Mémo

Les données que vous avez le droit de collecter dans le dossier RH

Ce mémo est un résumé du **webinaire** du **23 janvier 2025**

avec

Margaux Tedesco
Avocate en droit social et RH

Théo Dickel
Product Marketing Manager - Socle RH

01 RGPD : rappel de vos obligations

Le **RGPD** (Règlement Général sur la Protection des Données) est un texte réglementaire européen qui encadre le traitement des données de manière égalitaire sur tout le territoire de l'Union européenne (UE). Il est entré en application le 25 mai 2018.

Qu'est-ce qu'une donnée RH ?

Une donnée RH est toute information permettant d'identifier une personne physique, qu'elle soit professionnelle (comme un matricule de paie ou une adresse email professionnelle) ou personnelle (adresse postale, RIB, statut marital, etc.). Ces données sont régies par le RGPD dès lors qu'elles peuvent directement ou indirectement identifier une personne.

Quelles sont vos obligations ?

Le RGPD impose plusieurs règles clés :

- **Justification du traitement** : toute collecte ou traitement de données doit être fondé sur l'un des six principes légaux (consentement, contrat, obligation légale, mission d'intérêt public, intérêt légitime, sauvegarde des intérêts vitaux).
- **Interdiction spécifique** : certaines données, comme les opinions politiques, les convictions religieuses ou les données biométriques, sont interdites de traitement sauf exceptions prévues par la loi.
- **Sécurité et exactitude** : les données doivent être conservées de manière sécurisée, exactes et à jour.
- **Information des collaborateurs** : les personnes concernées doivent être informées des finalités de la collecte et du traitement de leurs données.

Que risquez-vous en cas de manquement ?

- **Sanctions financières** : amendes pouvant atteindre jusqu'à 4 % du chiffre d'affaires annuel mondial ou 20 millions d'euros (le montant le plus élevé est retenu).
- **Risques réputationnels** : perte de confiance des collaborateurs et clients.
- **Exemples concrets** : la conservation de données obsolètes ou la collecte de données interdites peut entraîner des poursuites ou des pénalités de la CNIL.

Comment être en conformité ?

- **Utiliser des outils sécurisés** : optez pour des solutions fiables pour la gestion des données RH.
- **Mettre à jour les données** : assurez-vous que les informations conservées dans le dossier RH sont exactes et pertinentes.
- **Informer et documenter** : fournissez une information claire sur les données collectées et maintenez des registres précis pour justifier les traitements en cas de contrôle ou de conflit.

02 RGPD : démêlons le vrai du faux

Vrai ou faux ?

La CNIL interdit de collecter le numéro de sécurité sociale **Faux**

Il n'y a pas d'interdiction de la CNIL, mais il est essentiel de collecter le numéro de sécurité sociale uniquement pour des besoins légaux spécifiques comme la DPAE ou l'affiliation à une mutuelle, et d'informer les salariés du motif de la collecte.

Les **commentaires** ("champ explications") ajoutés dans les **formulaires de mise à jour ou d'onboarding** permettent de fournir un contexte précis et de justifier la collecte des données. Une fois le formulaire complété et envoyé, le consentement du collaborateur est enregistré, garantissant qu'il a pris connaissance des informations.

Je n'ai pas droit de collecter les données santé de mes collaborateurs **Faux**

Par principe, les données de santé sont protégées. Toutefois, certaines données comme la qualité de travailleur handicapé peuvent être collectées si le salarié donne son consentement express, notamment pour des obligations légales (ex. BDESE).

Je demande un maximum d'informations pour éviter de devoir en demander à nouveau **Faux**

Le RGPD impose de ne collecter que les informations strictement nécessaires. Anticiper un besoin futur (comme demander un permis de conduire sans besoin immédiat) est une mauvaise pratique.

Demande de mise à jour : il est recommandé d'ajouter dans le mail reçu par le collaborateur des explications sur les raisons légales de la demande et pourquoi cette information est requise à ce moment précis. Cela permet de limiter les données demandées lors de l'onboarding et d'en collecter davantage plus tard, évitant ainsi une surcharge d'informations d'un seul coup.

