PRIVACY AND SECURITY DOCUMENTATION

Published: 2025-10-01

1. INTRODUCTION AND SCOPE

1.1 This document describes the technical and organizational measures implemented by Tink to ensure security and privacy compliance and supplements the Master Service Agreement (as updated from time to time) or other agreement between Customer and Tink governing Customer's use of Tink's Services (the "Agreement"). It covers all Tink Products and Services unless otherwise specified in this document or in the Documentation. All capitalized terms in this Privacy and Security Documentation shall have the meaning ascribed to them in the Agreement, unless otherwise defined herein.

2. INFORMATION AND CYBERSECURITY MEASURES

2.1 **Governance Framework**. Tink, as an Affiliate of Visa Inc., has adopted the Visa Information Security Policy and associated Visa Key Controls, which are aligned with the ISO/IEC 27002 standard. These function as the framework for information security activities at Tink and define requirements for the safeguarding of the Services and any Customer Data (including, where relevant, Personal Data). Tink's compliance with these policies, guidelines and procedures on a day-to-day basis is ensured by a dedicated security function that also oversees Tink's security operations. Tink's security operations are reviewed by internal stakeholders and additionally audited by independent third parties at least annually.

2.2 **Information Classification**. Tink classifies its information so that it is ascribed the right level of protection. The classification and criticality take into account the possible impact of the lack of confidentiality, integrity and availability of the information.

2.3 **Information Security Risk Management**. Tink has defined and implemented an Enterprise Risk Management Framework ("ERMF") that supports the achievement of Tink's objectives by bringing a consistent and pragmatic approach to risk management for identifying, assessing, treating, monitoring, and reporting risks. This process is performed at least annually on an enterprise level to identify, assess and manage information security risks. The consolidated results of the information security risk assessments as well as the risk register are reported to top management as part of the yearly management review process.

2.4 **Tink Employee Access Management**. Access to Customer Data as well as any internal systems within Tink is granted on a need-to-know basis and following the least privilege principle, according to formal access controls. Access to systems is reviewed at least annually, or when any major change to systems occurs. Tink has formal offboarding procedures and access is revoked as soon as an employee is offboarded. Tink uses federated access management technologies anywhere possible (i.e., Single-Sign-On) and/or multi factor authentication if applicable and according to the sensitivity of the information systems and the data being stored or processed on them.

2.5 **Tink Customer Access Management**. Tink has enforced industry best practices for Customer passwords on any customer facing web applications (e.g., minimum password length, secure storage, account lockouts based on a set of parameters such as failed login attempts). Customer API access keys to the Tink platform also follow industry best practices (e.g., OWASP) in terms of key length, randomness, storage and revocation.

2.6 **Network security**. Tink has deployed a zero-trust architecture for its corporate access network based on which there is no reliance on network authentication. Nevertheless, Tink uses strong wireless encryption protocols for its office premises and segregates the network for guest and employees. Tink does not offer wired network access to its employees. For its production systems and networks, Tink follows the principle of least access principle and applies micro-segmentation between its information systems.

2.7 **Data Segregation**. Tink operates a multi-tenant environment which is designed to segregate and restrict access to Customer Data based on business needs. Tink offers a logical separation between Customer Data based on distinct identifiers which enable the use of customer user role-based access control. Moreover, Tink maintains separate environments for production and non-production (e.g., testing, staging) use cases making it possible to segregate data with different security sensitivity effectively.

2.8 **Data Encryption and Pseudonymization.** Tink always ensures the secure storage and transmission (i.e., in transit and at rest) of Customer Data with the extensive use of modern encryption technologies appropriate for the different use cases. Tink uses encryption in its products and services, following best practices and procedures for encryption key algorithms and key management. In addition, Tink implements pseudonymization measures when deemed relevant and appropriate.

2.9 **Application Security**. Tink adheres to a set of modern application security standards relating to secure software development. Tink incorporates industry best practices, including security design reviews and threat modelling as well as technologies including source code composition and static analysis tools. In addition, Tink has defined its own Secure Software Development guideline (based on OWASP's Application Security Verification Standard) and frequently provides security training to the members of the Engineering department on application security subjects.

