OROCommerce™

Soyez prêt pour le RGPD avec OroCommerce

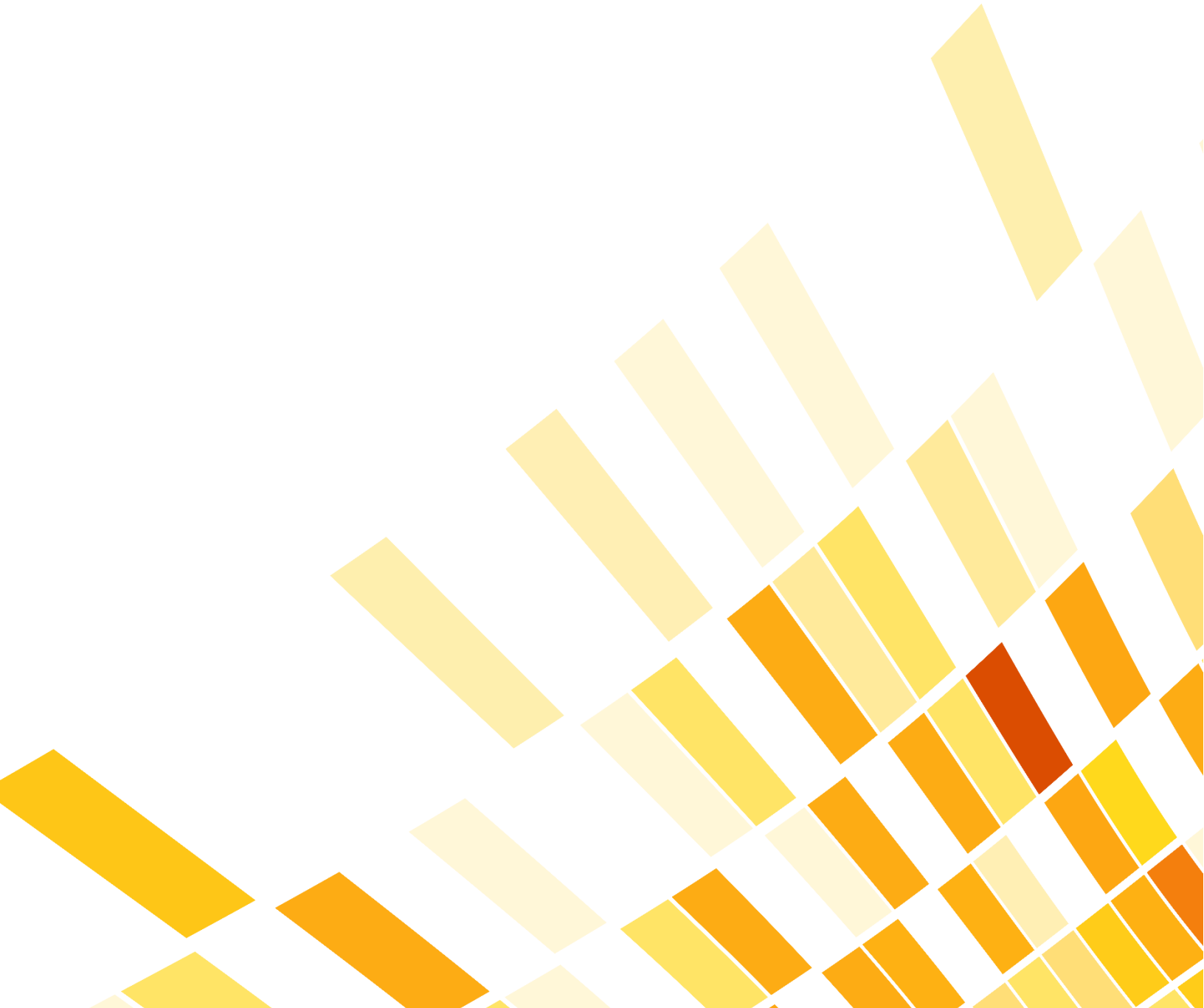

Table des Matières

Introduction

Le règlement général sur la protection des données (RGPD) est un règlement adopté par le Parlement et le Conseil européen protégeant les données personnelles des citoyens de l'UE. Il a été adopté dans la législation en mai 2016 et entrera pleinement en vigueur le 25 mai 2018.

Bien qu'il ne s'agisse pas de la première loi visant à protéger les données personnelles dans l'UE, la réglementation RGPD modifie radicalement le paysage de la protection de la vie privée. Le règlement s'applique à toute organisation ou organisme opérant dans l'UE. Il inclut également toute organisation ou entité internationale qui utilise les données personnelles des citoyens de l'UE.

