OroCloud Commitments to GDPR

Table of Contents

Purpose of Document

This document is intended for OroCloud customers who are data controllers according to the GDPR definition. It provides general information about the standards and best practices adopted by Oro Inc. as a data processor to support GDPR requirements.

This document also describes recommendations to data controllers on following GDPR requirements for parts that are under their control.

Privacy protection

Oro has implemented a “security by design and by default” approach for OroCloud services which covers all aspects from the hosting platform all the way up to the organization's processes.

Hosting

OroCloud is hosted on Google Cloud Platform (GCP). GCP is certified to be compliant with most of the widely recognized data security and privacy standards (specifically ISO 27018) which effectively covers all GDPR requirements. You can check the full list of standards as well as Google’s commitments to the GDPR here.

Oro Applications in OroCloud

All Oro Applications including OroPlatform, OroCRM, and OroCommerce have been developed according to the best security practices recognized by the industry. OroCommerce, which is hosted inside GCP by trained Oro personnel, has earned PCI DSS certification. While PCI DSS does not directly protect data privacy the security standard does safeguard processes touching cardholder data and also protects the private data of OroCommerce users.

The list below details safeguards placed in OroCloud which protects private user data ensuring a “security by default” approach:

Network Isolation and Segmentation

All production nodes containing sensitive data, including personal data, are located inside a secure network perimeter which protects data from any external connections. Objects that store user data can only be accessed by the OroCommerce application and only by authorized personnel. Oro does not allow direct connection from any components outside of the network into the DB server or any other components storing data.

All outgoing connections are directed via network gateways which provide close controls over outgoing traffic including whitelists for integration systems.

Per PCI DSS requirements, Oro performs semi-annual network penetration testing. The same tests are run after major changes in the network topology.

Vulnerability and Patch Management

Vulnerability and patch management is an integral part of the Oro software development and OroCloud support and maintenance processes. Vulnerability testing, based on OWASP recommendations, of OroCRM and OroCommerce products is performed during integration testing.

All security advisories from MS-ISAC, SANS Institute, CIS and other component vendors are monitored and trigger actions in the Patch Management process according to the Change Management policy. Oro's dedicated personnel, namely Security Lead and Cloud Lead, are responsible for implementing Vulnerability and Patch Management processes, supervised by Oro's Information Security Officer.

Backups and Retention Policies

Every OroCloud production instance performs daily automated backups. The default retention period for a production backup is 1 year. This period can be extended upon written request from the customer.

All backups are encrypted using strong encryption and stored in Google Cloud Storage buckets with limited and controlled access. Backup and restore operation are fully automated and do not require any access to the customer data from Oro employees.

There is a special mechanism for creating sanitized (anonymized) DB dumps for testing purposes. This mechanism uses data obfuscation and de-personalization to create production-like data sets used for testing but does not contain any sensitive or personal data. Oro strongly recommends using only sanitized DB dumps for testing and troubleshooting purposes.

Data Encryption

Oro uses HTTPS protocol with strong cryptography settings for data transfer to and from OroCloud production instances. Use of non-secure protocols is strictly prohibited and impossible by design.

Logs and Audit Trails

OroCloud and Oro products log all important events in both infrastructure nodes and the application including security events. All end-user security-related actions like changes to private end-user data, alterations to access rights, provisioning and termination of admin accounts are all logged by the system. All logs are securely stored according to the retention policy of 1 year. This period can be extended upon written request by the customer.

Access to the logs is based on "need-to-know" principle.

Change Management and Release Procedures

Oro uses an infrastructure Continuous Integration (CI) approach as well as change management procedures for both application and infrastructure code. This means that every change in code, no matter if the change is in the application or infrastructure, is closely tested and delivered into production after approval from the responsible team member.

Any release or change management of the code developed and maintained by the customer is the responsibility of the customer.

Access Management

Oro is responsible for managing access to the infrastructure nodes so only dedicated Oro support team members and specific users requested by the customer can have access to production hosts. No root console access is allowed. Oro uses a centralized identity management system and GCP Identity and Access Management in OroCloud. All Oro employee accounts are protected by MFA.

