementation relative à la Protection des Données à Caractère Personnel, de formation d'abord technique, Correspondant CNIL en 2012 (CIL : Correspondant Informatique et Libertés) puis en 2018 Délégué à la Protection des Données, en tant que praticien de la mise en conformité et formateur, il lui est ainsi aisé d'accompagner les organismes dans leur démarche de **mise en conformité avec le RGPD**.

« *Mon objectif, vous assurer une démarche de mise en*

conformité validée par la CNIL. ».

Nous vous aidons à vous mettre en conformité avec le RGPD de 2 manières :

Quelques articles sélectionnés par nos Experts :

Comment se mettre en conformité avec le RGPD
Accompagnement à la mise en conformité avec le RGPD de votre établissement
Formation RGPD : L'essentiel sur le règlement Européen pour la Protection des Données Personnelles
Comment devenir DPO Délégué à la Protection des Données
Des guides gratuits pour vous aider à vous mettre en conformité avec le RGPD et la CNIL
Mise en conformité RGPD : Mode d'emploi
Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016
DIRECTIVE (UE) 2016/680 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 27 avril 2016
Comprendre le Règlement Européen sur les données personnelles en 6 étapes
Notre sélection d'articles sur le RGPD (Règlement Européen sur la Protection des données Personnelles) et les DPO (Délégués à la Protection des Données)

Réagissez à cet article

Source : *RGPD en pratique : protéger les données de vos collaborateurs | CNIL*