



[Accueil](#) / [Blogue](#)

Comment Assurer la Conformité de votre Système NetSuite au RGPD

15 novembre 2024

Avec le RGPD (Règlement Général sur la Protection des Données) en vigueur, les organisations opérant au sein de l'Union européenne (UE) ou manipulant les données de résidents de l'UE doivent suivre des réglementations strictes pour protéger les informations personnelles. Si votre organisation utilise NetSuite, comprendre comment rendre le système conforme au RGPD est essentiel pour éviter les amendes, établir la confiance et protéger les données de vos clients. Ce guide décrit les étapes nécessaires pour assurer la conformité au RGPD dans NetSuite.

Ce que le RGPD signifie pour votre système NetSuite

Le RGPD, en vigueur depuis mai 2018, est un règlement complet visant à protéger les données personnelles des individus. Il impose aux organisations de :

- Obtenir un consentement clair pour la collecte et l'utilisation des données.
- Assurer la transparence et la responsabilité des données.
- Fournir aux individus le droit d'accéder, de corriger et de supprimer leurs données.
- Signaler toute violation de données dans un délai de 72 heures.

Le non-respect peut entraîner des amendes atteignant jusqu'à 4 % du chiffre d'affaires annuel mondial de l'entreprise, ce qui rend l'adhérence essentielle. NetSuite peut soutenir la conformité au RGPD, mais nécessite une configuration minutieuse et une gestion continue pour respecter les normes.

1. Cartographier le Flux et le Stockage des Données

Commencez par comprendre comment votre instance NetSuite collecte, stocke et transfère les données personnelles. Vous aurez besoin d'une carte claire pour documenter tous les points de contact des données.

- **Identifiez toutes les sources de données personnelles** : Incluez les formulaires de site web, les données de vente, les interactions du service client et toutes les intégrations tierces.
- **Documentez comment les données circulent dans NetSuite** : Cartographiez où les données personnelles sont stockées dans NetSuite, comme les enregistrements clients, les données de vente et les journaux de support client.
- **Évaluez les connexions tierces** : Assurez-vous que tout système tiers intégré à NetSuite respecte également le RGPD.

Un examen régulier des flux de données vous garantit de capturer chaque source de données et de la gérer conformément aux exigences du RGPD.

2. Mettre en Place la Minimisation des Données et le Contrôle d'Accès

Le RGPD impose la minimisation des données, ce qui signifie ne collecter que les informations nécessaires pour des finalités spécifiques et légitimes.

- **Restreignez les champs de collecte de données** : Évitez de collecter des données au-delà de ce qui est nécessaire. Dans NetSuite, vous pouvez

personnaliser les champs et restreindre les données collectées dans les formulaires.

- **Limitez l'accès aux données sensibles** : Configurez des permissions basées sur les rôles dans NetSuite pour contrôler quels employés peuvent accéder aux données personnelles.
- **Effectuez des audits réguliers d'accès** : Menez des examens périodiques des permissions d'accès pour garantir la conformité lorsque les rôles changent ou que de nouvelles données sont introduites.

La minimisation des données réduit le risque d'utilisation abusive et limite l'exposition potentielle en cas de violation.

3. Obtenir et Documenter Correctement le Consentement

La gestion du consentement est l'un des éléments clés du RGPD. Les clients doivent fournir un consentement clair et explicite pour que leurs données soient collectées et traitées.

- **Configurez des champs de consentement dans NetSuite** : Ajoutez des champs spécifiques dans les enregistrements NetSuite qui documentent le consentement, y compris des cases à cocher qui enregistrent les dates et types de consentement.
- **Créez des formulaires de consentement clairs et sans ambiguïté** : Si vous collectez le consentement via des formulaires intégrés à NetSuite, assurez-vous que le langage est clair, expliquant pourquoi les données sont collectées et comment elles seront utilisées.
- **Suivez la révocation du consentement** : Le RGPD exige que les utilisateurs puissent retirer leur consentement à tout moment. NetSuite peut gérer cela en permettant des mises à jour des enregistrements clients en cas de révocation de consentement.

Avec une documentation appropriée, vous disposerez d'une piste d'audit montrant que vous avez respecté les exigences de consentement du RGPD.

4. Activer la Portabilité des Données et les Droits d'Accès

Le RGPD accorde aux individus le droit d'accéder à leurs données et de demander leur transfert à une autre entité. Pour implémenter ces droits dans NetSuite, suivez ces étapes :

- **Créez des outils d'exportation de données accessibles** Utilisez les fonctions d'exportation de NetSuite pour fournir des données dans un format couramment utilisé (ex : CSV ou Excel).
- **Permettez un accès aux données à la demande** : Configurez NetSuite pour générer des rapports montrant aux utilisateurs les données personnelles stockées à leur sujet.
- **Automatisez les réponses aux demandes de données** : Mettez en place des workflows pour simplifier le traitement de ces demandes, assurant des réponses en temps opportun dans le respect du délai de 30 jours du RGPD.