02 RGPD : démêlons le vrai du faux

Vrai ou faux ?

Le contact d'urgence doit être public pour pouvoir prévenir rapidement Faux

Le contact d'urgence est une donnée sensible pouvant révéler des informations personnelles. L'accès doit être limité et ne pas être rendu public, même sous une forme partielle.

Permissions et rôles : il est crucial de bien gérer les permissions octroyées à chaque rôle au sein de l'entreprise. Assurez-vous que les utilisateurs n'ont accès qu'aux données qui sont strictement nécessaires à leurs fonctions, afin de respecter la confidentialité et la sécurité des informations personnelles.

Une fois que j'ai collecté une donnée avec justification, je peux en faire ce que je veux Faux

L'utilisation d'une donnée est strictement limitée au contexte et au motif pour lesquels elle a été collectée. Un nouvel usage nécessite une réévaluation des bases légales et une information aux salariés.

Demande de mise à jour des données : avant d'envoyer un formulaire de mise à jour des données, il n'est pas toujours nécessaire de justifier chaque information individuellement, surtout s'il n'y a pas de raison évidente de mise à jour. Utilisez **le module de génération de documents et de signature en masse** pour faire signer à vos collaborateurs un "bon pour accord" concernant la mise à jour des données administratives. Ce document, tel qu'une charte des données personnelles, servira de preuve en cas de litige.

03 CNIL : les bonnes pratiques à adopter

La **CNIL** (Commission Nationale de l'Informatique et des Libertés) est l'autorité française chargée de veiller à la protection des données personnelles et au respect de la vie privée. Elle a été créée en 1978.

La CNIL recommande de :

- **Sécuriser les données** : utilisez des outils fiables et sécurisés pour stocker les données (ex : Lucca), et assurez-vous qu'elles sont protégées contre toute utilisation abusive.
- **Veiller à l'exactitude des données** : les données doivent être exactes et à jour. Si vous utilisez un outil comme Poplee Socle RH, veillez à ce que les informations conservées dans les dossiers des collaborateurs soient régulièrement mises à jour.
- **Informer les collaborateurs** : vous devez informer vos collaborateurs de la collecte et de l'utilisation de leurs données. Ce principe de transparence est essentiel, et cela doit être fait dès le début de la collecte des données.
- **Rationaliser les données collectées**: ne collectez que les données nécessaires. Evitez de collecter des informations inutiles pour réduire les risques.

"C'est un exercice mental en tant que RH : dès qu'on demande une donnée, si nous pouvons nous-même deviner une information personnelle, cela signifie que toute personne qui accédera à ces données pourra aussi deviner cette information." - **Margaux Tedesco, Avocate en droit social et RH**

Ressources complémentaires

- Protégez les données de vos collaborateurs
- Guide pratique de sensibilisation au RGPD pour les petites et moyennes entreprises
- Référentiel - relatif aux traitements de données à caractère personnel mis en oeuvre aux fins de gestion du personnel

04 Sanctions : ce que vous risquez si vous ne jouez pas le jeu

Contrôle de la CNIL, qui est concerné ?

Contrairement à une idée reçue, le contrôle par la CNIL ne se limite pas aux grandes entreprises. Toute organisation peut être contrôlée, sans critères prévisibles.

Les contrôles peuvent être réalisés :

- suite à un signalement ou la plainte d'un individu (ex. : salarié mécontent, client, etc.).
- dans le cadre de procédures juridiques, comme un contentieux entre l'entreprise et un collaborateur.

Quelles sont les sanctions possibles ?

La CNIL applique des sanctions graduées, en fonction de la gravité des manquements :

- **Rappel à l'ordre** : invitation à corriger les pratiques.
- **Injonction** : obligation de se conformer dans un délai imparti.
- **Limitation ou interdiction temporaire/définitive** : suspension de la collecte ou du traitement des données en question.
- **Retrait de certifications** : s'applique surtout aux entreprises gérant des données complexes.
- **Amendes administratives** : jusqu'à 4 % du chiffre d'affaires annuel mondial ou 20 millions d'euros.
- **Sanctions pénales** :
  - 5 ans d'emprisonnement.
  - 300 000 € d'amende pour le dirigeant.

