https://hypeauditor.com/legal/security/

Technical and Organizational Measures for Data Protection

Infrastructure

- All of our services run in the cloud. Hypeauditor does not run our own routers, load balancers, DNS servers, or physical servers.
- Our services and data are hosted in several data centers across Europe, including AWS, Digital Ocean, and Hetzner. Security measures taken by these data centers are described in the respective document:
    - http://aws.amazon.com/security/sharing-the-security-responsibility.
    - https://www.hetzner.de/pdf/en/Sicherheit_en.pdf
    - https://www.digitalocean.com/trust/faq/
- All of our servers are within our own virtual private cloud (VPC) with network access control lists (ACL's) that prevent unauthorized requests getting to our internal network.
- Hypeauditor uses a backup solution for datastores that contain customer data.

Data

- All customer data is stored in the European Economic Area ("EEA").
- Customer data is stored in multi-tenant datastores; we do not have individual datastores for each customer. However strict privacy controls exist in our application code that are designed to ensure data privacy and to prevent one customer from accessing another customer's data (i.e., logical separation). We have many unit and integration tests in place to ensure these privacy controls work as expected. These tests are run every time our codebase is updated and even one single test failing will prevent new code being shipped to production.
- Each Hypeauditor system used to process customer data is adequately configured and pathed using commercially-reasonable methods according to industry-recognized system-hardening standards.
- Hypeauditor engages certain sub processors to process customer data. These sub processors are listed at https://hypeauditor.com/legal/third-parties/, as may be updated by Hypeauditor from time to time.

Data Transfer & Storage

- Data sent to or from Hypeauditor is encrypted in transit using 256-bit encryption.
- All data transferred between our data centers is encrypted using industry-grade encryption.
- Our API and application endpoints are TLS/SSL only and score an "A" rating on SSL Labs' tests. This means we only use strong cipher suites and have features such as HSTS and Perfect Forward Secrecy fully enabled.
- We also encrypt data at rest using an industry-standard AES-256 encryption algorithm.

Authentication

- Hypeauditor is served 100% over https. Hypeauditor runs a zero-trust corporate network.
- We have two-factor authentication (2FA) and strong password policies on AWS, Digital Ocean and Hetzner to ensure access to cloud services is protected.

Application Monitoring

- All access to HypeAuditor applications is logged and audited.
- Bastion hosts are used to login to devices.

Security Audits and Certifications

- We annually engage with well-regarded third-party auditors to audit our code-base, and work with them to resolve potential issues.
- We use technologies to provide an audit trail over our infrastructure and the Hypeauditor application. Auditing allows us to do ad-hoc security analysis, track changes made to our setup and audit access to every layer of our stack.
- Information about our cloud hosting security certifications and obtaining copies of security reports are available at:
  http://aws.amazon.com/compliance/pci-data-privacy-protection-hipaa-soc-fedramp-faqs/
  https://www.digitalocean.com/legal/certifications/
  https://www.hetzner.com/unternehmen/zertifizierung/

Payment Processing

- All payment instrument processing for purchase of the Hypeauditor services is performed by Stripe and Paypal. For more information on Stripe's security practices, please see https://stripe.com/docs/security/stripe. Paypal's security policy is located here https://www.paypal.com/re/webapps/mpp/paypal-safety-and-security

Confidentiality

- We place strict controls over our employees' access to your data and are committed to ensure that any customer data is not seen by anyone who should not have access to it. All of our employees and contract personnel are bound to our policies regarding customer data privacy and security and we treat these issues as matters of the highest importance within our company.

Personnel Practices

- HypeAuditor conducts background checks on all employees before employment, and employees receive security training during onboarding as well as on an ongoing basis. All employees are required to read and sign our strict data security and privacy policy covering the security, availability, and confidentiality of our services.