whistlelink

SP CERTIFIED ISO 27001 Information security management systems RI. SE

Organisational and technical measures for data protection

Introduction

Whistleblowing Solutions handles large amounts of data for itself and on behalf of others. This applies, among other things, to personal data. Whistleblowing Solutions' activities are regulated by various laws, and internal guidelines which can be found in company documents such as plans, policies and procedures. Whistleblowing Solutions is certified according to ISO 27001.

This summary outlines how Whistleblowing Solutions acts to fulfil its obligations and to minimise the risks associated with the processing of data.

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.

In cases where Whistleblowing Solutions uses subcontractors, it will ensure the subcontractors implement the required security controls to comply with the organisational and technical measures.

Organisation

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

Whistleblowing Solutions maintains guidelines on how all employees, including subcontractors, should act to minimise data security threats. These guidelines are well circulated, understood and implemented by all concerned.

General information on technical security measures

The basic principle of technical security measures at Whistleblowing Solutions is that the level of confidentiality determines the requirements of the security controls (e.g., type of authentication, cryptographic protection, etc.). The levels of confidentiality are:

- Open - data accessible by all, inside and outside the company
- Internal - data accessible by employees only
- Confidential - Sensitive data (such as personal data) accessible by a limited number of employees only

Continuity planning

In the event of a serious incident, such as an office or data centre fire, Whistleblowing Solutions has a data processing crisis and contingency plan in place, to minimise disruption to operations and commitments to customers.

Access / Authorization

Data is protected from all forms of unauthorised processing, such as unauthorised access, unauthorised distribution and unintentional or intentional destruction.

Access to confidential data is restricted to persons working at Whistleblowing Solutions. Each individual’s access is limited to only the data and permissions needed to carry out the task.

Whistleblowing Solutions has control systems in place to prevent unauthorised access to confidential data. Access is through personal user-IDs, and access to secret information, such as sensitive personal data, requires specific authorisation. Two-factor authentication is used when logging in to all systems that contain personal data.

There are designated functions for approving, amending, or withdrawing authorisations. Authorisations that are not used will be deactivated.

Physical and environmental protection

Whistleblowing Solutions restricts access to physical premises and facilities, which contain systems processing data, to authorised persons only. The premises are protected against fire and theft.

Technical security

Whistleblowing Solutions has security measures in place to reduce the risk of harmful software being executed in the IT environment. These include firewalls, layered networks, and the latest antivirus software, with updated versions on all workstations. A combination of antivirus software and other measures are applied to servers.

Backup and recovery

Whistleblowing Solutions makes regular backups of data, i.e., daily.

The backup and data recovery procedures are stored in a secure location separate from the primary IT equipment that processes the data.

Compliance with other GDPR requirements

Whistleblowing Solutions will, upon request, assist the Data Controller to amend/update personal data for which they are responsible.

Unless agreed otherwise (or it is prevented due to legal reasons), Whistleblowing Solutions will delete all related data following cancellation of an agreement.