Exemple : le cas Ikea France

Entre 2009 et 2012, IKEA France a illégalement collecté des données sensibles sur ses salariés (antécédents judiciaires, patrimoine) sans les informer.

Sanction : le PDG a été condamné à 4 mois de prison avec sursis et 20 000 € d'amende.

Foire aux questions

Casier judiciaire

Q : Peut-on demander un extrait de casier judiciaire même si celui-ci est vierge ?

R : Peu importe que le casier judiciaire soit vide, un employeur peut uniquement consulter le casier judiciaire d'un candidat si cette demande est justifiée par la nature des fonctions à exercer. Vous pouvez donc uniquement consulter le casier judiciaire mais vous ne pouvez pas en conserver de copie.

Q : Un prestataire affirme que la demande du casier judiciaire est obligatoire pour toutes les embauches. Est-ce exact ?

R : Non, un employeur ne peut demander un extrait de casier judiciaire que si la loi l'exige ou si la nature du poste le justifie.

Q : La fonction publique est-elle soumise à la même règle ?

R : Oui, l'extrait du casier judiciaire ne peut être demandé que si la loi ou la nature du poste le justifie.

Conservation des documents d'identité

Q : Peut-on conserver la carte nationale d'identité d'un employé pendant toute la durée du contrat ?

R : Lors de l'embauche, l'employeur peut demander une copie de la CNI pour vérifier l'identité du salarié et, le cas échéant, pour s'assurer de son autorisation à travailler en France. Une fois cette vérification effectuée, la CNIL recommande de ne pas conserver de copie de la CNI au-delà de ce qui est strictement nécessaire pour remplir les obligations légales. Ainsi, dès que vous avez effectué les vérifications légales nécessaires, vous devrez détruire la copie de la CNI.

Q : Comment prouver qu'un document d'identité a bien été demandé si celui-ci a été détruit ?

R : Vous pourrez prouver que vous avez agi conformément à la réglementation en fournissant les échanges et preuves de votre demande, montrant une trace des vérifications effectuées et expliquant votre processus de destruction sécurisé des données personnelles.

Foire aux questions

Données personnelles et RGPD

Q : Un prestataire de paie est-il soumis au RGPD ?

R : Oui, en tant que sous-traitant, il doit respecter le RGPD.

Q : Peut-on mentionner le numéro de sécurité sociale dans le contrat de travail ?

R : La collecte et l'utilisation du NIR doivent respecter le principe de proportionnalité, c'est-à-dire qu'elles doivent être strictement nécessaires à la finalité poursuivie. Or, le contrat de travail n'est pas un document destiné à la gestion de la paie ou aux déclarations sociales obligatoires. Par conséquent, la mention du numéro de sécurité sociale dans le contrat de travail n'est pas justifiée et pourrait être considérée comme excessive au regard des finalités du traitement des données personnelles. La CNIL a d'ailleurs rappelé cela.

Q : Peut-on conserver les entretiens annuels après le départ d'un salarié ?

R : Selon la CNIL, les données d'évaluation ne doivent pas être conservées après le départ d'un salarié, sauf archivage en base intermédiaire pour se prémunir contre d'éventuelles actions en justice, dans la limite des délais de prescription (1 à 5 ans). Dans ce cas, elles doivent être stockées sur un support distinct et accessibles uniquement par des personnes habilitées, comme le service contentieux. Les justificatifs appartenant à l'entreprise doivent être conservés en cas de contrôle, mais les données personnelles (documents, entretiens, évaluations) doivent être supprimées après cinq ans. Le module de droit à l'oubli permet d'anonymiser certaines données, mais d'autres (justificatifs d'absence, bilans d'entretien, contrats) nécessitent une suppression manuelle. Chez Lucca, nous avons conscience de ces enjeux et de la nécessité d'automatiser ces tâches de nettoyage. Toutefois, ce sujet n'est pas encore prévu dans l'immédiat, car il implique plusieurs solutions et une mise en place complexe.

