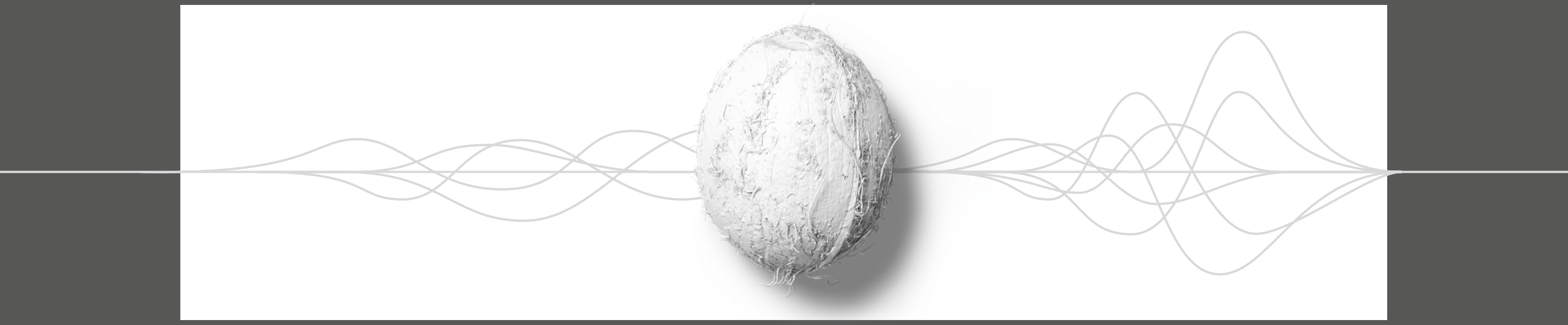
whistlelink

# Your data stays secure with us



When it comes to something as sensitive as whistleblowing, we know exactly how critical data security is. We leave nothing to chance. Whistlelink is built with the tightest security levels to protect your data, organisation and the whistleblower. Always.

## Hosted in the European Union

As a Swedish owned company, Whistlelink hosts all its servers in the EU. By storing data in the EU, we guarantee compliance with the GDPR and all data relating to the whistleblower stays within the European Economic Area (EEA).

Schrems II, a ruling from the Court of Justice of the European Union (CJEU), invalidated the EU-US Privacy Shield because it doesn't believe the US provides sufficient data protection levels. Companies transferring personal data outside of the EEA may not be GDPR compliant.

## ISO certified, 27001, Information Security

SP
CERTIFIED
ISO 27001
Information security
management systems
RI.
SE

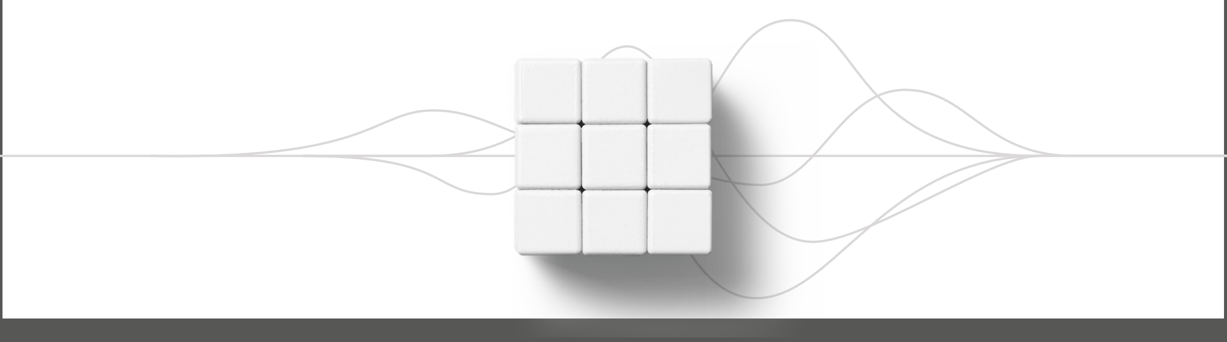
Whistleblowing Solutions AB, the company behind Whistlelink, shows commitment to data protection and minimising security risks with ISO/IEC 27001 certification. The international standard for an information security management system. This confirms that we handle data security correctly and it is always a part of our product and technical development.

## GDPR compliant

As we only host data on EU-based servers, the data that we store for you is also compliant with the GDPR. So that's one less thing to think about. Data is also automatically deleted according to the time constraints set out in the GDPR.
Full details in our Privacy Notice.

whistlelink

# Our measures for data protection



This overview refers to the current minimum security levels. However, Whistleblowing Solutions is committed to continuously improving its data security, whereby it will adapt measures to safeguard from new outside threats and utilise newly available data protection tools.

## Organisational measurement of data

Whistleblowing Solutions data security activities are based on current legislation and the company's governing documents which are determined by the Company's CEO or Board of Directors. The company's Information Security Officer is responsible for leading and coordinating data security within the business, which includes the following:

- Responsibility for policies and procedures relating to data security and its compliancy
- Conducting risk analysis and management in relation to data security
- Coordinating activities to ensure data security compliancy
- The overall requirements of various security controls
- Spreading knowledge about data security throughout the organisation
- Documenting and coordinating non-conformances

## Technical measurement of data

- Encryption of case data in transit and at rest
- Secure multi-factor verification
- Action and data logs
- Strict user access control
- External penetration testing
- Redundancy of data