Oro is not responsible for managing accounts in the Web admin console and end-users in any Oro application production instance. The customer is fully responsible for creating and managing users and setting and maintaining password policies. OroCommerce provides a comprehensive set of security features that protect both web admin console users and end-user accounts from brute force attacks and other actions targeted at the user account.

Security Policies and Trainings

Oro has developed and maintained PCI DSS compliant security policies which protect both Oro and the customer’s data. Policies cover data classification and protection, password protection, email and other sensitive technologies usage, configuration management etc. All Oro employees have signed the policy forms upon hiring and Oro continues to confirm compliance on a regular basis.

Every Oro employee receives security training annually and also upon request . Training progress and results are tracked by our Learning Management system for auditing purposes.

International Data Transfers

Hosting Locations

OroCloud production instance can be hosted in any region provided by Google for GCP. There are 4 regions located in the EU and available for OroCloud. Oro EU customers can select any of these regions to host any Oro application in order to fulfill GDPR requirement regarding international data transfers.

Disaster Recovery Locations

In order to protect customers from catastrophic events which can affect the whole GCP region, Oro has a Disaster Recovery (DR) location - another GCP region geographically separated from the main hosting location. This region will be used if the primary location is not available because of failure in Google's infrastructure or network issues outside of Google and Oro's control. According to GDPR requirements regarding international data transfer, the DR location is situated inside of the EU.

This allocation can be extended upon written request from a customer.

Data Transfers

There are some particular cases when the customer needs to provide data from a production instance to Oro support for testing or troubleshooting purposes. Oro's policies require this data to be sanitized (anonymized) before transfer to the Oro Support engineer. Oro encourages customers to use standard OroCloud tools for that. The customer is responsible for anonymizing data transferred to Oro team members.

Data Audit

Per GDPR requirements, data controllers must create and maintain an inventory of systems storing personal data. Oro has developed white papers to describe all components inside OroCRM and OroCommerce which store personal data. Due to the flexibility of the Oro products, customers can create additional entities to store any kind of information including personal data. It is the responsibility of the customer to keep the data inventory updated using OroCRM and OroCommerce built-in features.

Consents

Oro is not responsible for collecting and storing consents since this is the responsibility of data controller. Oro has developed an extension for OroCommerce to create, manage and store user consents "Customer Consent Management in OroCommerce". This flexible yet powerful extension implements all recommendations of regulatory bodies regarding end-user consent. Using this extension, data controller can create, store and manage different versions of consents, including user locale-specific language versions. The exact text of user consent, management procedures and reporting is the responsibility of the Oro customer.

You can find full documentation for this extension is here.

User's Individual Rights

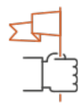
One of the key requirements for GDPR is to create and maintain processes for supporting individual's right for access, rectification, portability, and erasure of personal data. This is the responsibility of the customer to implement these processes using features and guidelines described in the whitepaper for OroCRM and OroCommerce.

Glossary

GDPR	General Data Protection Regulation, privacy protection law passed EU legislation on May 25, 2016.
Personal data	any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier (Key definitions).
User	Person who is registered inside OroCommerce having one or more role inside the system.
Person	An individual whose personal data is stored and processed inside OroCommerce but not a user of the system.
PCI DSS	Payment Card Industry Data Security Standard
OWASP	Open Web Application Security Project
MS-ISAC	Multi-State Sharing and Analysis Center
CIS	Center for Internet Security

About OroCommerce

The #1 B2B eCommerce Platform



Build Your Online Presence

It doesn't matter if you're a manufacturer, distributor, wholesaler, retailer, or brand. Expand your business into new markets with an online and mobile presence.

Get eCommerce & CRM. All-in-One

Get a 360-degree view of all customer touch-points across sales, marketing, customer support, and eCommerce with a built-in CRM.

One Platform for All Your Commerce

Addresses all B2B, B2C, and B2X (B2B2B, B2B2C, etc.) scenarios in a single platform. Easily customize it to fit your needs.

CONTACT US