

# Data Security Documentation

## 1. Purpose and status

This document describes the technical and organisational measures Insurely AB ("Insurely") applies to protect customer data and personal data in the Insurely service, as referred to in the Data Processing Agreement (DPA) and article 32 of the GDPR.

Insurely may update it from time to time, provided that the overall level of security is not materially reduced. Each version is dated and listed in the version history at the end, and the version applicable on a given date is available on request.

The measures are described at principle level. Detailed technical information, such as test reports and certificates, is available on request under confidentiality.

## 2. Governance and organisation

Insurely manages information security through a documented information security management system aligned with ISO/IEC 27001. It includes:

- Security policies that are approved by management and reviewed at least annually
- Defined security responsibilities, including a person accountable for information security
- Regular risk assessments of the service and its suppliers
- An ICT risk management framework in line with DORA

## 3. Personnel

Only employees, consultants and other personnel who need access to customer data to perform their work are given access, and only to the extent needed.

- Personnel are bound by confidentiality undertakings, which continue after the engagement ends.
- Personnel receive security and data protection training when they join and annually after that.
- Access rights are changed when a role changes and removed without delay when the engagement ends.

## 4. Access control

Access to systems and customer data is restricted by role and granted on a least-privilege basis.

- Every user has a personal account, and shared accounts are not used for access to production systems.
- Multi-factor authentication is required for administrative and production access.
- Privileged access is limited to named personnel, and its use is logged.
- Access rights are reviewed at least quarterly.
- Sessions time out automatically, and repeated failed sign-ins are blocked.

## 5. Encryption and handling of credentials

All customer data is encrypted in transit and at rest.

- Data in transit is protected with TLS 1.2 or higher.
- Data at rest, including backups, is encrypted with AES-256 or equivalent.
- Encryption keys are managed in AWS KMS and access to them is restricted and logged.
- Credentials, tokens and consent records used to collect data from data sources on an end-user's behalf are stored encrypted, used only to provide the service, and deleted immediately after the session is completed.

## 6. Hosting, infrastructure and network security

The service is hosted with the sub-processors listed in the DPA. Physical security of the data centers, including access control, surveillance and power supply, is provided by those hosting providers, which hold independent security certifications.

- Networks are segmented and protected by firewalls, and only the traffic the service needs is allowed.
- Production, test and development environments are separated.
- Customer data is logically separated from Insurely's own data and from other customers' data.
- Production customer data is not used in test or development environments.

## 7. Secure development and change management

Changes to the service follow a documented process.

- Code changes are reviewed by a second person before release.
- Changes are tested before they reach production, and releases can be rolled back.
- Dependencies and code are scanned for known vulnerabilities.
- Secrets, such as keys and passwords, are kept out of source code and stored in a managed secrets store.

## 8. Vulnerability management and security testing

Insurely tests the effectiveness of its security measures regularly.

- Systems are scanned for vulnerabilities, and security patches are applied in line with our SLA.
- Penetration tests are carried out by an independent party at least annually, and findings are remediated based on risk.
- Summaries of test results are available to customers on request under confidentiality.

## 9. Logging, monitoring and incident management

Access to and changes in systems that hold customer data are logged, and the logs are protected against alteration. Systems are monitored, and alerts are followed up by designated personnel.

Insurely has an incident response procedure that classifies incidents, assigns roles and requires a review after each significant incident.

- A personal data breach affecting a customer is reported to the customer without undue delay and no later than 48 hours after Insurely becomes aware of it, as set out in the DPA.
- For customers covered by the DORA schedule, ICT incidents are handled as stated there.

## **10. Availability, backup and recovery**

The service is protected against accidental loss and destruction. Availability commitments are set out in the Service Level Agreement.

- The infrastructure is built with redundancy across more than one data center or availability zone.
- Backups are taken at least every 4 hours, encrypted, and stored separately from production.
- Recovery procedures are documented and tested at least annually.
- A business continuity and disaster recovery plan is maintained and reviewed regularly.

## **11. Deletion, suppliers and premises**

**Deletion.** Personal data is deleted at the times set out in the DPA and its appendix, using secure deletion methods.

**Suppliers and sub-processors.** Suppliers are assessed before they are engaged, are bound by written agreements with data protection and security terms equivalent to those in the DPA, and are reviewed regularly. Changes to sub-processors are notified as set out in the DPA.

**Premises and devices.** Offices are protected by access control, and visitors are registered and accompanied. Work devices are managed, with disk encryption, anti-malware protection, automatic screen lock and the ability to be remotely wiped.