Comment protéger concrètement les documents confidentiels d'un service RH ?

Réponse courte

Par des mesures **adaptées au risque**, seule exigence que pose l'article 32 du RGPD. Le texte ne dresse aucune liste : il impose de tenir compte de l'état des connaissances, des coûts, de la nature des données et de la gravité des conséquences pour les personnes.

Trois familles de mesures répondent à la quasi-totalité des situations. Les mesures **organisationnelles** — habilitations par fonction, engagement de confidentialité, procédure de retrait des accès. Les mesures **techniques** — cloisonnement des données sensibles, chiffrement des supports mobiles, journalisation des consultations. Les mesures **physiques**, régulièrement oubliées : armoires fermées, locaux d'archives contrôlés, destruction sécurisée.

Le critère est celui de la gravité : les données de santé, dont le traitement est interdit par principe hors exceptions, appellent une protection renforcée par rapport à un fichier d'adresses.

Définition

La **confidentialité** n'est pas une catégorie juridique en soi : c'est l'un des objectifs de la sécurité du traitement, aux côtés de l'intégrité et de la disponibilité.

Les **mesures techniques et organisationnelles appropriées** sont l'expression retenue par le RGPD. Elle signifie que la conformité ne se démontre pas par un référentiel, mais par la cohérence entre le risque encouru et les moyens déployés.

Conditions d’exercice

Le niveau de protection se règle sur la donnée la plus sensible du dossier, non sur la moyenne.

© 2026 www.pixie.lu · IA/RH spécialisée en droit du travail luxembourgeois

Catégorie de données	Niveau de protection	Motif
Données de santé, certificats médicaux	Renforcé : cloisonnement et accès nominatif	RGPD, article 9
Données de rémunération	Élevé : accès limité au service du personnel et à la paie	Sensibilité pratique et risque de conflit
Évaluations et procédures disciplinaires	Élevé : accès restreint et journalisé	Conséquences pour la personne
Coordonnées et données administratives	Standard	Risque limité
Données de surveillance	Selon la finalité annoncée	L.261-1
Archives papier	Locaux fermés et accès tracé	Souvent le maillon faible

Modalités pratiques

La sécurité se démontre par des mesures écrites et appliquées, pas par des intentions.

Mesure	Mise en œuvre
Habilitations	Matrice fonction / catégorie, revue au moins une fois par an
Engagement de confidentialité	Signé par les personnes ayant accès aux données sensibles
Cloisonnement	Séparer les données de santé du reste du dossier
Supports mobiles	Chiffrer les ordinateurs portables et les supports amovibles
Journalisation	Enregistrer les consultations sur les catégories sensibles
Archives physiques	Locaux fermés, registre d'accès, destruction par prestataire avec attestation

Pratiques et recommandations

Le papier reste le point faible de la plupart des services. Les mesures se concentrent sur les applications, tandis que les dossiers les plus anciens dorment dans des armoires ouvertes, sans inventaire ni durée de conservation. Une revue des archives physiques apporte davantage que le renforcement d'un mot de passe.

Le cloisonnement des données de santé est la mesure la plus rentable en droit. Elle limite le risque de traitement illicite, facilite la purge, et se démontre immédiatement lors d'un contrôle — trois effets pour une réorganisation de classement.

© 2026 www.pixie.lu · IA/RH spécialisée en droit du travail luxembourgeois

La sécurité s'apprécie aussi à la sortie. Le départ d'un membre du service du personnel suppose le retrait de ses accès, la restitution des supports et, le cas échéant, la vérification des copies locales. C'est au moment des mouvements que les fuites se produisent, rarement au quotidien.

Cadre juridique

Référence	Objet
RGPD, article 32	Mesures techniques et organisationnelles appropriées au risque
RGPD, article 9	Interdiction de principe du traitement des données de santé
RGPD, article 5, paragraphe 1, point f)	Intégrité et confidentialité des données
RGPD, articles 33 et 34	Notification des violations de données
RGPD, article 28	Encadrement des sous-traitants ayant accès aux données
Article L.261-1 du Code du travail	Information préalable pour les traitements à des fins de surveillance

L'article 32 n'impose aucune liste : il impose une cohérence entre le risque et les moyens. Cloisonnez les données de santé et traitez les archives papier, qui concentrent le risque tout en échappant à la plupart des politiques de sécurité.

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.