Le RGPD promet des fortes amendes pour tout manquement au règlement. Le montant le plus élevé retenu étant de 20 millions d'euros ou 4% du chiffre d'affaires d'une entreprise. Il n'est pas étonnant que ces deux faits à eux seuls aient attiré beaucoup d'attention.

Comme toutes les lois sur la protection de la vie privée, le RGPD a besoin d'une approche holistique pour protéger les données privées. Il s'agit là d'examiner toutes les mesures de protection technologique de l'infrastructure organisationnelle existantes, ainsi que les logiciels utilisés.

Ce document a été créé pour aider les organisations utilisant OroCommerce à se conformer au RGPD. Il décrit comment utiliser les fonctions d'OroCommerce pour effectuer les préparations et les tâches de routine nécessaires à une mise en conformité avec le RGPD. Cependant, il ne décrit pas les processus qui doivent être exécutés au sein de votre organisation à l'étape préparatoire et par la suite.

Ce livre blanc est basé sur les recommandations et la liste de contrôle du bureau du Commissaire à l'information du Royaume-Uni.

Vous pouvez également trouver plus d'informations sur le RGPD sur le site web du RGPD de l'UE.

Points de contrôle du RGPD

La section suivante fournit les directives du RGPD sur les mesures à prendre avant et après le 25 mai 2018, date d'entrée en vigueur du règlement.

Audit des données

Les guides préparatoires et les listes de contrôle du RGPD recommandent la réalisation d'un audit des données de votre organisation afin d'identifier tous les composants et les systèmes qui stockent et

traitent des données personnelles. De par sa nature, le logiciel OroCommerce recueille, stocke et traite les données personnelles de vos clients. Votre organisation a besoin de documenter les systèmes, les composants et les éléments physiques de votre infrastructure qui stockent les données personnelles de vos clients. Nous avons listé les composants du logiciel ci-dessous pour vous faciliter la tâche.

OroCommerce utilise les entités suivantes pour stocker des données personnelles :

- Contact
- Pistes
- Demande de contact
- Compte
- Utilisateur client
- Demande de devis
- Devis

Il y a aussi des cas spéciaux comme :

- Les entités des clients et de commandes - bien que ces entités ne contiennent généralement pas de données personnelles, elles contiennent des champs d'adresse de facturation et de livraison qui sont classés comme des données personnelles.

La structure de ces entités dépend de la configuration particulière d'OroCommerce. Vous pouvez utiliser la fonction de gestion des entités ou le formulaire CRUD (créer, lire, modifier et supprimer) pour inspecter le contenu de chaque entité.

Lors de l'audit des données, nous vous conseillons de configurer la propriété « Auditable » sur « True » pour toutes les entités contenant des données personnelles. Ceci activera les pistes d'audit des données et vous permettra de traquer les changements de données personnelles au sein d'OroCommerce.

Entreposage physique

Toutes les données sur les entités d'OroCommerce sont stockées dans la base de données MySQL ou PostgreSQL (selon la configuration choisie lors de la mise en œuvre d'OroCommerce). Les indices d'Elasticsearch et de Redis contiennent également des données personnelles provenant d'entités listées.

Les journaux d'accès au serveur Web, ainsi que tout autre journal système configuré par les administrateurs système de votre organisation, peuvent également contenir des données personnelles. Ces journaux doivent également être examinés pendant l'audit au cas où une demande ou une requête serait faite.

Intégrations

OroCommerce utilise différents types d'intégrations pour les fournisseurs de services, les systèmes d'envoi d'e-mails en masse, les plateformes d'E-commerces et les services d'assistance (voir la documentation d'OroCommerce pour la liste complète). Cela signifie qu'OroCommerce peut effectuer des échanges de données personnelles avec ces systèmes. Vous devrez donc définir quelles données seront envoyées, fournir ces informations aux utilisateurs (si besoin) et développer un processus pour coordonner les demandes des utilisateurs (par exemple : supprimer les données personnelles).

Collecter, stocker et présenter le consentement de l'utilisateur pour la collecte et le traitement des données personnelles

Oro a développé un système de gestion pour la collecte des réponses de consentement pour les utilisateurs d'OroCommerce. Ce système de gestion permettra aux commerçants d'avoir un dispositif flexible pour gérer les réponses de consentement et traiter les demandes relatives à la protection des renseignements personnels. La sortie de ce système de gestion est prévue début mai 2018.