Ces actions vous permettront de répondre efficacement aux demandes de portabilité des données, aidant vos clients à garder le contrôle sur leurs informations.

5. Désigner un Délégué à la Protection des Données (DPO) pour la Supervision

Un Délégué à la Protection des Données (DPO) aide à garantir que votre organisation respecte le RGPD. Bien que toutes les entreprises n'en aient pas besoin, celles traitant des données personnelles de manière extensive ou opérant dans l'UE devraient envisager ce rôle.

- **Assignez un DPO ou un responsable de la confidentialité** : Le DPO ou un responsable désigné doit superviser les efforts de conformité, y compris les audits, les mises à jour des politiques et la formation.
- **Menez des sessions de formation régulières** : Votre DPO ou responsable de la confidentialité peut organiser des sessions pour les employés, en particulier ceux qui traitent directement des données personnelles.
- **Surveillez la conformité** : Le DPO doit évaluer régulièrement la conformité, rester informé des modifications du RGPD et affiner les politiques au besoin.

Un responsable dédié garantit qu'il y a une personne axée sur le maintien des normes de conformité et l'éducation de l'équipe.

6. Activer les Procédures de "Droit à l'Oubli"

Le RGPD donne aux individus le droit de demander la suppression de leurs données dans certaines circonstances, appelé "Droit à l'Oubli". NetSuite peut faciliter cela, mais nécessite des configurations spécifiques.

- **Développez des workflows pour la suppression des données** : Utilisez les workflows de NetSuite pour standardiser le processus de suppression, en supprimant les données personnelles de toutes les zones concernées lorsqu'une demande est soumise.
- **Assurez-vous de la suppression des sauvegardes** : Confirmez que les données supprimées ne restent pas dans les sauvegardes ou archives au-delà de la période de rétention nécessaire.
- **Documentez la suppression des données** : Enregistrez chaque suppression pour démontrer la conformité au RGPD, en notant quand, pourquoi et comment les données ont été effacées.

Des procédures claires de suppression des données garantissent que les demandes sont remplies avec précision, minimisant le risque de conservation de données indésirables.

7. Configurer la Détection et le Signalement des Violations

Le RGPD exige que les entreprises signalent toute violation de données impliquant des informations personnelles dans les 72 heures suivant sa découverte.

- **Mettez en place des alertes pour les activités inhabituelles** : Utilisez les options de personnalisation de NetSuite pour configurer des alertes en cas d'accès ou de modification de données inhabituels.
- **Développez un processus de notification de violation** : Définissez les étapes que votre équipe doit suivre en cas de violation, garantissant une notification et une réponse rapides.
- **Préparez des notifications pré-rédigées** : Pour une réponse rapide, ayez des notifications pré-approuvées prêtes en cas de violation, détaillant le type de données affectées et les étapes de remédiation.

Une stratégie de réponse aux violations bien planifiée permet à votre équipe d'agir rapidement en cas d'incident de sécurité, minimisant les risques et assurant la conformité.

8. Mettre à Jour et Auditer Régulièrement vos Pratiques de Confidentialité

La conformité n'est pas un événement ponctuel ; c'est un processus continu. Le RGPD exige de revoir et de mettre à jour les pratiques de confidentialité en permanence.

- **Planifiez des audits périodiques** : Menez des audits réguliers des configurations, workflows et permissions de NetSuite pour garantir qu'ils respectent les normes actuelles du RGPD.
- **Examinez les politiques de consentement et de conservation des données** : Les politiques de confidentialité doivent refléter les pratiques actuelles et être révisées chaque année ou chaque fois que des changements importants surviennent.
- **Restez informé des mises à jour du RGPD** : Suivez les modifications réglementaires susceptibles d'affecter la gestion des données dans NetSuite.

Des mises à jour régulières de votre système garantissent que les nouveaux risques sont traités rapidement et que la configuration de NetSuite est conforme aux dernières exigences en matière de conformité.

Conclusion

Maintenir la conformité au RGPD dans votre système NetSuite nécessite un effort constant et une planification minutieuse. En cartographiant les flux de données, en gérant le consentement, en automatisant les droits de données et en développant un plan de réponse aux violations solide, vous pouvez protéger votre organisation contre les amendes potentielles et établir une relation de confiance avec vos clients. Rappelez-vous que la conformité au RGPD n'est pas une tâche unique, mais un engagement continu envers la confidentialité et la sécurité des données.