OrbitMI

Platform Data Management & Security

March 2021

orbitmi.com
info@orbitmi.com

Introduction

At the heart of digital transformation in the global maritime industry is the need to make the vast amounts of critical and immensely valuable data sources available to and actionable by end-users. With increased pressures from IMO regulations, geopolitical conflict, trade volatility, new technologies and the changing nature of the workforce, that need is more important than ever. In short, being data-driven was once an aspiration; now it's an imperative.

Data security and data privacy are also imperatives for IT leaders and their organizations. OrbitMI understands these concerns and we believe it's critical to deliver security and data privacy across all aspects of our platform.

This overview outlines the data managed in Orbit, and how they are secured. It also includes our statement on GDPR compliance.

What data is stored in Orbit?

User Information

Orbit stores user information including name, email address, and other contact information, is stored and if the user chooses, displayed in the Contact List. This data is given voluntarily by users of the system, and all except email address can be removed or left blank.

Third Party System Data

Third party system data including vessel and port information, weather and market data, are used to create the Orbit experience for the user. These data feeds are obtained under contract/license by OrbitMI on behalf of all clients. For a list of current data and technology partners, click here.

Client Data

Client data is received from the client's voyage management and/or reporting systems, including Orbit Reporter if applicable. This data is fed directly to Orbit via API integration using the client's access license and credentials.

User Generated Content (UGC)

Orbit stores content including account information, edits to imported data, reports created in Orbit Reporter, comments, additional port, terminal and berth information and user edits to third party data. These items are stored and used variously throughout the application on behalf of the user. This data is given voluntarily by users of the system and is not required for successful use of Orbit.

Application Log Files

Application log files, including access and debugging information. These data are generated by the application and contains PII including IP address, the ID of the user making the request, etc.

Which GDPR Categories of Data are Processed by OrbitMI?

Personal Data

- **Contact data** such as name, email, phone number, URL are stored until deleted
- **Location data** may be recorded in log files and stored temporarily for up to 30 days

“Special Category” Data

- OrbitMI does not collect, store or use any “Special Category” data

Data Subjects

The personal data transferred concerns the following categories of data subjects:

- Registered Users of the platform
- Registered Administrators of the platform

How is access to data protected?

Access to any Orbit installation requires access via an encrypted HTTP connection (HTTPS), then successful entry of a valid username and password for the installation being accessed. Non-encrypted connections are redirected to a secure connection.

Access to Orbit infrastructure requires SSH, and that the request comes from a pre-configured, limited set of IP addresses. Only Orbit administrators can access the SSH key repository.

How is Data Transmitted?

Data Transfer Activities - Examples

- Manual input of user contact information
- Manual input of comments
- Manual correction of vessel voyage data
- Exporting of data, primarily reports, in XLSX, CSV or PDF format

Data Transfer Processing Activities - Examples

- Application logging of person data – log files with IP address and session information, including the user’s ID, is stored temporarily in AWS Cloud Watch and deleted after 30 days
- Personal data display is limited to the user’s profile information, which is voluntarily entered
- Transmission of personal data is limited to the user’s profile information when initiating an outbound email message, such as from the Position List

User information is manually input by customers, or OrbitMI customer success staff. All such interactions required use of HTTPS and sign-in as noted in the previous section.

Third party data are transmitted from the providers to Orbit via various methods including HTTPS, HTTP over a restricted IP range, etc. Some providers provide downloads for our use, every 3 to 6 months.

User generated content is generally manually input by customers, with all interactions required use of HTTPS and sign-in as noted in the previous section.

A notable exception are daily reports from vessels. If these are obtained using Orbit Reporter, the reports are transported via the client's email infrastructure. Orbit does not assure the security of such transmission.

Orbit retrieves messages using an email client that supports encryption, TLS, DKIM and other standard protocols, but they are only engaged if the customer's mail system requires it.

Orbit also supports users in sending out relevant material to their partners. This is always done by email on behalf of the user. This requires customers to add an MX record to their email infrastructure; they can revoke it at any time; in this event, most messages will be marked a spam or rejected, depending on the customer's email configuration.

Emailed content is not stored in Orbit. (It is, of course, stored in the involved email infrastructure.)

Where is the data stored? And how is it protected?

Each customer has their own dedicated installation of Orbit, on physically separate hardware. Data is never shared between customers; third party data is copied into each environment that needs it.

We expect to offer multi-tenant support for customers who want such an offering in the future; at that time we will provide a different paper outlining how information is managed in that environment.

Orbit stores data in three places for each installation:

1. PostgreSQL database is used to store user data
2. MongoDB is used to store third party data
3. Application log files are stored in AWS Cloud Watch and deleted after 30 days

All data transmitted, received or stored, are encrypted in motion, meaning use of HTTPS is required.

Currently user passwords are stored in the Orbit database. Passwords are protected using a Key Derivation Function with random salt, taken from the asp.net core identity capability. It is not possible to identify the password for a user, only to match against the hash to verify that the correct one has been entered. As of 2020, most users will access Orbit via Single Sign On (SSO) in which case the platform will NOT store passwords.

Orbit uses AWS Secrets Manager to protect access information including customer integration points.

Is the system GDPR compliant?

Yes. It is very easy to extract all User Information and User Generated Content from the system that belongs to a specific user, provide it to them, and optionally delete it.

How is third party access information managed?

Orbit stores third party data, per our licensed options, to provide the Orbit service, even if there are temporary interruptions of the data feeds from the providers.

Orbit uses AWS Secrets Manager to protect access information for third party systems.

AWS Secrets Manager helps you protect secrets needed to access your applications, services, and IT resources. The service enables you to easily rotate, manage, and retrieve database credentials, API keys, and other secrets throughout their lifecycle. Users and applications retrieve secrets with a call to Secrets Manager APIs, eliminating the need to hardcode sensitive information in plain text.

Has OrbitMI completed any security audits?

Yes. OrbitMI has successfully completed two major security audits in 2024. Both audits were conducted by and independent service auditor.

1. Type 2 SOC 2 Examination: OrbitMI underwent a Type 2 SOC 2 examination, which assessed the suitability of the design and operating effectiveness of controls relevant to the Security Trust Services Criteria.

2. ISO 27001:2022 Certification Audit: OrbitMI also completed an ISO 27001:2022 certification audit for its Information Security Management System (ISMS), which assessed the design and implementation of OrbitMI's ISMS supporting the confidentiality, integrity, and availability of customer data, supplier information, and internal data related to the vessel performance and maritime intelligence platform.

In addition, the Orbit development team performs regular, basic OWASP testing of the application. Finally, Orbit receives a third-party security review every year, generally in Q4.

What do these audits demonstrate?

1. Our security controls are suitably designed and operating effectively to meet industry-standard criteria.

2. We have implemented a comprehensive Information Security Management System that meets international standards.

3. We are dedicated to ensuring the confidentiality, integrity, and availability of our customers' data.

4. We continuously assess and improve our security practices to address evolving threats and meet regulatory requirements.

For more information on these audits, please contact us at info@orbitmi.com

OrbitMI

orbitmi.com
info@orbitmi.com