Quelles précautions prendre en cas de sous-traitance du traitement des données RH ?

Réponse courte

La sous-traitance d'un traitement de données RH (paie, SIRH, gestion des temps, santé au travail) impose à l'employeur, en sa qualité de **responsable de traitement**, de **sélectionner** un prestataire offrant des **garanties suffisantes** en matière de protection des données et de **signer** un **contrat conforme à l'article 28 du RGPD**.

L'employeur doit **vérifier** les mesures techniques et organisationnelles du sous-traitant, **encadrer** par écrit les conditions du traitement (finalité, durée, instructions, confidentialité, sécurité), **interdire** toute sous-traitance en chaîne sans autorisation écrite préalable, et **auditer** régulièrement la conformité du prestataire. À l'issue du contrat, les données doivent être **restituées** ou **supprimées** de manière certifiée.

Définition

La **sous-traitance** au sens du RGPD désigne le fait pour un responsable de traitement de confier à un tiers l'exécution d'opérations de traitement pour son compte. Le sous-traitant n'agit que sur **instructions documentées** du responsable et engage sa propre responsabilité en cas de manquement, aux côtés de celle du responsable.

Questions fréquentes

Comment gérer une violation de données par un sous-traitant ?

Le contrat doit prévoir la notification immédiate par le sous-traitant à l'employeur en cas de violation. L'employeur doit alors notifier la CNPD dans les 72 heures conformément à l'article 33 du RGPD si la violation présente un risque.

L'employeur reste-t-il responsable des manquements du sous-traitant ?

Oui, l'employeur reste responsable vis-à-vis de ses salariés et de la CNPD des manquements de son sous-traitant. Un contrat non conforme à l'article 28 expose à des sanctions pouvant atteindre 10 millions d'euros ou 2 % du chiffre d'affaires.

Le sous-traitant peut-il sous-traiter à son tour ?

Non, sans autorisation écrite préalable de l'employeur. Toute sous-traitance ultérieure doit être autorisée par le responsable de traitement et soumise aux mêmes obligations RGPD que le contrat initial, conformément à l'article 28.2 du règlement.

Qu'impose l'article 28 du RGPD au sous-traitant ?

L'article 28 du RGPD impose un contrat écrit définissant la finalité, la durée, les instructions documentées du responsable, la confidentialité, la sécurité, l'autorisation préalable de sous-traitance ultérieure et la restitution ou destruction des données en fin de contrat.

Quelles précautions prendre lors d'une sous-traitance RGPD ?

L'employeur doit sélectionner un prestataire offrant des garanties suffisantes, signer un contrat conforme à l'article 28 du RGPD, vérifier les mesures de sécurité, interdire la sous-traitance en chaîne sans autorisation écrite et auditer régulièrement le prestataire.

Quels prestataires RH critiques nécessitent un audit annuel ?

Un audit annuel est recommandé pour les sous-traitants critiques : prestataire de paie, SIRH, santé au travail. Cet audit vérifie le respect continu des engagements contractuels et la pertinence des mesures techniques et organisationnelles de sécurité.

Conditions d’exercice

L'employeur doit choisir un prestataire offrant des garanties RGPD documentées, signer un contrat article 28 avant tout traitement, et conserver un droit d'audit ainsi qu'une obligation de restitution des données en fin de contrat.

Condition	Détail
Sélection du prestataire	Garanties suffisantes de conformité RGPD documentées
Contrat écrit	Accord conforme à l'article 28 RGPD signé avant tout traitement
Instructions documentées	Le sous-traitant n'agit que sur demande écrite
Confidentialité	Engagement du sous-traitant et de son personnel
Sécurité	Mesures techniques et organisationnelles appropriées
Sous-traitance ultérieure	Autorisation écrite préalable obligatoire
Audit	Droit de contrôle du responsable sur le sous-traitant
Fin du contrat	Restitution ou destruction certifiée des données

Modalités pratiques

Le cycle de vie d'une sous-traitance RH comporte sept étapes : due diligence préalable, rédaction d'un contrat article 28 RGPD, onboarding sécurisé, suivi opérationnel, audits périodiques, gestion des incidents (art. 33 RGPD) et clôture avec restitution ou destruction certifiée.

Étape	Détail
Due diligence	Analyse préalable des garanties techniques et organisationnelles
Rédaction du contrat	Clauses RGPD obligatoires, annexes de sécurité
Onboarding	Transfert sécurisé des données et formation
Suivi opérationnel	Monitoring des accès et des incidents
Audits périodiques	Vérification du respect des engagements
Gestion des incidents	Notification des violations dans les meilleurs délais
Clôture	Restitution ou destruction certifiée, attestation écrite

Pratiques et recommandations

Établir une grille d'évaluation préalable des prestataires pour vérifier leurs garanties de conformité RGPD avant toute contractualisation.

Utiliser un modèle de contrat type intégrant toutes les clauses obligatoires de l'article 28 du RGPD, validé par le DPO et le service juridique.

Maintenir une liste à jour des sous-traitants dans le registre des activités de traitement, accessible à la CNPD en cas de contrôle.

Auditer annuellement les sous-traitants critiques (paie, SIRH, santé) pour vérifier le respect continu des engagements contractuels et des mesures de sécurité.

Prévoir contractuellement la gestion des violations de données et les modalités de notification à l'employeur dans les meilleurs délais.

Cadre juridique

Le cadre juridique repose sur le RGPD et la loi luxembourgeoise.

Référence	Objet
Art. 28 RGPD	Obligations contractuelles du responsable et du sous-traitant
Art. 29 RGPD	Traitement sur instructions du responsable
Art. 32 RGPD	Sécurité du traitement
Art. 33 RGPD	Notification des violations
Loi du 1er août 2018	Régime général au Luxembourg
Clauses contractuelles types	Décision 2021/915 de la Commission européenne
Art. L.261-1 Code du travail	Protection dans la relation de travail

L'employeur reste **responsable** vis-à-vis de ses salariés et de la CNPD des manquements de son sous-traitant. Un contrat non conforme à l'article 28 expose à des **sanctions administratives** pouvant atteindre 10 millions d'euros ou 2 % du chiffre d'affaires mondial.