COMPLY

Security Ecosystem

AN OVERVIEW OF ADMINISTRATIVE, PHYSICAL AND TECHNOLOGICAL SAFEGUARDS

Security at Every Level

COMPLY implements security at all levels of the infrastructure stack and employs the latest technologies to safeguard client information. Critical information security practices like software development and infrastructure security are regularly reviewed by independent information security organizations.

Administrative Safeguards

- COMPLY maintains and regularly updates its information security program
- COMPLY maintains policies consistent with the organization's obligations under the EU's General Data Protection Regulation (GDPR), UK's Data Protection Act 2018, and California Consumer Privacy Act (CCPA)
- Multi-jurisdictional background and identity checks are performed on all employees
- Access to COMPLY production infrastructure, including client relevant systems, is restricted to a small subset of employees whose access is based on need-to-know principles
- Employees are provided regular security training utilizing a third-party curriculum as well as frequent follow-up alerts and security reminders

Physical Security

COMPLY maintains infrastructure in the most technically sophisticated datacenters available, which are also used by some of the most security-conscious technology organizations and financial institutions, like Salesforce.com and Microsoft.

Physical security features include:

- Anonymous buildings with embassy grade car barriers and damage resistant construction
- Comprehensive access controls consisting of 24x7 staffing, one-time use ID cards, mantraps, biometric authentication, complete area video surveillance, silent alarms and roving security patrols
- Sophisticated environmental control systems including redundant electrical connections, independent power generation provided by onsite diesel generators with priority fuel resupply, battery backup, IR gas/leak detection systems, redundant physically separated Internet circuits
- Independently audited to SOC criteria
- Independent security assessment provided by third-party auditors, with results available upon request

Network Security

COMPLY employs proven security practices along with multi-level security products from leading security vendors.

Network security features include:

- 24x7 security operations center administered by a nationally recognized managed security services firm
- 24x7 incident response and management
- Latest perimeter firewall and intrusion detection systems coupled with network based intrusion protection together with 24x7 log monitoring and analytics
- Two-factor authentication for employee remote access to internal networks together with host lockdown to prevent unauthorized data transfer

Host Security

COMPLY uses well-known branded hardware products with proven reliability and security features.

- Vulnerability management program with periodic scans across COMPLY's infrastructure to detect insecure configurations or newly found vulnerabilities
- Third-party penetration testing to confirm infrastructure security posture
- Email threat defense provided by Mimecast

Application Security

COMPLY employs layered safeguards within all COMPLY systems, and implements security best practices including:

- Strong password policies including lockout and auditing
- One-way encryption for stored passwords
- Industry standard TLS encryption for user sessions
- AES 256 full database encryption
- AES 256 encryption for all feed data
- Granular supervisor and user permission options to permit minimum access needed to complete tasks
- Third-party code review against 100+ point threat model and OWASP top 10 criteria

Reliability and Recovery

COMPLY maintains disaster recovery safeguards such as:

- Backup datacenter located in a separate region from the primary datacenter
- Encrypted replication of COMPLY data between datacenters to ensure a backup of the most recent client data without the security and custody issues of removable storage
- Periodic failover testing to assure contracted mean time to recovery and recovery point objectives

Privacy and Confidentiality

COMPLY believes that principles of privacy and integrity lie at the core of everything we do as an organization. COMPLY listens to and understands its customer's concerns regarding the confidentiality of their business data and the privacy of the personal data they maintain. The organization:

- Maintains and routinely reviews its privacy policies and contractual commitments related to confidentiality
- Has implemented Data Privacy Addenda, EU Standard Contractual Clauses (SCCs), UK International Data Transfer Addenda (IDTAs) to adhere to GDPR
- Monitors the evolving world of data privacy to ensure it is prepared to implement and adhere to new regulations applicable to its business

Certifications and Documentation

- COMPLY is SSAE 18 SOC certified
- COMPLY third-party security assessment available upon request
- COMPLY Information Security policies available upon request