Quelles données de santé des salariés un outil d'IA peut-il traiter en entreprise ?

Réponse courte

Les données de santé des salariés bénéficient d'une **protection renforcée** au titre de l'article 9 du RGPD, qui interdit par principe leur traitement. Un outil d'IA ne peut traiter ces données que dans des cas **strictement limités** : obligation légale de l'employeur en matière de sécurité et santé au travail, médecine du travail, ou consentement explicite du salarié pour des finalités précises.

L'employeur ne peut pas utiliser l'IA pour **profiler** les salariés en fonction de leur état de santé, prédire les arrêts maladie ou évaluer la productivité sur la base de données médicales. L'AI Act classe tout système d'IA traitant des données de santé dans un contexte d'emploi parmi les niveaux de risque les plus élevés (Annexe III). Une AIPD est obligatoire et la CNPD doit être consultée en cas de risque résiduel élevé. Les sanctions peuvent atteindre **20 millions d'euros** ou 4 % du chiffre d'affaires mondial au titre du RGPD.

Définition

Les **données de santé** au sens du RGPD (article 4, paragraphe 15) sont les données à caractère personnel relatives à la santé physique ou mentale d'une personne, y compris la prestation de services de soins de santé, qui révèlent des informations sur l'état de santé de cette personne. Elles incluent les certificats médicaux, les résultats d'examens, les données biométriques liées à la santé et les informations sur les handicaps.

Dans le contexte professionnel, ces données sont traitées par le **médecin du travail**, les organismes de sécurité sociale et, de manière très limitée, par l'employeur pour ses obligations légales. L'utilisation de l'IA pour traiter ces données ajoute un niveau de risque supplémentaire qui justifie des protections renforcées.

Conditions d’exercice

Le traitement de données de santé par un outil d'IA en entreprise est soumis à des conditions cumulatives strictes.

Critère	Détail
Interdiction de principe	Le traitement des données de santé est interdit (article 9, paragraphe 1, RGPD) sauf exceptions limitatives
Exceptions autorisées	Obligations de l'employeur en santé-sécurité (art. L.312-1), médecine du travail, consentement explicite du salarié, intérêt vital
Finalité strictement limitée	Le traitement doit être nécessaire à la finalité invoquée ; aucune utilisation secondaire non autorisée
Minimisation	Seules les données de santé strictement nécessaires peuvent être traitées ; principe du moindre accès
AIPD obligatoire	Analyse d'impact relative à la protection des données obligatoire avant tout traitement de données de santé par IA (art. 35 RGPD)
AI Act - Haut risque	Systèmes d'IA traitant des données de santé en contexte d'emploi classés à haut risque (Annexe III)
Accès restreint	Données de santé accessibles uniquement au médecin du travail et aux personnes habilitées ; secret professionnel
Interdictions absolues	Profilage de santé, prédiction d'arrêts maladie, scoring de santé pour évaluation, discrimination basée sur l'état de santé

Modalités pratiques

Le déploiement d'un outil d'IA traitant des données de santé doit suivre un processus rigoureux.

Étape	Détail
Évaluation de la nécessité	Vérifier qu'il est indispensable de traiter des données de santé et qu'aucune alternative moins intrusive n'existe
Base légale	Identifier et documenter la base légale du traitement : obligation légale, consentement explicite ou intérêt vital
AIPD	Réaliser une analyse d'impact détaillée, consulter la CNPD si le risque résiduel reste élevé
Mesures techniques	Pseudonymisation ou anonymisation des données, chiffrement renforcé, cloisonnement des accès, journalisation
Information du salarié	Information complète sur les données traitées, les finalités, les destinataires, les droits (accès, rectification, opposition)
Audit et contrôle	Vérification régulière de la conformité, audits de sécurité, tests de biais sur les données de santé

Pratiques et recommandations

Éviter autant que possible le traitement de données de santé par l'IA en privilégiant des traitements agrégés et anonymisés qui ne permettent pas l'identification individuelle des salariés.

Cloisonner strictement les données de santé des autres données RH en utilisant des systèmes séparés avec des droits d'accès différenciés et une journalisation complète.

Consulter le médecin du travail et le DPO avant tout projet de traitement de données de santé par l'IA, pour valider la nécessité et les mesures de protection.

Interdire formellement dans la charte IA de l'entreprise l'utilisation de données de santé à des fins de profilage, de scoring ou de prédiction comportementale des salariés.

Sensibiliser les managers au caractère strictement confidentiel des données de santé et à l'interdiction de demander des informations médicales détaillées aux salariés pour alimenter un outil d'IA.

Cadre juridique

Référence	Objet
RGPD - Article 9	Interdiction de principe du traitement des données de santé, exceptions limitatives
RGPD - Article 4, paragraphe 15	Définition des données concernant la santé
RGPD - Article 35	Analyse d'impact obligatoire pour les traitements de données de santé à grande échelle
RGPD - Article 36	Consultation préalable de la CNPD en cas de risque résiduel élevé
AI Act (UE 2024/1689) - Annexe III	Classification à haut risque des systèmes d'IA traitant des données de santé en contexte d'emploi
Art. L.312-1	Obligation de l'employeur en matière de sécurité et santé au travail
Art. L.326-1 et suivants	Service de santé au travail, missions du médecin du travail
Art. L.251-1	Interdiction de toute discrimination fondée sur l'état de santé

Le traitement de données de santé par l'IA constitue l'un des domaines les plus sensibles du droit du numérique. Les entreprises luxembourgeoises doivent adopter une posture de prudence maximale en limitant ces traitements au strict nécessaire et en mettant en place des mesures de sécurité renforcées. Les sanctions RGPD pour violation de l'article 9 sont parmi les plus sévères.

Les contenus sont rédigés et mis à jour régulièrement à partir de sources officielles. Leur usage ne remplace pas une consultation juridique et doit être validé par un professionnel du droit.