Trust & Security

We value security. For more information or if you have any questions, please contact us.

CONTACT US

Security is an integral component of our business. HqO's customers and users entrust us with their work-life information, and we aim to process and store that information thoughtfully and intelligently.

Our security team has designed and implemented a comprehensive information security management system (ISMS) program following the best practices described in ISO 27001 and NIST frameworks. The team aims to continuously improve the ISMS program alongside the business growth, reach, and input from various stakeholders including customers and regulators.

On this page, we describe the various security measures and compliance overviews at HqO. For more information about our security measures, please contact security@hqo.co.

COMPLIANCE

ISO 27001

HqO is ISO 27001:2013 certified. The certification covers the ISMS supporting the confidentiality, integrity, and availability of customer data, supplier information, and HqO's internal data related to developing, operating, and planning a workplace experience platform environment.

Download Certification for HqO →

Download Certification for Office App →

SOC 2

HqO has obtained the SOC 2 Type II report by an examination of an independent third party. The report helps understand the controls HqO has established to support operations and compliance. The report is available upon request.

Email to Request →

COMPLIANCE

PRIVACY & DATA PROTECTION

HqO's solution is compliant with various data protection laws and regulations where our customers are residing, such as GDPR, CCPA, and PIPEDA. View our Privacy Policy for more details.

HqO also leverages a number of third-party applications and services in support of the delivery of our solution to customers. We recognize that the company's information assets and vendor dependencies are critical to our continuing operations and delivery of services. As such, we have established a vendor management program that sets forth the requirements to be established and agreed upon when HqO engages with third parties or external vendors. For a complete list of HqO's sub-processors, please refer to our Data Processing Addendum document on our Legal Hub.

ORGANIZATIONAL SECURITY

TECHNOLOGICAL SECURITY

Frequently asked questions

COMPLIANCE

PRIVACY & DATA PROTECTION

ORGANIZATIONAL SECURITY

HqO maintains a comprehensive set of security policies and procedures which are communicated and accessible to all employees. We ask our employees during their onboarding and annually thereafter to read and understand these policies and procedures. We also plan, run, and continuously improve security awareness campaigns across the company to ensure all employees are aware of security best practices and how to best protect customers and other business information.

All policies and procedures that we have internally are bound to regular review at least annually. We also perform tests and compliance controls on all these areas to ensure that the measures are running effectively.

TECHNOLOGICAL SECURITY

Frequently asked questions

Does HqO collect, store, and process personal information (PII data) from the customers?

COMPLIANCE

PRIVACY & DATA PROTECTION

ORGANIZATIONAL SECURITY

TECHNOLOGICAL SECURITY

We host customer data on Amazon Web Services (AWS) infrastructure in the US East region data center located in Northern Virginia and the EU Central region data center located in Frankfurt, Germany. All primary instances of our infrastructure are replicated in real-time to secondary instances across multiple availability zones to ensure high availability service.

All data is encrypted during transmission and at rest. Backup snapshots of the database are captured at 5-minute intervals and retained for 30 days.

For ensuring the continuous security of our production environment, security vulnerability scanning is performed every 2 weeks using a third-party solution. Every year an external party performs a penetration test on our applications (web and mobile) and infrastructure. All identified observations are tracked and resolved according to the policy and procedure previously defined.

Frequently asked questions

Does HqO collect, store, and process personal information (PII data) from the customers?

We collect, store, and process a very limited amount of personal data from customers to deliver our service, such as name, work email address, and main work location.

Where does HqO store or host customer data?

HqO utilizes Amazon Web Services (AWS) as the application and data hosting provider. We use the US East Region data center located in Northern Virginia and the EU Central Region data center located in Frankfurt, Germany.

How does HqO ensure that the application is always available?

The primary instance of our application and database are replicated to a secondary instance for redundancy across multiple availability zones. Our infrastructure, app deployment, and connected services are all provisioned with code that increases the recoverability in the event of disruptions.

We also have defined and maintained a Business Continuity and Disaster Recovery Plan which is tested at least annually.

Please refer to this page for our service availability objective (SLA): https://www.hqo.com/sla/

Does HqO backup customer data regularly?

Backup snapshots of the database are captured at 5-minute intervals and maintained for 30 days. The restoration of backup data is performed regularly.

How does HqO manage employee access to customer data?

We have implemented a comprehensive policy and procedure for Access Management, which incorporates least privilege and need-to-know principles. User' access is reviewed regularly

Does HqO encrypt customer data for transportation and storage?

We always encrypt data-in-transit using TLS1.2+ and data-at-rest using AES 256.

Does HqO perform regular security testing on the application?

We perform penetration testing on our application and infrastructure at least annually. We also check our production environment for vulnerabilities using an automatic third-party security scanning tool every 2 weeks.

Does HqO use third-party suppliers or vendors to deliver its product and service?

We use third-party suppliers or vendors as part of application development and service production, such as Amazon Web Services (AWS) for hosting and Braze for notifications. As part of our risk management, we perform annual security risk assessments on these vendors.

Which user authentication method does HqO support?

At a minimum, we support username and password for user authentication. We also support Single-Sign-On (SSO) through SAML protocol.

Does HqO have procedures to handle security incidents such as data breaches?

We have defined comprehensive policies and procedures for handling security incidents, including the communication channel and methodology toward customers and regulators. We test our incident response procedure annually.

How long does HqO store customer data in the database?

We will only retain your information for as long as necessary to fulfill the purposes we collected it for, including for the purposes of satisfying any legal, accounting, or reporting requirements.