SIRH cloud ou on-premise au Luxembourg : quelles différences pour l'employeur ?

Réponse courte

Le choix entre un **SIRH en cloud** (SaaS) et un **SIRH on-premise** hébergé sur ses propres serveurs est une décision de gestion qui engage l'employeur sur plusieurs dimensions : sécurité, coût, conformité RGPD et capacité de maintenance.

Les **deux modèles sont valables** — c'est le résultat qui compte : les obligations de l'employeur en matière de registre du personnel, de conservation des documents et de protection des données doivent être remplies quel que soit le mode d'hébergement choisi.

En pratique, le choix entre SIRH cloud et on-premise au Luxembourg est principalement guidé par les exigences du **RGPD** (Règlement UE 2016/679) et de la **loi du 1er août 2018**.

Un SIRH cloud implique un transfert de données vers un prestataire externe, ce qui oblige l'employeur à vérifier la localisation des serveurs au regard du RGPD (idéalement dans l'UE), à conclure un **contrat de sous-traitance** conforme à l'article 28 du RGPD et à s'assurer que le prestataire offre des garanties suffisantes de sécurité.

Un SIRH on-premise conserve les données en interne mais impose à l'employeur d'assurer lui-même la sécurité, les sauvegardes et la conformité technique.

Définition

Un **SIRH cloud** (ou SaaS — Software as à Service) est un logiciel de gestion RH hébergé sur les serveurs d'un prestataire externe et accessible via internet. L'employeur paie un abonnement et n'a pas à gérer l'infrastructure technique.

Un **SIRH on-premise** est installé sur les serveurs propres de l'entreprise, sous sa responsabilité technique complète. Le mode **hybride** combine les deux approches, avec certains modules en cloud et d'autres en local.

La tendance du marché luxembourgeois est clairement orientée vers le cloud : la majorité des nouveaux déploiements SIRH se font en mode SaaS, en particulier dans les PME qui ne disposent pas d'une infrastructure informatique dédiée. Les entreprises du secteur financier, soumises à des exigences réglementaires supplémentaires de la **CSSF** en matière d'externalisation, doivent cependant évaluer plus attentivement les risques liés au cloud, même si ces exigences concernent davantage les données clients que les données RH.

Vous cherchez un SIRH adapté au Luxembourg ? myHR centralise vos processus RH dans une solution Made In Luxembourg. Demander une démo ?

Conditions d’exercice

Le choix du mode d'hébergement dépend de critères juridiques et opérationnels.

Critère	Cloud (SaaS)	On-premise
Obligation légale	Aucune interdiction	Aucune obligation
Localisation des données	Vérifier que les serveurs sont dans l'UE (RGPD)	Données sur site, pas de transfert
Contrat de sous-traitance	Obligatoire (art. 28 RGPD)	Non applicable
Responsabilité sécurité	Partagée entre employeur et prestataire	Entièrement à charge de l'employeur
Mises à jour légales	Assurées par l'éditeur (SSM, index, cotisations)	À charge de l'employeur ou de son prestataire
Coût initial	Faible (abonnement mensuel)	Élevé (licence, serveurs, maintenance)
Accessibilité	Depuis tout appareil connecté	Généralement limité au réseau interne

Modalités pratiques

La mise en place d'un SIRH cloud ou on-premise au Luxembourg implique des démarches spécifiques, organisées en étapes.

1. Réalisation de l'analyse d'impact (AIPD)

Conduire une analyse d'impact relative à la protection des données lorsque le traitement est à grande échelle ou porte sur des données sensibles, conformément à l'article 35 du RGPD.

La CNPD recommande cette démarche pour tout SIRH traitant les données de plus de 250 salariés. L'AIPD identifie les risques liés au mode d'hébergement choisi et les mesures d'atténuation à mettre en place. Elle doit être documentée et mise à jour en cas de changement significatif.

2. Négociation du contrat de sous-traitance (cloud)

Exiger un contrat conforme à l'article 28 du RGPD avec le prestataire cloud, précisant les mesures de sécurité techniques et organisationnelles, la localisation exacte des serveurs, les conditions de restitution des données en fin de contrat, les obligations de notification en cas de violation et le droit d'audit de l'employeur.

Ce contrat doit être distinct des conditions générales de vente et négocié spécifiquement pour les besoins de l'entreprise.

3. Vérification de la localisation des serveurs (cloud)

Privilégier un hébergement dans l'UE où l'EEE. Si le prestataire utilise des serveurs situés hors de cet espace, vérifier l'existence de garanties suffisantes : décision d'adéquation de la Commission européenne pour le pays concerné, ou mise en place de clauses contractuelles types conformes au RGPD.

Les transferts vers les États-Unis nécessitent une attention particulière depuis l'invalidation du Privacy Shield et sa remplacement par le Data Privacy Framework.

4. Mise en place du plan de sauvegarde et de reprise (on-premise)

Configurer des sauvegardes quotidiennes sur des supports distincts et géographiquement séparés. Définir un plan de reprise d'activité (PRA) avec un objectif de temps de reprise (RTO) et un objectif de point de reprise (RPO) compatibles avec les obligations légales de l'employeur. Tester régulièrement la procédure de restauration pour garantir son efficacité en cas de sinistre.

5. Documentation dans le registre des traitements

Mentionner le choix d'hébergement, l'identité du sous-traitant cloud le cas échéant, la localisation des serveurs et les mesures de sécurité dans le registre des activités de traitement (article 30 du RGPD). Ce registre est obligatoire pour les entreprises de 250 salariés et plus, et recommandé pour toutes les autres.

6. Information et formation des utilisateurs

Informer les salariés du traitement de leurs données conformément aux articles 13 et 14 du RGPD, en précisant l'identité du prestataire cloud et la localisation des serveurs. Former les gestionnaires RH à l'utilisation sécurisée de l'outil choisi, en particulier pour le cloud : bonnes pratiques d'authentification, gestion des mots de passe, signalement des incidents de sécurité.

Pratiques et recommandations

Vérifier la localisation exacte des serveurs du prestataire cloud avant toute signature de contrat, car un hébergement hors UE complique significativement la conformité RGPD.

Exiger un contrat de sous-traitance conforme à l'article 28 du RGPD, précisant les mesures de sécurité, la localisation des données, les conditions de restitution et les obligations de notification en cas de violation.

Évaluer la capacité du prestataire cloud à intégrer rapidement les évolutions législatives luxembourgeoises (adaptation du SSM, indexation des salaires, modifications des taux de cotisation CCSS), en tenant compte des critères de sélection d'un SIRH adaptés au marché local.

Prévoir une clause de réversibilité dans le contrat cloud, permettant de récupérer l'intégralité des données dans un format exploitable en cas de changement de prestataire ou de retour à un hébergement interne.

Documenter le choix d'hébergement dans le registre des traitements de l'entreprise et informer les salariés du traitement de leurs données conformément aux articles 13 et 14 du RGPD.

Cadre juridique

Référence	Objet
RGPD (Règlement UE 2016/679), art. 28	Obligations du sous-traitant de données
RGPD, art. 30	Registre des activités de traitement
RGPD, art. 44-49	Transferts de données hors UE
Loi du 1er août 2018	Transposition nationale du RGPD

Le choix entre cloud et on-premise est une décision de gestion, pas une obligation légale. L'employeur doit simplement s'assurer que ses obligations légales sont remplies et que les données des salariés sont protégées conformément au RGPD, quel que soit le mode d'hébergement retenu.