HOUSEBLEND

Comment s'assurer que votre système NetSuite est conforme au RGPD

15 novembre 2024

Avec le RGPD (Règlement Général sur la Protection des Données) en place, les organisations opérant au sein de l'Union européenne (UE) ou traitant des 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, bâtir la confiance et protéger les données de vos clients. Ce guide vous accompagne à travers les étapes nécessaires pour assurer la conformité au RGPD dans NetSuite. Pour des informations complètes sur les principes de conformité au RGPD, lisez notre guide détaillé sur **les principes et droits de conformité au RGPD dans NetSuite**.

Ce que le RGPD signifie pour votre système NetSuite

Le RGPD, en vigueur depuis mai 2018, est une réglementation complète conçue pour protéger les données personnelles des individus. Il exige que les organisations :

- Obtiennent un consentement clair pour la collecte et l'utilisation des données.
- Assurent la transparence et la responsabilité des données.
- Fournissent aux personnes concernées le droit d'accéder, de corriger et de supprimer leurs données.
- Signalent toute violation de données dans les 72 heures.

Le non-respect peut entraîner des pénalités allant jusqu'à 4 % du chiffre d'affaires annuel mondial de l'entreprise, donc l'adhésion est essentielle. NetSuite peut soutenir la conformité au RGPD, mais cela nécessite une configuration soigneuse et une gestion continue pour répondre aux 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.

- **Identifier toutes les sources de données personnelles** - Incluez les formulaires du site web, les données de vente, les interactions du service client et toutes les intégrations tierces.
- **Documenter comment les données circulent dans NetSuite** - Cartographiez où les données personnelles sont stockées dans NetSuite, comme les dossiers clients, les données de vente et les journaux de support client.
- **Évaluer les connexions tierces** - Assurez-vous que tout système tiers intégré à NetSuite a ses propres pratiques conformes au RGPD.

Examiner régulièrement le flux de données garantit que vous capturez chaque source de données et que vous la gérez conformément aux exigences du RGPD.

2. Mettre en œuvre la minimisation des données et les contrôles d'accès

Le RGPD exige la minimisation des données, ce qui signifie ne collecter que les données nécessaires à des fins spécifiques et légitimes.

- **Restreindre les champs de collecte de données** - Évitez de capturer des données au-delà de ce qui est nécessaire. Dans NetSuite, vous pouvez personnaliser les champs et restreindre les données collectées dans les formulaires.
- **Limiter l'accès aux données sensibles** - Définissez des permissions basées sur les rôles dans NetSuite pour contrôler quels employés peuvent accéder aux données personnelles. N'accordez l'accès qu'à ceux qui en ont besoin pour exercer leur rôle.

- **Auditer régulièrement l'accès** - Effectuez des examens périodiques des permissions d'accès pour assurer la conformité à mesure que 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 composants critiques du RGPD. Les clients doivent fournir un consentement clair et explicite pour que leurs données soient collectées et traitées.

- **Configurer des champs de consentement dans NetSuite** - Ajoutez des champs spécifiques dans les enregistrements NetSuite qui documentent le consentement. Cela peut inclure des cases à cocher qui enregistrent les dates et les types de consentement.
- **Créer 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 simple, expliquant pourquoi les données sont collectées et comment elles seront utilisées.
- **Suivre la révocation du consentement** - Le RGPD exige que les utilisateurs puissent retirer leur consentement à tout moment. NetSuite peut gérer cela en permettant les mises à jour des dossiers clients si un utilisateur retire son consentement.

Avec une documentation appropriée, vous aurez 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. La mise en œuvre de la portabilité des données et des droits d'accès dans NetSuite nécessite les étapes suivantes :

- **Créer des outils d'export de données accessibles** - Utilisez les fonctions d'export de NetSuite pour fournir des données dans un format couramment utilisé (ex. : CSV ou Excel). Cela rend le transfert de données transparent.
- **Permettre l'accès aux données à la demande** - Configurez NetSuite pour générer des rapports qui montrent aux utilisateurs les données personnelles stockées les concernant.
- **Automatiser les réponses aux demandes de données** - Configurez des workflows pour rationaliser le traitement de ces demandes, assurant des

réponses dans le 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 données.

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 est conforme au RGPD. Bien que toutes les entreprises n'aient pas besoin d'un DPO, celles qui traitent des données personnelles étendues ou opèrent au sein de l'UE devraient envisager ce rôle.

- **Assigner un DPO ou un responsable de la confidentialité** - Le DPO ou un responsable de la confidentialité désigné devrait superviser les efforts de conformité, y compris les audits, les mises à jour des politiques et la formation.
- **Organiser des sessions de formation régulières** - Votre DPO ou responsable de la confidentialité peut organiser des sessions pour les employés, particulièrement pour ceux qui manipulent directement des données personnelles.
- **Surveiller la conformité** - Le DPO devrait évaluer régulièrement la conformité, rester informé des amendements du RGPD et affiner les politiques si nécessaire.

Avoir un responsable dédié aide à garantir qu'il y a quelqu'un concentré sur le maintien des normes de conformité et l'éducation de l'équipe.

6. Activer les procédures du « Droit à l'oubli »

Le RGPD donne aux individus le droit de demander la suppression de leurs données dans certaines circonstances, connu sous le nom de « Droit à l'oubli ». NetSuite peut faciliter cela, mais cela nécessite des configurations spécifiques.

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

Des procédures claires pour la suppression des données garantissent que les demandes sont satisfaites avec précision, minimisant le risque de conserver des données non désirées.

7. Configurer la détection et le signalement des violations

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

- **Mettre en place des alertes pour les activités inhabituelles** - Utilisez les options de personnalisation de NetSuite pour configurer des alertes pour les accès ou modifications de données inhabituels.
- **Développer un processus de notification de violation** - Décrivez les étapes que votre équipe doit suivre si une violation se produit, assurant une notification et une réponse rapides.
- **Préparer des notifications pré-rédigées** - Pour une réponse plus rapide, ayez des notifications pré-approuvées prêtes en cas de violation, détaillant le type de données affectées et les mesures correctives.

Une stratégie de réponse aux violations bien planifiée garantit que votre équipe peut agir rapidement si un incident de sécurité se produit, 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 que vous examiniez et mettiez à jour continuellement les pratiques de confidentialité.

- **Planifier des audits périodiques** - Effectuez des audits de routine des configurations NetSuite, des workflows et des permissions pour vous assurer qu'ils répondent aux normes actuelles du RGPD.
- **Examiner les politiques de consentement et de rétention des données** - Les politiques de confidentialité devraient refléter les pratiques de données actuelles et être examinées annuellement ou chaque fois que des changements significatifs se produisent.
- **Rester informé des mises à jour du RGPD** - Suivez tout changement réglementaire qui pourrait affecter la façon dont vous gérez les données dans NetSuite.

Des mises à jour régulières de votre système garantissent que les nouveaux risques sont traités rapidement et que votre configuration NetSuite est alignée avec les dernières exigences de conformité.

Conclusion

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