2.10 **Security Logging, Monitoring and Intrusion Detection**. Tink employs an observability platform where logs from production and non-production systems are collected. These logs include application, infrastructure and network level information in order to correlate relevant information related to user activity (both Tink Employee and Tink Customer). Tink also aggregates a large part of these logs which are security relevant (e.g., for security incident management and forensics purposes) into a Security Incident & Event Management (SIEM) infrastructure so as to detect anomalies (e.g., suspicious or unauthorized user activity) which indicate possible intrusions. The SIEM infrastructure is deployed in a separate environment accessible only by authorized personnel and implements measures to guarantee the data integrity of the logs and prevent tampering. The SIEM infrastructure triggers alerts when there are strong indications that a detected security event might lead to a security incident. These alerts are monitored by a dedicated security team.

2.11 **Security Incident Management**. Tink leverages a Security Incident Management program, which includes appropriate incident management responsibilities and procedures to ensure identification, response, and reporting of security incidents. The program is reviewed regularly to ensure that recommended best practices are followed. Plans for the incident management program are exercised on a regular basis

2.12 **Endpoint Security**. Security controls are deployed via a mobile device management solution to manage and monitor all employee devices in order to prevent attacks (e.g., anti-malware software) and to enforce security controls (e.g., password policy, software patching).

2.13 **Physical Security**. Tink implements measures to ensure that only authorized individuals have access to Tink's premises or locations where the Services are performed or where Customer Data is stored, processed or transmitted.

2.14 **Business Continuity and Disaster Recovery**. Tink has a well-defined, documented and tested Business Continuity Management (BCM) framework which consists of Business Continuity, Technical Recovery and Crisis Management Plans. The framework aims to ensure efficient and timely recovery efforts in a structured and methodical manner. Business Continuity and Disaster Recovery exercises are conducted at least annually.

2.15 **Backup**. Tink has clearly defined, documented controls related to backup and redundancy of the Services and any Customer Data. Backup and restoration capabilities are tested at least annually.

2.16 **Secure Deletion**. Tink ensures the secure deletion of Customer Data upon termination of the Agreement in accordance with industry best practices.

2.17 **Penetration Tests**. Tink conducts penetration testing internally as part of its operations and with security consultants at least annually.

2.18 **Vulnerability and Patch Management**. Tink implements a multi-layer vulnerability management program where vulnerability scanning is performed on the network perimeter, cloud configuration, operating system, container and application layer. Tink uses an industry accepted vulnerability scoring framework (CVSS 3.0 or above scoring). Any detected issues are assigned severity ratings and remediated as per timelines defined by severity.

2.19 **Third-Party Supplier Management**. Tink maintains control and operational management of the Services and relies on its trusted cloud or hosting providers to support delivery of the Services (as set out in the Agreement). Tink utilizes a Third Party Lifecycle Management process to ensure that suppliers' information security & risk management practices align with stringent security requirements based on security industry standards (e.g., ISO/IEC 27001, CSA), and to perform continuous monitoring of suppliers. These reviews include financial checks, confirmation of data security requirements (e.g., PCI DSS, SOC reports, etc.) and business continuity requirements**.** Periodic holistic risk assessments are conducted based on the suppliers' risk tiering.

2.20 **Security Awareness**. Tink ensures that all employees regularly receive security awareness training to be able to fulfill their security responsibilities.

3. PRIVACY

3.1 **Control of Processing**. Tink implements technical and organizational measures to ensure that personal data is processed only in accordance with the Customer's instructions and in accordance with the Agreement.

3.2 **Customer Controls**. Tink provides technical controls in the Services for customers to be able to edit, delete and extract copies of Customer Data relating to End-Users. The controls are made available through Tink's API and/or the Customer's Account in the Site as further described in the Documentation.

3.3 **Data Minimization**. Tink implements measures to minimize the amount of Personal Data processed in products with respect to how those products are offered generally to our customers, and Customer is responsible for assessing the suitability with respect to its specific use case.

3.4 **Data Quality**. Tink's products generally make use of data from financial institutions and consequently, Tink's products rely on that data and the format in which it is provided to Tink. Depending on the product, we implement measures to increase the quality of that data by cleaning and standardizing it.

3.5 **Accountability**. Tink has adopted measures for ensuring accountability, such as implementing data protection policies, operating documented information security management controls, maintenance of a record of processing activities and appointing a Data Protection Officer.

3.6 **Personal Data after Termination.** Tink will delete all Personal Data after the termination of the Agreement within 30 days, unless otherwise required by applicable laws.

3.7 **Privacy Notice**. Tink adheres to its Privacy Notice for any Personal Data processed by Tink as a Data Controller. For clarity, Personal Data in Customer Data is governed by the Agreement.