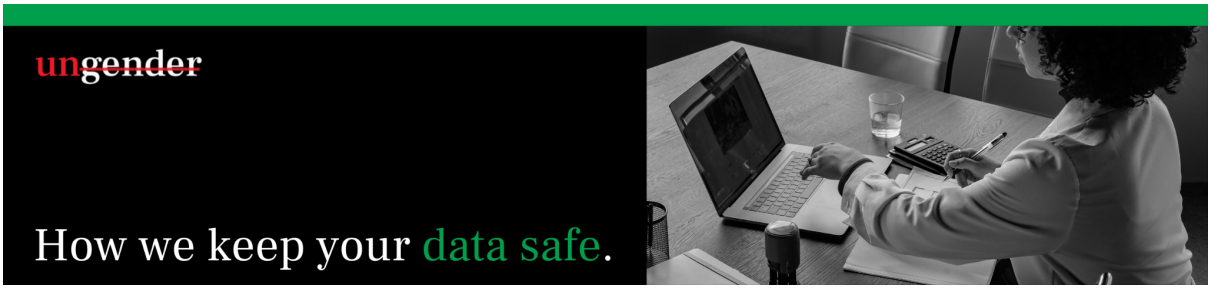
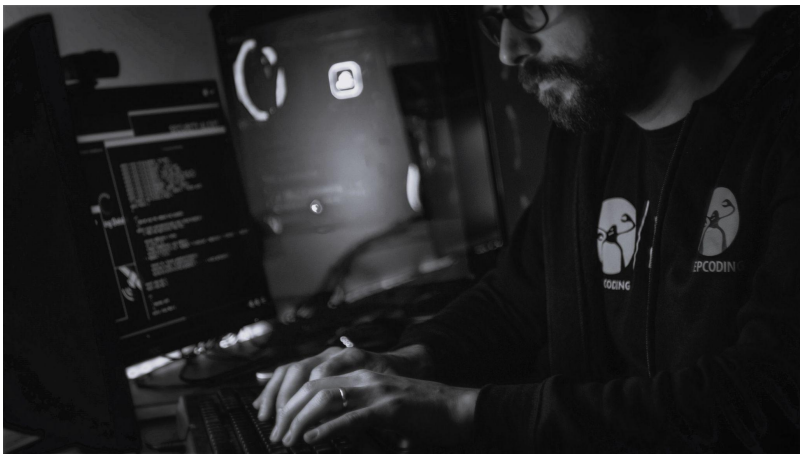


Conduct maintains an internal security threat model and commissions internal penetration testing at regular intervals to ensure the security of the platform.

Here's how we do it:

Certification and licenses



Ungender is ISO 27001:2013 certified and we comply with a set of international industry procedures and policies relating to information security management.

Ungender has been audited against SOC2 compliance. It is a voluntary compliance standard for service organizations and is based on security, availability, and confidentiality.

We operate a security program that includes regular security audits, vulnerability scans, internal penetration testing, automated monitoring, and security training for our staff.

We continually monitor developing standards and legislation to ensure that Ungender adheres to the security requirements of leading industry bodies.

Trusted and secure hosting infrastructure

Our servers are located within the United States, in AWS (Amazon Web Services) data centres that are ISO 27001, SOC 1, and SOC 2 certified.

Customer data is stored in multiple locations in our hosting provider's data centres to ensure availability. We operate a business continuity program that includes backup and restoration procedures that are regularly reviewed and tested.

AWS data centres have round-the-clock security and strict controls for physical access.

Data encryption: Transit and Rest

Ungender utilises some of the most advanced technologies for Internet security available today. When you access the application using a browser, Transport Layer Security (TLS) technology is designed to facilitate privacy and data security for communications over the Internet using Encryption, Authentication, and Integrity.

At rest, all the data is encrypted using the 256-bit advanced encryption standard (AES-256).

We regularly monitor changes to the cryptographic landscape and implement best practices as they evolve.

Application security

We provide regular training for our engineers in secure coding, that covers key OWASP security risks, common attacks, and security controls best practices.

As part of the software development process at Ungender, code and configuration changes are thoroughly reviewed. Before being deployed, these changes are tested using a quality assurance process to help ensure an expected, consistent, experience across supported devices and platforms.

Organizational security and practices

All Ungender employees are vetted before joining and are required to complete quarterly security awareness training. Training topics include information security,

data privacy, and risk mitigation.

Employees are prohibited from using unauthorised software or portable media. Any new software goes through a request-analyse-approve mechanism.

Administrative access to systems within the production environment is limited to engineering staff with a specific need to support our services. Access to our servers is monitored and audited, we regularly review system and access logs.

Data storage and removal

To minimise the chances of your information being hacked or stolen, we only store data when absolutely necessary.

Our Data Retention Policy and Access Control Policy (both available on request) clearly outline what happens with our customer's data and the measures we take to ensure that data is stored securely.

Ungender has daily automated backups, which are retained for 7 days. All backups are stored on encrypted storage, with access limited to key people on the Ungender team.

Log data is stored for 90 days, but it doesn't contain any personal data.

Backups are located where our servers are hosted: AWS's US-East 1 location (North Virginia).