Comment gérer les données de santé des salariés en respectant le RGPD ?

Réponse courte

Au Luxembourg, les **données de santé** des salariés bénéficient d'une protection renforcée au titre du **RGPD** et de la loi du 1er août 2018. L'employeur ne peut traiter ces données que pour des **finalités légalement justifiées** : gestion des absences maladie, adaptation du poste de travail, ou respect des obligations en matière de santé et sécurité au travail.

Le **médecin du travail** et les **services de santé au travail** sont les seuls habilités à accéder au dossier médical complet. Les responsables RH ne peuvent accéder qu'aux informations strictement nécessaires à l'exercice de leurs missions, dans les cas expressément prévus par la loi ou une convention collective. L'employeur reçoit uniquement des **avis d'aptitude** ou des **certificats d'absence**, jamais le détail médical.

Des **procédures internes documentées** doivent garantir la confidentialité, la sécurité et la **traçabilité des accès**. Les données de santé sont conservées **séparément** des autres données RH, dans des systèmes sécurisés avec accès restreints. Les salariés doivent être **informés** de leurs droits, des finalités du traitement et des destinataires.

Une **analyse d'impact relative à la protection des données (AIPD)** doit être réalisée avant tout traitement de données de santé. La désignation d'un **délégué à la protection des données (DPO)** est obligatoire pour les employeurs traitant régulièrement des données sensibles. Toute évolution des pratiques RH impliquant des données de santé doit être validée par le DPO et, en cas de doute, soumise à l'avis de la **CNPD**. L'utilisation abusive ou illicite expose l'employeur à des sanctions administratives et civiles.

Définition

Les **données de santé** désignent toute information relative à la santé physique ou mentale d'une personne identifiée ou identifiable. Cela inclut les données issues de la prestation de soins, les résultats d'examens médicaux, les diagnostics, ou toute information révélant l'état de santé.

Au Luxembourg, ces données sont qualifiées de **catégories particulières de données** (données sensibles) au sens de l'**article 9 du RGPD** et de la **loi modifiée du 1er août 2018** relative à la protection des personnes à l'égard du traitement des données à caractère personnel.

Leur traitement est **interdit par principe**, sauf exceptions limitativement énumérées par la loi. Toute manipulation de ces données doit respecter les principes de **licéité**, **loyauté**, **transparence** et **minimisation** des données.

Questions fréquentes

Comment sécuriser les données de santé en entreprise ?

Les données de santé doivent être conservées séparément des autres données RH dans des systèmes sécurisés avec accès restreints aux seules personnes habilitées. Il faut mettre en place une traçabilité complète des consultations, des mesures de sécurité techniques (chiffrement, contrôle d'accès) et des procédures internes documentées garantissant la confidentialité.

Quelles données de santé l'employeur peut-il traiter au Luxembourg ?

L'employeur luxembourgeois ne peut traiter des données de santé que dans des cas strictement encadrés : gestion des absences maladie (certificats médicaux), adaptation du poste de travail (avis du médecin du travail), respect des obligations de santé et sécurité au travail, et examens médicaux d'embauche et périodiques. Il ne peut jamais accéder aux diagnostics médicaux détaillés, seulement aux avis d'aptitude et certificats d'absence.

Qui peut accéder aux données médicales des salariés ?

Seuls le médecin du travail et les services de santé au travail sont habilités à accéder au dossier médical complet du salarié. Les responsables RH ne peuvent accéder qu'aux informations strictement nécessaires à leurs missions (avis d'aptitude, durée d'absence) dans les limites légales, jamais aux détails médicaux.

Une analyse d'impact est-elle obligatoire pour traiter des données de santé ?

Oui, il est fortement recommandé et souvent obligatoire de réaliser une analyse d'impact relative à la protection des données (AIPD) avant tout traitement de données de santé, conformément à l'article 35 du RGPD. La désignation d'un délégué à la protection des données (DPO) est également obligatoire pour les employeurs traitant régulièrement des données sensibles.

Conditions d’exercice

L'employeur luxembourgeois ne peut traiter des données de santé que dans des cas strictement encadrés par la loi. Le traitement est autorisé uniquement s'il est **nécessaire** pour remplir des **obligations légales** et exercer des **droits spécifiques** en matière de droit du travail, de sécurité sociale ou de protection sociale, conformément à l'**article 9(2)(b) du RGPD**.

Le **Code du travail luxembourgeois** impose des obligations à l'employeur en matière de santé et sécurité au travail, notamment via les services de santé au travail, sans pour autant lui donner accès aux données médicales détaillées des salariés.