Q : Peut-on collecter et conserver les noms, prénoms et dates de naissance des enfants des collaborateurs ?

R : Oui, uniquement pour des finalités légitimes comme les avantages sociaux.

Données de santé des salariés

Q : Peut-on collecter des données de santé des salariés, comme leur statut vaccinal ?

R : Oui, uniquement si la loi l'exige ou si cela est justifié par la nature du poste. Le salarié peut refuser de communiquer cette information.

Q : Peut-on conserver des informations sur les pathologies de santé des salariés ?

R : Les informations sur la santé d'un salarié sont des données sensibles, dont le traitement est en principe interdit. Collecter des données de santé dans le cadre de la prévention des risques professionnels ne respecte pas forcément les principes de finalité et de proportionnalité imposés par le RGPD et même avec le consentement des salariés, la collecte directe par l'employeur est problématique en raison du déséquilibre inhérent à la relation de subordination. La médecine du travail a un rôle primordial sur ces aspects en appréciant notamment l'aptitude des salariés et en récoltant des données de santé.

Foire aux questions

Durée de conservation des données

Q : Combien de temps peut-on conserver les documents administratifs des salariés ?

R : Les durées de conservation varient selon les obligations légales. Pour plus de précisions, consultez le référentiel de la CNIL.

Q : Les arrêts maladie sont-ils conservés après le départ d'un salarié ?

R : En principe, les arrêts maladie doivent être conservés pendant 5 ans, conformément à l'article D4711-3 du Code du travail. En cas de contentieux, ils peuvent être conservés jusqu'au règlement définitif de l'affaire. Les justificatifs d'arrêts maladie doivent être supprimés après cinq ans, sauf obligation légale ou contrôle. Lucca a conscience de cet enjeu et prévoit d'automatiser ces tâches de nettoyage, mais cela implique plusieurs solutions et reste un projet complexe qui ne verra pas le jour immédiatement.

Q : Une purge automatique des dossiers est-elle prévue dans Lucca ?

R : Non, l'anonymisation des données nécessite une action manuelle via le module de droit à l'oubli. .

Signature de documents

Q : Le module de signature en masse est-il disponible ?

R : Oui, il est en cours de déploiement et sera activé d'ici la fin du trimestre sur toutes les bases Lucca.

Q : La fonctionnalité de signature en masse est-elle gratuite ?

R : Oui, elle est accessible gratuitement si vous avez Socle RH.

Accès et gestion des données dans Socle RH

Q : Peut-on paramétrer des accès donnée par donnée sur Poplee ?

R : Non, les permissions se font par sections de données.

Q : L'historique des données dans Lucca peut-il poser un problème RGPD ?

R : Oui, sauf si une justification légale existe. Il est recommandé d'anonymiser ou de supprimer les données inutiles via le module de droit à l'oubli. .

Consentement et clauses contractuelles

Q : Un consentement oral est-il suffisant pour la collecte des données ?

R : Non, un consentement écrit est recommandé pour prouver son obtention.

Q : Que doit contenir une clause RGPD dans un contrat de travail ?

R : Elle doit préciser l'identité du responsable du traitement, les finalités du traitement, la base légale du traitement, Les destinataires des données, la durée de conservation des données, les droits du salarié et comment les exercer.

À propos de Lucca

Lucca développe des logiciels qui simplifient la vie des collaborateurs, de leurs managers et des responsables RH.

Nous aidons les entreprises à devenir plus performantes et réduire les tâches qui coûtent pour se consacrer à celles qui comptent.

Les logiciels que nous éditons couvrent **un large éventail des enjeux en matière de gestion des ressources humaines :** dossier collaborateurs, temps et activités, dépenses professionnelles, gestion des talents, préparation de la paie.

www.lucca.fr
+ 33 (0)1 83 64 53 20 - info@lucca.fr