L'exercice des droits d'utilisateur

En fonction de la demande d'un utilisateur sur ses données, l'entreprise devra accorder certains droits : le droit d'accès, le droit de rectification, le droit à la portabilité des données et le droit d'effacement.

Droit d'accès

En vertu du règlement RGPD, une personne a le droit de savoir si ses données personnelles sont stockées et traitées. La personne a également le droit d'accéder à ces données, y compris des informations sur la structure exacte des données. Ce droit peut être demandé de différentes manières.

OroCommerce possède des fonctions de recherche puissantes et faciles à utiliser pour trouver toutes les entités reliées à la personne qui demande des renseignements personnels. Vous pouvez utiliser les formulaires CRUD d'OroCommerce pour consulter, recueillir et exporter des informations sur les données personnelles stockées.

Droit de rectification

Le RGPD protège le droit d'une personne de corriger des données personnelles si celles-ci sont incorrectes ou obsolètes. Ceci peut être fait grâce à une demande spéciale. Les outils de recherche et CRUD d'OroCommerce sont parfaits pour répondre à ce type de demande. Votre équipe gestion des données utilisateur pourront facilement corriger les données personnelles dans le système.

Droit à la portabilité des données

L'une des exigences les plus récentes en matière de protection de la vie privée est le droit des individus d'obtenir et de réutiliser des données personnelles dans d'autres systèmes ou organisations.

D'un point de vue technique, cela signifie que votre organisation doit pouvoir exporter des données personnelles dans un format lisible. Bien que le format exact ne soit pas encore défini par les organismes de réglementation, OroCommerce est en mesure d'exporter toute entité dans un format CSV à l'aide de sa fonction d'exportation standard. Actuellement, le format CSV est un format approprié pour la portabilité des données personnelles.

Droit d'effacement

Le RGPD stipule qu'une personne peut faire une demande pour supprimer ses données personnelles des systèmes d'information.

L'effacement des données personnelles comporte de nombreux aspects différents. Voici les points à exécuter et à considérer :

Suppression d'entités standards

OroCommerce stocke les données personnelles dans des entités décrites dans la section « Vérification des données » du présent document. Toutes les entités contenant des données personnelles peuvent être facilement trouvées en utilisant la fonction de recherche dans notre système. Toutes les entités peuvent prendre en charge la suppression d'un enregistrement, ce qui facilite la tâche des gestionnaires autorisés du système.

Certains champs nécessitent une attention particulière lors de la suppression de données personnelles liées à un utilisateur spécifique, par exemple « adresse de facturation » et « adresse de livraison » et « adresse de facturation par défaut » et « adresse de livraison par défaut» pour n'en nommer que

quelques-uns. Ces champs peuvent contenir des données personnelles et lorsque quelqu'un demande la suppression de ses informations, vous devrez le faire manuellement.

Systèmes connectés par des intégrations

Vous devez faire la demande d'effacement des données des systèmes et des intégrations connectés à votre plateforme d'OroCommerce en utilisant les procédures de communication développées lors de l'audit des données.

Webtracking

La fonction de suivi Web (Webtracking) d'OroCommerce est un outil très flexible et puissant pour la collecte et l'analyse des données reçues au travers de sites connectés. En raison de la nature hautement personnalisée des scripts de suivi, nous recommandons de vérifier la présence de données personnelles qui doivent être effacées dans les événements de suivi.

Sauvegardes

Pour l'instant, le RGPD ne contient pas d'exigences directes sur la suppression des sauvegardes, ce qui peut représenter un défi technique. Cependant, gardez à l'esprit qu'une panne système et une restauration de la base de données peuvent se produire juste après la suppression des données, ce qui entraînera la restauration des données supprimées. Nous vous recommandons de garder les demandes d'effacement ouvertes jusqu'à la prochaine sauvegarde de la base de données et de vérifier si les données personnelles ont effectivement été supprimées avant de clôturer ces demandes.

Voici l'exemple d'une sauvegarde du système effectuée chaque nuit en dehors des heures d'ouverture :

- L'opérateur supprime les données personnelles d'OroCommerce mais garde la demande ouverte.
- Le lendemain matin, l'opérateur ou le superviseur de l'opérateur vérifie les demandes ouvertes d'effacement de données personnelles dans OroCommerce et ferme la demande si l'effacement est confirmé.