L'accès aux données médicales doit être **strictement réservé** aux personnes légalement habilitées :

- Le **médecin du travail** détient et conserve le **dossier médical** du salarié
- Les **services de santé au travail** assurent le suivi médical et la prévention
- Les **responsables RH** ne peuvent accéder qu'aux informations nécessaires (avis d'aptitude, durée d'absence) dans les limites légales

L'**égalité de traitement**, la **non-discrimination** et la **confidentialité** doivent être garanties à chaque étape du traitement.

Modalités pratiques

L'intégration des données de santé dans une politique RH impose la mise en place de **procédures internes documentées**. La collecte doit être limitée à des finalités précises :

- Gestion des absences pour maladie (certificats médicaux)
- Adaptation du poste de travail (avis du médecin du travail)
- Respect des obligations en matière de santé et sécurité
- Examens médicaux d'embauche et périodiques (article L.326-1 du Code du travail)

Les données de santé doivent être **conservées séparément** des autres données RH, dans des **systèmes sécurisés** avec :

- Des **accès restreints** aux seules personnes habilitées
- Une **traçabilité complète** : toute consultation ou transmission doit être enregistrée
- Des **mesures de sécurité techniques et organisationnelles** (chiffrement, contrôle d'accès)

Les **durées de conservation** doivent être définies en fonction de la finalité du traitement. À titre d'exemple, le **Service de Santé au Travail (STM)** luxembourgeois conserve les dossiers médicaux pendant **40 ans**, conformément aux standards internationaux en matière de médecine du travail.

Les **salariés** doivent être informés :

- De la nature des données collectées et de la base légale
- Des finalités du traitement et des destinataires
- De leurs droits (accès, rectification, limitation) et des modalités d'exercice
- Des coordonnées du **DPO** pour toute question

Pratiques et recommandations

Il est **fortement recommandé** de réaliser une **analyse d'impact relative à la protection des données (AIPD)** avant tout traitement de données de santé, conformément à l'**article 35 du RGPD** et aux recommandations de la **CNPD**. La CNPD a publié une liste des traitements pour lesquels une AIPD est obligatoire, incluant les traitements de données de santé à grande échelle.

La politique RH doit prévoir une **information claire et accessible** des salariés sur :

- La nature des données collectées
- La base légale du traitement
- Les finalités poursuivies
- Les droits des personnes concernées

La désignation d'un **délégué à la protection des données (DPO)** est **obligatoire** pour les employeurs qui traitent régulièrement des données sensibles, conformément à l'**article 37 du RGPD** et à la loi du 1er août 2018. Le DPO doit :

- Contrôler le respect du RGPD
- Conseiller l'employeur sur les obligations légales
- Être le point de contact avec la CNPD
- Ses coordonnées doivent être communiquées à la CNPD

Bonnes pratiques opérationnelles :

- Limiter les demandes d'information sur l'état de santé au **strict nécessaire**
-

Documenter toute procédure impliquant des données de santé

- Consulter le **DPO** avant toute nouvelle procédure
- Former le personnel RH aux obligations de confidentialité
- Ne jamais exiger de diagnostic médical détaillé
- Se contenter des **avis d'aptitude** émis par le médecin du travail

En cas de doute sur la licéité d'un traitement, solliciter un **avis préalable de la CNPD** avant sa mise en œuvre.

Cadre juridique

Référence	Objet
Règlement (UE) 2016/679 (RGPD)	Article 9 : catégories particulières de données Article 35 : analyse d'impact (AIPD) Article 37 : délégué à la protection des données
Loi modifiée du 1er août 2018	Protection des personnes à l'égard du traitement des données à caractère personnel
Code du travail luxembourgeois	Article L.261-1 : traitement de données à des fins de surveillance Article L.321-1 et suivants : services de santé au travail Article L.326-1 : examen médical d'embauche Article L.326-3 : examens médicaux périodiques
Article 458 du Code pénal	Secret professionnel médical
Recommandations CNPD	Liste des traitements nécessitant une AIPD Lignes directrices concernant les DPO Décisions et délibérations
Conventions collectives sectorielles	Sous réserve de leur conformité à la législation nationale

L'utilisation abusive ou illicite de données de santé expose l'employeur à des **sanctions administratives** de la CNPD (amendes pouvant atteindre 20 millions d'euros ou 4% du chiffre d'affaires annuel mondial) et à des **actions en responsabilité civile**.

Il est **impératif** de garantir :

- La **confidentialité** : le secret médical s'impose à tous
- La **traçabilité** : journalisation de tous les accès
- La **limitation des accès** : seules les personnes habilitées
- L'**encadrement humain** : pas de décisions automatisées

Consulter **systématiquement le DPO** avant toute évolution des pratiques RH impliquant des données de santé. En cas de violation de données, l'employeur doit **notifier la CNPD** dans les 72 heures et, si nécessaire, informer les personnes concernées.