Security Practices

Last Updated September 14, 2019

Introduction

Our customers depend on Yembo to provide moving surveys at unprecedented speed using cutting-edge artificial intelligence. In today's sophisticated security landscape, Yembo has implemented industry-leading security practices to keep our customer's business data safe.

This booklet provides an overview of Yembo's data security practices, both internally and across various environments.

Compliance

Yembo's products are designed to serve an ever-increasing number of use cases. As some of those use cases may implicate certain regulated forms of data, please note that customers are ultimately responsible for complying with the law governing the data they submit to Yembo through Yembo products, including those regarding the privacy and protection of personal, sensitive, and/or financial data.

Yembo provides certain types of assistance in order to help customers meet their compliance goals. For example, Yembo's certification to the EU-U.S. Privacy Shield Framework is helpful for those customers subject to the GDPR. Yembo also maintains a suite of rigorous security policies, surpassing the practices of many of its peers. The specifics of Yembo's various security practices are described below.

Cross-Border Data Transfers

The EU Data Protection Directive prohibits the transfer of personal data outside the European Economic Area (EEA) without appropriate safeguards that provide adequate protection. Beginning in May 2018, the General Data Protection Regulation (GDPR) imposes the same prohibition. Switzerland imposes similar restrictions on cross-border data transfers.

Yembo provides its customers with two adequacy mechanisms to comply with EU cross-border data transfer regulations – the Privacy Shield and the Model Clauses.

Physical Security

Yembo uses physical and procedural safeguards to help protect data facilities and equipment. Access to facilities is limited to employees and authorized contractors. Upon termination of the employee/contractor relationship, keys are collected and access privileges are revoked. Visitors must be invited in advance by authorized Yembo personnel. Physical alarms and 24/7 video surveillance are deployed throughout our facilities, where appropriate.

Yembo personnel are trained on policies and proper security steps that must be taken with office equipment such as laptops, printers, mobile devices, removable media, and visible office spaces (such as desks and screens).

Access Restrictions

Yembo restricts access to confidential information (including customer information), networks, and other resources based on job function and need. Any requests for access privileges require approval from the business owner responsible for the data, and all requests and approvals are documented.

Access to Customer Data within Yembo Software

Yembo provides role-based access control which allows our customers to restrict customer data access only to authorized personnel. The following roles are provided:

- **Reviewer**: Reviewer Accounts have access to the system to view inventory and videos for moves. Customer details and pricing are hidden from the Reviewer. Reviewer Accounts are best used for individuals that the company desires to have review and update inventory lists only.
- **Employee**: An Employee Account has all of the permissions of the Reviewer to view and edit inventories, and also has the ability to see customer information for all moves assigned to companies the Employee belongs to. Employee Accounts may be best suited for salespeople to review and provide pricing information to end consumers.
- **Consultant**: Consultants are afforded the same permissions as Employees, but only for moves they have been assigned to. If a Consultant is not personally assigned to a move, they will be unable to see or interact with it in any way.
- **Admin**: An Admin Account has all of the permissions as the Reviewer and the Employee roles, and also the ability to create and edit Accounts for their company. This Account type is best used by a limited number of people at the company to setup and control Accounts for other staff at the company.

Systems Access

For corporate access (i.e., for general access to Yembo's internal corporate systems), requests for new or modified network access are submitted and logged. Access is not granted without approval from the individual's manager. Yembo uses identity management software with two-factor authentication to confirm the identity of authorized users. Access to in-scope applications is reviewed quarterly. Administrator-level access is revalidated by IT management at each office location.

Any additional access privileges (including administrator privileges) are tailored to job function and need, and require approval from Yembo administrators. Access is reviewed monthly by each designated

administrator, and Yembo regularly verifies the completeness and accuracy of the review.

Access to Yembo's source code repositories and cloud services such as Amazon Web Services ("AWS") are restricted to authorized personnel and two-factor authentication is required.

Intrusion Detection

Yembo employs cloud-based vulnerability scanning, which logs attempted access and is reinforced with automatic alerts that are configured to trigger incident management procedures in certain cases. Yembo collects its own log, event, and sensor-based data continuously to monitor, detect, and investigate suspicious activity as permitted by law. Customers may request a third-party report of Yembo's compliance with its intrusion detection system at security@yembo.ai.

Yembo's intrusion detection procedures are bolstered by the Cyber Incident Response Plan (discussed below) in the event an intrusion attempt results in a security incident.

Cyber Incident Response Plan

Yembo's Cyber Incident Response Plan (CIRP) provides a documented framework for identifying, containing, and eradicating security incidents. The CIRP establishes the organization, actions, and procedures that allow Yembo to prepare for incidents, initiate responsive action, remediate any consequences of an incident, and document lessons learned for iteration and improvement of internal processes. Yembo routinely tests the CIRP using a combination of spot checks, live simulations, and periodic training.

Built-In Encryption

Yembo's cloud environments provide mandatory encryption both in-transit and at-rest. Neither form of encryption may be disabled.

Data Encryption In-Transit

Yembo uses industry-standard SSL encryption for data in transit. All SSL configurations are routinely monitored by a third-party service to ensure compliance with current best practices. Each user session is secured in this manner with no exceptions. Customers may request a third-party report of Yembo's SSL encryption configuration via email at security@yembo.ai.

Electronic messaging is secured by opportunistic TLS encryption on the email gateways.

Data Encryption at Rest

Yembo stores data in MongoDB Atlas and AWS S3. Data is encrypted at rest in both deployments using 256-bit AES. Encryption at rest is provided for all deployments with no exceptions, for both textual data and multimedia uploads.

Data Backups

All data submitted to Yembo is backed up for resiliency to natural disasters or hardware failures. Databases are snapshotted automatically and backed up on AWS via MongoDB's Atlas product. Multimedia uploads are stored in S3 and are backed up to both AWS Glacier and an on-premise NAS. Access to data on AWS is controlled by AWS Identity Access Management roles and rights. Please note that the S3 bucket encryption process is managed by AWS. Keys are rotated on a routine basis and are access is continuously monitored.

Secure Disposal

Yembo permanently deletes personally-identifiable customer data 30 days after termination. Please note that this includes backups. AWS provides automated assistance in the secure disposal of customer data by helping wipe all disks and verifying that data is permanently deleted.

Vendors

Yembo retains suppliers, subprocessors, and other vendors ("Vendors") who may from time to time perform services for Yembo or for customers on Yembo's behalf. Yembo only retains those Vendors that meet Yembo's stringent security criteria so as to ensure they provide at least the same level of protection to customer data as does Yembo.

Additionally, Yembo maintains internal environments separate from production that do not contain customer data. Vendors are provided access only to these internal environments unless their job function explicitly requires access to customer data.

When performing services at Yembo facilities, Vendors may only access the available guest network unless explicitly authorized.

Periodically, Yembo may ask a Vendor to re-evaluate its security posture to help ensure compliance with evolving privacy and security policies and procedures.

Chief Compliance Officer and Data Protection Officer

As required by the GDPR, Yembo has appointed a Data Protection Officer, Zach Rattner, who can be reached via email at dpo@yembo.ai. Yembo's Chief Compliance Officer is Siddharth Mohan, who can be reached via email at cco@yembo.ai.

GDPR Data Subject Rights

Under Article 15 of the GDPR, data subjects have the right to "access" the personal data about them that is being processed. If you are such a data subject and would like to view, correct, amend, or delete the data, please send an email request to privacy@yembo.ai. Note that we will require verification of identity before divulging personal information.