Data Processing - Non Disclosure
Platform Security, Privacy and Architecture
Policy

Published: April 13, 2021

You (**You**") have signed up to the Ocean.io services or you are considering signing up for the Ocean.io services and in this connection, you are granting Ocean.io ("**We**" "**Our**") access to Your CRM Account Data (as defined below).

I - Which types of Your data we use and for which purposes

We use your CRM Account Data to perform an analysis of Your customer segments and to help You optimize your sales and marketing effectiveness and identify sales opportunities for You.

We use the identification data of Your CRM Account Data to fuzzy match your CRM accounts against Our database. Once we have matched your CRM accounts against our database, We use the transactional data of Your CRM Account Data to analyze Your performance within the various segments to identify sales efficiencies and opportunities.

Ocean.io Commitment

We use Your CRM Account Data to enhance the performance of our algorithm we make available to you. We do NOT use your data for any other purposes than enhancing the algorithm. We do NOT include any of your data in the Ocean.io general database. We do keep a copy of your data in a segregated database for your use only - see below.

We are committed to achieving and maintaining the trust of our customers. Providing a robust security and privacy program that carefully considers data protection matters across our suite of services, including protection of Your CRM Account Data and Content (as defined below) are the cornerstones of this mission.

"CRM Account Data" means electronic data and information from Your CRM system submitted by or for You to the Ocean.io platform.

"Content" means information generated by Ocean.io and/or obtained by Ocean.io from publicly available sources or its third-party content providers and made available to You through the Services.

II - Non-disclosure

Your CRM Account Data are Your proprietary data. We will keep them confidential and will take the same measures to protect Your CRM Account Data as we protect our own data. We will not disclose Your CRM Account Data to any third party. We will maintain appropriate administrative, physical and technical safeguards for the protection of the security, confidentiality and integrity of Your CRM Account Data - see section III below.

III - Platform Security, Privacy and Architecture

This documentation describes the architecture, the security and data protection applicable to Ocean.io services that get activated when You integrate your CRM system or CRM Account Data with the Ocean.io Platform ("**Covered Services**").

Architecture and Data Segregation

The Covered Services are operated in a multitenant architecture that is designed to segregate and restrict CRM Account Data access. The architecture provides an effective logical data separation for different customers via unique ID. Additional data segregation is ensured by providing separate environments for different functions, especially for testing and production.

Security Policies and Procedures

Access to the Covered Services is via the Ocean.io Platform API, and requires a valid key/secret/token which is encrypted via TLS while in transmission. To enhance security Org IDs are assigned to ensure that activities can be attributed to the responsible account.

Intrusion Detection

Ocean.io, or an authorized independent third party, will monitor for unauthorized intrusions using multiple detection mechanisms. Ocean.io may analyze data collected by users' web browsers (e.g., device type, screen resolution, time zone, operating system version, browser type and version, system fonts, installed browser plug-ins, enabled MIME types, etc.) for security purposes, including to prevent fraudulent authentications, and to ensure that the Covered Services function properly.

User Authentication

Access to the Covered Services requires a key/secret/token, which are encrypted via TLS while in transmission.

Physical Security

Ocean.io uses Google Clo for data storage. Google Cloud has systems that control physical access to the data center. These systems permit only authorized personnel to access secure areas. The facilities are designed to withstand adverse weather and other reasonably

predictable natural conditions, are secured by around-the-clock guards, physical access screening and escort-controlled access, and are also supported by on-site back-up generators in the event of a power failure.

Reliability and Backup

All networking components, load balancers, Web servers and application servers are configured in a redundant configuration. All CRM Account Data submitted to the Covered Services is stored on a primary database server that is clustered with a backup database server for higher availability. All CRM Account Data submitted to the Covered Services is backed up daily.

Disaster Recovery

Production data centers are designed to mitigate the risk of single points of failure and provide a resilient environment to support service continuity and performance. Ocean.io has disaster recovery procedures in place which provide for backup of critical data and services. A system of recovery processes exists to bring business-critical systems for Covered Services back online within a brief period of time.

Viruses

The Covered Services do not scan for viruses that could be included in attachments or other data uploaded into the Covered Services by You.

Data Encryption

The Covered Services use industry-accepted encryption products to protect CRM Account Data and communications during transmissions between a customer's network and the Covered Services, including through Transport Layer Encryption (TLS).

Deletion of CRM Account Data

After termination of all subscriptions or tests associated with any of the Covered Services, CRM Account Data submitted to the Covered Services shall be deleted by Ocean.io within 30 days after expiry.

Sensitive Data

Important: The following types of sensitive personal data (including images or other information containing or revealing such sensitive data) may not be submitted to the Covered Services: government- issued identification numbers; financial information (such as credit or debit card numbers, any related security codes or passwords, and bank account numbers); racial or ethnic origin, personal health information, political opinions, religious or philosophical beliefs, trade-union membership, and information concerning sex life. The only Personal Data

that may be submitted are Names of professionals within the Account and their professional emails or telephone numbers. Private telephone numbers, addresses and the likes may not be submitted.

Analytics

Ocean.io may track and analyze the usage of the Covered Services for the purposes of security and of helping Ocean.io improve both the Covered Services and the user experience in using the Covered Services. For example, we may use this information to understand and analyze trends or track which of our features are used most often to improve product and feature functionality. Ocean.io may share anonymous usage data with Ocean.io's service providers for the purpose of helping Ocean.io in such tracking, analysis, and improvements. Additionally, Ocean.io may share such anonymous usage data on an aggregate basis in the normal course of operating our business; for example, we may share information publicly to show trends about the general use of our services.

In addition, Ocean.io may use CRM Account Data on an aggregate basis for purposes such as research, marketing, analysis, and benchmarking, and other purposes reasonably required to develop, deliver, and provide ongoing innovation to the Covered Services. No CRM Account Data consisting of personally identifiable information will be shared in this manner, nor any data that would identify customers, their users, their consumers, or any individual, company or organization. By using the Covered Services, customers consent to the use and disclosure of their CRM Account Data in anonymized and aggregated form.