Entrusting your data to a third-party service provider requires rigorous security measures. The security and integrity of your data is critically important for us, and we’ve built our services around this idea.

This article describes the technologies and processes that we use to secure your data, and explains our security culture. We need to be clear and understandable from a legal perspective – unfortunately that doesn’t always make for the simplest explanations. If you find anything hard to understand, please get in touch using the Contact Support button at the bottom of this page.

Physical security

Typeform’s infrastructure is hosted by Amazon Web Services (AWS). Our main servers are located in Virginia, USA and backup servers are located in Frankfurt, Germany. They are compliant with security and privacy standards, including the Privacy Shield. Our offices and facilities also include 24 hour access monitoring, cameras, visitor logs and door entry pin requirements.

So basically, our data is hosted and backed up in safe places, and our offices are secure.

Network security

All our environments are hosted in a Virtual Private Cloud (VPC) in Amazon Web Services. Our production networks are separated between public and internal services. No inbound internet traffic is allowed on the private subnets, and all application servers only reside in private subnets without public IP addresses. Only Amazon managed and maintained load balancers have ingress access to the application internal servers. Tight security groups control inbound and outbound access to the servers.

Firewalls and Intrusion Detection Systems (IDS) are installed at the edge locations to provide an additional layer of internal and external network security.

In short, all the networks we use are as secure as we can manage. Access to our servers we use is strictly limited, and no outside traffic is permitted on them.

Architecture overview

Typeform is designed to be both scalable and fault-tolerant. If one machine fails, another will be ready to take over immediately. This redundancy is found in all levels of the platform.

Also in alignment with AWS best-practices, a Multi-availability Zone architecture is in place. Should an entire Availability Zone fail, remaining machines in the functioning availability zone have the capacity to run the entire service.

Redundant backups of critical data are also in place and moved to a different account to ensure business continuity in case of disaster.

Access control

Access to Typeform resources is only permitted through secure connectivity (e.g.,VPN, SSH bastions) and in some cases requires multi-factor authentication. We follow the principle of least privilege, and existing access is audited on a regular basis to ensure that employees only have the permissions necessary to perform their duties.

This means employees can only access Typeform systems with an extra-secure connection. And as soon as anyone leaves the company, their access is blocked.

Security policies and awareness

We have a comprehensive set of information security policies to ensure compliance, and to guide our employees and contractors in making the right security decisions. Examples include a password policy, data protection policy, acceptable use policy and backup policy amongst others. We review and update them annually.

We have non-disclosure agreements with all employees and contractors, and run various security awareness training courses within the company.

This all means that all of us here at Typeform follow internal security guidelines. We get training on these, and they are updated regularly.

Penetration tests

As part of our security strategy, we hire well recognised security research firms to perform gray-box penetration tests on the our platform. Vulnerabilities and findings are ranked according to severity and prioritized accordingly.

This means we let security experts come in and try to break stuff, to help us find any weaknesses.

Data protection measures

Once your information entered Typeform's systems, it's secured with multiple levels of encryption and access controls. We encrypt your data in-transit (end-to-end, including within the virtual private cloud at AWS) using secure TLS cryptographic protocols (currently TLS 1.0, 1.1 and 1.2 supported).

Warning! To improve our our security measures, we will be deprecating support for TLS 1.0 and 1.1 in late 2018.

The Advanced Encryption Standard (AES) is used with a 256-bit key to encrypt data at rest including the backups of the information.

Access to customer data is restricted based on role: only authorized employees have access to data. Access is revoked immediately upon employee termination.

Data is retained for as long as you keep it in our systems. Once you have deleted the data or after the end of the engagement, it will be retained in our systems and backups for thirty five days until is completely deleted. Data that we have in other third party systems and logs can take up to ninety days for full deletion.

Compliance

Typeform is compliant with the Payment Card Industry's Data Security Standards (PCI DSS 3.2) and can therefore accept or process credit card information securely in accordance with these standards always using the Payment block. Typeform re-certifies this compliance annually with our third party payment processor. Typeform is currently working towards achieving other security certification and standards.

Security monitoring and auditing

Typeform collects application, infrastructure and systems logs in a centrally managed log repository for monitoring, troubleshooting, security reviews, and analysis by authorized personnel. Logs are preserved in accordance with regulatory requirements to assist in the case of a security incident.
We have to keep some data by law, and we do that.

Shared Responsibility

Protecting access to your data and responses requires that as Typeform customer, you maintain the security of your account by using secure passwords and protecting them as necessary. Find out more about good password behavior.

At Typeform we take the security and privacy of our user data very seriously. Here is a comprehensive overview of our security measures and privacy policy.

Where do you store my data and how is it protected?

- All data is hosted on Amazon's AWS service. Our main servers are located in Virginia, USA and backup servers are located in Frankfurt, Germany. You can read more about AWS here.
- All Typeform employees are bound by strict confidentiality agreements.
- TLS is used to secure all data in transit.
-

Do I retain ownership of my typeforms and their content?

Yes, the typeforms you create are yours! We will not share your data with 3rd parties unless:

- It's required by 3rd parties you have asked to use. (Zapier integrations for example!)
- We obtain your express permission.
- We are required by law.

Cookies

The cookies Typeform uses are small text files that store data made available by your web browser, such as language preference. This information helps us give you
a better experience.

- Cookies do not provide us with any personally identifiable information.
- You can change or block cookies in your browser settings.
- Cookies do not harm your computer or impact your online security.