1010data ensures the protection of your data throughout its lifecycle

Security Standards and Practices

1010data takes a holistic approach to securing access and customer data. We do this with a multi-level approach that incorporates company policies, integrated security practices, compliance features, physical security, secure data transmission, and secure system design. As each customer need is unique, we are happy to consult with you on any specific security requirements.

1010DATA CORPORATE SECURITY POLICIES

1010data's technical controls strictly define who can access data. Key elements include:

- 1010data developers have access to databases only for their job, and access is monitored by 1010data's Security Operations team
- Business analysts are assigned to specific customers and only access data with the customer's permission
- Customer data is not allowed to be loaded by 1010data onto portable or removable storage, desktops or laptops
- Servers containing customer data are not directly reachable from the internet
- Firewalls and intrusion detection software are monitored 24 hours a day
- Security patches are installed promptly when applicable to our systems
- 1010data maintains complete, auditable logs of all user interactions involving customer data, including user account, IP address, and tables accessed

INTEGRATED 1010DATA SECURITY PRACTICES

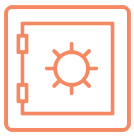
The way 1010data designs the platform makes the platform more secure and keeps our services and customer's data safe.

- 1010data provides customers with granular permissions to allow for users and role level control over access to tables, rows, and columns
- With a written agreement, 1010data can accept information restricted by applicable data privacy laws, including PII and HIPAA PHI

1010DATA COMPLIANCE FEATURES

The 1010data platform supports multiple compliance requirements:

- SOC 2 Type II Certified - dedicated information security director, two person approval for any security changes, confidentiality provision in our contracts (all data is 100% confidential by default and the customer has complete control over any party access to any information)
- HIPAA compliant - servers containing HIPAA PHI data comply with federal security standards and are held in locked cabinets with an audit trail for cabinet access
- Support for Single Sign-On (SSO) via SAML 2.0 authentication - customers that implement a SAML Identity Provider can authenticate user access



PHYSICAL AND LOGICAL SECURITY

1010data houses all physical servers at Equinix data centers. Equinix is an industry leader and imposes high standards for security and environmental controls. Equinix is annually audited for compliance and holds multiple compliance certifications, including ISO 27001, SOC 2 Type II, and HIPAA. Furthermore, 1010data limits access to physical servers to mission-critical IT staff only for physical maintenance and upgrades. IT staff do not have access to customerdata unless necessary to resolve customer issues.

Additionally, 1010data leverages Azure and Amazon Web Services (AWS), which have strict physical security controls for employees and third-party data center access. Rules include valid business justification, time-bound access, and an audited approval process. Both providers perform on-going regular threat and vulnerability reviews. Azure and AWS are certified for world-wide compliance, including ISO 27001, SOC 2 Type II, HIPAA, NIST 800, and GDPR.

DATA TRANSPORT SECURITY

Electronic transit of customer data and all electronic interactions between users and the 1010data platform is secure

- For browser interactions, transmissions use a Transport Layer Security (TLS) 1.2 or higher secured connections. TLS is the successor to the Secure Socket Layer (SSL) security standard
- Data import is performed using PGP-encrypted and signed batch files, which are sent over an encrypted connection using a Secure File Transfer Protocol (SFTP) session
- Data files transmitted to 1010data are automatically backed up for disaster recovery

1010DATA IS SECURE BY DESIGN

There are several aspects of the 1010data platform that make it inherently more secure. These include:

- The 1010data platform utilizes a novel stateful architecture that places each user in a unique dedicated instance of the database with a privately allocated working session
- 1010data is not an SQL or RDBMS database, therefore it is not susceptible to SQL injection attacks
- The 1010data platform can only be accessed via secure HTTPS, the industry-standard protocol used worldwide to secure Internet transactions