CloudSense Solution and GDPR Compliance

On May 25, 2018 the General Data Protection Regulation (GDPR) took effect in the European Union (EU). The new regulation imposes broad new data privacy protections for EU individuals and applies to any company that collects or handles EU personal data, regardless of the company's location.

CloudSense is committed to helping its customers comply with GDPR through robust privacy and security protections in its products and services.

Below, we describe the steps we've taken to implement GDPR-compliant functionality in our CloudSense Commerce and Subscriber Management Platform (“Cloudsense Solution”).

How Cloudsense Solution Addresses GDPR Requirements

CloudSense is taking a multi-level approach to fulfill GDPR product compliance requirements with minimal impact to customers:

- Level I - Addressing core infrastructure requirements around encryption, backups, and data retention.
- Level II - Addressing additional GDPR requirements through the existing user interface and APIs.

Level I - Infrastructure

Key GDPR Requirements	**Cloudsense Solution Capabilities**
Encryption-at-rest of Personal Data	Our customers take advantage of encryption at rest in our AWS data center. Databases are encrypted and can only be read via

Key GDPR Requirements	Cloudsense Solution Capabilities
	the DBMS by the application or by an administrator who has username and password access.
Encryption-in-transit of Personal Data	Communication between clients and the Cloudsense Solution Server is encrypted using HTTPS/SSL. Communication between the Cloudsense Solution Server and 3rd-party systems is encrypted via HTTPS/SSL. Cloudsense Solution internal server-to-server uses SSL and network isolation for a customer's server cluster.
Data Mapping / Data Inventory	Cloudsense Solution documentation provides a comprehensive overview of the standard data model and the fields which can be used to store personal data. Custom added fields need to be documented by the customer.
Individual's Right - Data Retention	Customers have the ability to remove data when they decide it is necessary using the existing APIs or user interface.
Data Backups	Backups are kept for a period of minimum 7 days.
Privacy by Design	The Cloudsense Solution development processes include data privacy reviews during architecture and design phases for new major features.

Level II - User Interface ("UI") and APIs

The features listed below are provided in the currently supported versions of Cloudsense Solution.

Key GDPR Requirements	Cloudsense Solution Capabilities
Individual's Right to Access and Review	Cloudsense Solution does not interact directly with individuals. Customers are provided with an existing API and UI to access and review personal data by individuals.

Key GDPR Requirements	Cloudsense Solution Capabilities
Individual’s Right to Update Data	Cloudsense Solution provides capabilities to update an individual's personal data. In addition, Cloudsense Solution provides an existing API to update personal data by individuals.
Individual’s Right - Data Portability	Cloudsense Solution provides comprehensive data export capabilities.
Individual’s Right - Commonly Used Format	Cloudsense Solution provides different file formats for data export, such as CSV, TXT, PDF, and HTML.
Individual’s Right to Erasure	Cloudsense Solution provides capabilities to delete personal data.
Individual’s Right - Consent	Cloudsense Solution does not interact directly with individuals and does not require obtaining consent from individuals.

We're Here to Help

If you have any additional questions or need assistance, please contact support. CloudSense's Professional Services team is also available to assist with special customizations or configuration needed to achieve GDPR compliance; for more information please contact your account manager.

Legal Notice