

Information Security at Typeform

A Guide For Customers

Introduction

At Typeform, we understand that security is a top priority for our customers. We are committed to protecting your data by implementing a comprehensive security program that aligns with our compliance frameworks, regulatory requirements, and industry standards. This document provides a summary of our security, compliance, and privacy practices to give you confidence in our platform and services. For more detailed information on Information Security, please refer to our full documentation available in our Trust Centre.

Terminology Summary

The Typeform platform is used for building online forms and surveys, and analysing the data collected. These services are governed by our Data Processing Agreement.

We process the following data on your behalf for that purpose:

- **Response data:** the data you collect from respondents to your typeforms. The type(s) of data collected is fully at the discretion of the customer.
- **Forms data:** which includes the questions you create, files uploaded to forms, your knowledge base if used, etc.
- **All other customer data**: which includes personal information, and payment details

For a full list of all data processed, please see our help article: What other companies do we share data with.

1. Governance & Certifications

Our security program is compliant with major global standards, which are annually independently audited to provide external assurance.

- **Security Frameworks:** We maintain an information security program based on security standards and frameworks including NIST and OWASP.
- **Certifications:** We are certified with SOC 2 Type 2, ISO 27001, 27017 and 27018, and HIPAA, with our reports available for download on our Trust Centre.
- **Compliance:** We comply with a variety of laws and regulations, including GDPR, CCPA, and HIPAA.

For a full list of our certifications, and their accompanying reports, please visit our Trust Centre.

2. Data Security & Encryption

We employ multiple layers of defence to protect customer data, at rest and in transit.

- **Data Hosting:** Our infrastructure is hosted on Amazon Web Services (AWS).
  - For US customers, our primary hosting is in North Virginia (us-east-1), with backups in Oregon (us-west-2).
  - For EU customers, our primary hosting is in Frankfurt (eu-central-1).
  - For more details on AWS' Data Centre controls, please visit https://aws.amazon.com/trust-center/data-center/our-controls/
- **Data Encryption:**
  - **At Rest:** Personal data is encrypted using AES-256 bit encryption.
  - **In Transit:** Personal data is encrypted in transit using TLS 1.2 or greater.
- **Data Segregation:** Customer data is logically separated within our databases and S3 buckets, ensuring that your data is only accessible by you.
- **Data Retention:** Data is retained for as long as necessary, as determined by the customer, and in compliance with applicable laws.
- **Data Deletion:** Data can be deleted by customers at any time, at the account or form level, and is disposed of securely.

3. Access Management

Access to our corporate and production environments is strictly controlled to follow the principle of least privilege and need-to-know.

- **Employee Access:** Access to the corporate network requires a company-managed device, SSO, and MFA. Access to production systems requires VPN and MFA.
- **Password Policy:** Our password policy requires a minimum length of 12 characters, with complexity requirements for lower case, upper case, numbers, and symbols. Passwords cannot be reused from the last five passwords.
- **Session Management:** Sessions automatically expire after a period of inactivity, not exceeding a half-hour.

4. Incident Response & Vulnerability Management

We have established processes to proactively identify and address security risks and to respond effectively in the event of an incident.

- **Logging and Monitoring:** Security events are centralised in our SIEMs where alerts are viewed and monitored.
- **Vulnerability Scanning**: Vulnerability scans are performed weekly and identified vulnerabilities are patched or remediated by severity, in accordance with our policy timelines.
- **Penetration Testing:** Penetration tests are conducted annually by an independent security firm. A summary of our most recent report can be found here.
- **Vulnerability Disclosure Program (VDP):** We have a VDP hosted through HackerOne. You can find more information on how to report a security vulnerability on our help page: How to report a security vulnerability to Typeform.
- **Incident Response Plan:** We have security incident response policies and procedures that complies with articles 34 & 35 of GDPR, and is tested annually.

5. Organisational Security Measures

- **Third-Party Risk Management:** Our vendor management program includes a security and privacy risk assessment before the contractual relationship begins, as well as an annual re-assessment.
- **Endpoint Security:** All company-issued devices are managed through an MDM solution, with multiple layers of defence to protect against malware and data exfiltration, including EDR and AV, monitoring and encryption.
- **Secure Development:** We have a Secure Software Development Lifecycle (S-SDLC) following best practices from OWASP to ensure the necessary security and privacy measures are in place.
- **Business Continuity and Disaster Recovery:** Backups are maintained and tested annually for disaster recovery purposes. Our Recovery Time Objective (RTO) is 24 hours, and the Recovery Point Objective (RPO) is one hour for response data and 24 hours for all other data.

6. Platform Information

- **API:** We offer an API, which can be found at: https://www.typeform.com/developers/.
- **Uptime:** We offer a 99.5% commercially backed service level agreement (SLA). Our public status page can be found at: https://status.typeform.com/.
- **Customer Access:** We support SSO with identity providers like Okta, OneLogin, and Azure, using SAML, OAuth, or OpenID. Customers can also enable MFA through their SSO provider. For more information, please visit our help article: Set up SSO authentication for your account.
- **Roles and Permissions**: Account owners can control user access, permission levels and authentication methods for their accounts. Please visit our help article: Access management: roles, access & permissions
- **Logging**: Logs are available for customers and can be exported from the platform: https://help.typeform.com/hc/en-us/articles/25907779354260-Organization-activity-log
- **Backups**: We provide 15-day backups of our customers' accounts, allowing data to be recovered if required. Please visit our help article: Backup and restoration procedures
- **Email preferences**: In accordance with the GDPR, customers can control what emails they receive from Typeform. Please visit our help article: How to manage your email preferences.
- **Data subject rights**: For information on how to exercise your privacy rights, please see visit our help article: How do I exercise my GDPR rights