Il est également recommandé de développer des procédures de restauration des bases de données en utilisant des sauvegardes plus anciennes que vos sauvegardes régulières. *(Par exemple : votre organisation décide de restaurer une sauvegarde de la base de données vieille de 2 mois).*

Autres points de contrôle à surveiller

Transfert de données personnelles à l'extérieur de votre organisation

Le RGPD interdit strictement le transfert de données personnelles en dehors de l'UE. Oro Inc. est une société américaine dont les centres technologiques sont situés en dehors de l'UE. C'est pourquoi nous vous demandons de rendre illisible toutes les données de production (dépôts de bases de données, etc.) fournies au service à la clientèle d'Oro.

Protection de la vie privée dès la conception

L'un des points de contrôle du RGPD est le respect de la vie privée dès la conception du système, ce qui signifie que les organisations doivent utiliser des solutions de pointe pour le traitement et le stockage des données personnelles. Oro Inc. a incorporé les meilleures pratiques de développement sécuritaire dans ses processus de développement tout en continuant d'effectuer des tests de sécurité sur OroCommerce selon le SANS, l'OWASP et les meilleures pratiques en matière de sécurité de l'information. Le produit OroCommerce fait partie du service OroCloud et détient la certification PCI DSS. Cela signifie qu'une fois déployé dans une infrastructure sécurisée et maintenu en conformité avec les processus ITIL, OroCommerce fournit un niveau de sécurité de l'information de pointe et protège toutes les données privées et sensibles qui y sont stockées.

Conservation des données

OroCommerce, par sa fonction commerciale, ne traite aucune entité contenant des données personnelles avec une date d'expiration. Votre organisation peut envisager de supprimer les commandes, les contacts et d'autres entités grâce à nos capacités de filtrage.

Résumé

Afin de se conformer au RGPD, votre organisation doit passer par des étapes préparatoires pour être prête pour l'entrée en vigueur du RGPD le 25 mai 2018. Cela comprend l'élaboration d'un processus interne pour répondre aux demandes des utilisateurs voulant exercer leur droit protégé par le RGPD.

Choses à faire avec OroCommerce avant le 25 mai

- Effectuer un audit des données.
- Une mise en conformité totale d'OroCommerce avec le RGPD sera mise en œuvre d'ici le début du mois de mai.
- Planifier la gestion des consentements pour vos sites liés à OroCommerce et préparer un libellé de consentement adapté à vos utilisateurs et vos marchés.
- Créer et exécuter des campagnes de marketing par e-mail pour recueillir le consentement des utilisateurs existants à l'égard de leurs données personnelles déjà stockées et traitées.
- Mettre à jour les dossiers des personnes qui ont donné leur consentement.
- Documenter l'utilisation légale des données personnelles pour ceux qui n'ont pas donné leur consentement.
- Développer des procédures et des scripts pour l'exportation de bases de données et l'offuscation des données personnelles.

Processus de gestion des données personnelles pour répondre aux exigences du RGPD

- Processus de partage d'informations sur les données personnelles stockées.
- Processus de correction des données personnelles.
- Processus d'exportation des données personnelles.
- Processus d'effacement des données personnelles.

Glossaire

RGPD - Le Règlement général sur la protection des données est une loi visant à protéger la vie privée adopté par la législation européenne le 25 mai 2016.

Données à caractère personnel - Toute information concernant une personne identifiable qui peut être identifiée directement ou indirectement, notamment en référence à un identifiant (définitions clés).

Utilisateur - Personne qui est inscrite et qui utilise OroCommerce ayant un ou plusieurs rôles à l'intérieur du système.

Personne – Un individu dont les données personnelles sont stockées et traitées dans OroCommerce mais qui n'est pas un utilisateur du système.

CRUD - Élément de l'interface utilisateur (généralement un formulaire) pour créer/réviser/mettre à jour/supprimer des actions.

À Propos d'OroCommerce

La plateforme d'E-commerce B2B numéro 1

Construisez votre présence en ligne

Peu importe que vous soyez un fabricant, un distributeur, un grossiste, un détaillant ou une marque, atteignez de nouveaux marchés avec une meilleure présence en ligne et sur téléphonie mobile.

Obtenez une plate-forme d'E-commerce et un CRM tout-en-un

Grace à cette plate-forme d'E-commerce avec CRM intégré, obtenez une vue à 360 degrés de tous les points de contact du client à travers les ventes, le marketing et le support clientèle.

Une seule plate-forme pour tous vos échanges commerciaux

Faites face à tous les scénarios B2B, B2C et B2X (B2B2B, B2B2C, etc.) possibles sur une seule plate-forme. Personnalisez-le facilement en fonction de vos besoins.

Voir l'extension RGPD