Supplier Technical and Organisational Measures

Author: Georg Chapman

Date: February 2025

Version Number: 1.0

Contents

Executive Summary

At Keyloop, safeguarding sensitive information is not just a regulatory necessity. For us, it is a foundation for fostering trust with our customers, partners, and stakeholders. As such we expect our suppliers to share this commitment to security, ensuring that all interactions with our systems, services, and data remain secure and compliant.

Suppliers must proactively address evolving cybersecurity threats by adhering to industry best practices, regulatory frameworks, and advanced security technologies to maintain a resilient security posture. Transparency, accountability, and continuous improvement are at the core of our security expectations.

Purpose & Scope

This document outlines the technical and organisational measures (TOMs) that our suppliers must implement to ensure the secure and compliant processing of Personal Data. These measures ensure an appropriate level of security, including the ongoing confidentiality, integrity, availability and resilience of data processing systems and services.

These Supplier Technical and Organisational Measures are listed in the Supplier Hub which provides further information regarding the way in which Providers will process Personal Data when providing Services under the Relevant Contract. Unless otherwise defined in this document, terms used in this document shall have the meanings given to them in the Standard Purchase Order Terms and Conditions or Data Processing Agreement, each being available at https://www.keyloop.com/legal-documentation.

Confidentiality

1. Access Control and Authentication

- The Provider must implement a risk-based authorisation and authentication framework to ensure that only authorised persons can access and read Personal Data:

  - This framework should consider the least privilege access principle, ensuring that access to Personal Data is strictly limited to what is necessary for the provision of contracted Services; and
  - This framework should encompass physical, logical, and data access controls.
- Multi-factor authentication (MFA) must be implemented when any Provider is accessing Personal Data or IT systems processing and storing Personal Data
- Access controls must be implemented at the network, infrastructure, and application layers to ensure Personal Data is accessible only for approved purposes

2. Encryption and Data Protection

- Encryption must be applied to Personal Data in transit and at rest using industry-standard algorithms:
  - Data at rest must be encrypted using full-disk encryption or database-level encryption where applicable; and
  - Secure encryption protocols must be used for data transmission.
- All Personal Data should be protected at the application layer using industry-standard encryption methods

3. Privacy and Confidentiality

- The Provider must implement measures to ensure that Personal Data processed on behalf of Keyloop can only be processed in accordance with instructions
- The Provider must protect any Personal or Confidential Data in accordance with applicable Data Protection Laws and regulations
- The Provider must implement measures to ensure compliance with the principles of *Privacy by Design* and *Privacy by Default*
- The Provider shall ensure that Employees and Contractors with access to Personal Data are bound by confidentiality obligations to protect Keyloop's intellectual property and confidential information

Integrity

4. Transmission Control

- The Provider must implement measures to secure data traffic and communication connections to ensure Personal Data cannot be read, copied, altered or deleted by unauthorised persons during electronic transmission
- The Provider must continuously monitor IT systems, applications and relevant network zones to detect malicious and/or abnormal network activity using appropriate security technologies, including, but not limited to:
    - Endpoint Detection & Response (EDR) and Security Information & Event Management (SIEM) solutions;
    - Firewalls configured to ensure access to Personal Data and IT systems is strictly limited to approved business needs; and
    - Industry standard Anti-Malware solutions must be installed on all IT systems and applied at all data ingress/egress points processing and storing Personal Data.

5. Input Control

- The Provider must implement suitable measures to ensure that it is possible to check and establish whether and by whom Personal Data has been entered, modified or removed from data processing systems

Availability and Resilience

6. Availability and Recoverability

- The Provider must implement and maintain suitable measures to ensure Personal Data is protected against accidental destruction or loss
- The Provider must define, document and implement measures to ensure the capability of rapidly restoring the availability of and access to Personal Data in the event of a physical or technical incident
- The Provider must ensure high availability and redundancy for critical services
- The Provider must also ensure that third-party data centres or cloud infrastructure providers used in the delivery of Services meet the above minimum standards

7. Business Continuity and Disaster Recovery

- The Provider must establish, maintain, and document their business continuity plan(s), ensuring it includes procedures for operational resilience, risk mitigation, and continuity of services, and must regularly test the plan to verify its effectiveness
- The Provider must establish, maintain, and document their disaster recovery plans, ensuring they include procedures for data backup, recovery, and continuity of services, and to regularly test these plans to verify their effectiveness
- The Provider must also ensure that third-party data centres or cloud infrastructure providers used in the delivery of Services meet the above minimum standards

General Security Requirements

8. Compliance and Audit

- The Provider should hold and maintain ISO 27001 certification or an equivalent, widely recognised security certification
- The Provider must implement and maintain security controls in accordance with relevant industry standards such as ISO 27001, NIST, CIS Critical Security Controls or an equivalent recognised framework
- A risk management framework must be maintained to identify, assess, mitigate, and monitor potential threats to the security and privacy of data
- Keyloop reserves the right to conduct annual audits of the Provider, as well as ad hoc audits in response to security incidents or significant changes in risk posture
- The Provider must provide documented evidence of compliance with contractual security requirements upon request
- The Provider must designate an individual responsible for information security governance, risk management and compliance (e.g. CISO, Director of Security, or an equivalent senior role)
- Providers must ensure ongoing compliance with any applicable Data Protection Laws and regulations
- Providers must notify Keyloop of any changes to the geographic location of services or data processing locations before implementation to obtain approval and ensure compliance with applicable Data Protection Laws
- Providers must proactively inform Keyloop of any major changes to their environment (e.g. infrastructure, security controls or risk profile) that could impact Keyloop's business operations or security posture

9. Systems Security

- The Provider must ensure that all networking, infrastructure, middleware, applications, and cloud services comply with industry security standards, such as ISO 27001, NIST and CIS Critical Security Controls. This should include:
    - All IT systems processing & storing Personal Data must be built to a security standard approved by the Provider;
    - Only authorised software may be used on any IT systems processing and storing Personal Data;
    - Implementing vulnerability management on all IT systems processing and storing Personal Data;
    - A process to implement vendor security fixes;
    - Ensuring Keyloop data is separated from other client data in IT systems and storage facilities; and
    - Maintaining security logs for all security event types as specified by Keyloop.

10. Incident Response Management

- The Provider must promptly report any data or security incidents, breaches, or vulnerabilities that could affect Keyloop, including any critical control failures
- A formal incident management process shall be in place which ensures that these notification processes to Keyloop are triggered in the event of security incidents or Personal Data breaches

11. Third-Party and Subcontractor Management

- The Provider can only outsource any element of processing or storing Personal Data to a third party with the consent of Keyloop
- The Provider must ensure that third parties or subcontractors comply with contractual Information Security and Data Protection clauses, at a minimum matching the requirements in this document
- The Provider must conduct regular security and compliance assessments of third-party vendors
- The Provider shall retain the right to audit the third party or subcontractors' operation of security controls

Further Information

If you have any questions regarding the content of this document, please contact your Keyloop Account Manager.

Keyloop may update or modify these requirements at any time without prior notice provided that such changes do not result in a material change of the overall security expectations for our suppliers. These measures shall be reviewed annually or where significant business or regulatory changes occur and updated where appropriate.

Document Control

CREATION DATE	February 2025
LAST REVIEWED	February 2025
NEXT REVIEW	February 2026
VERSION NUMBER	1.0
DOCUMENT OWNER	Craig Duff, General Counsel

Version	Author	Date	Comments	Approval
0.1	Georg Chapman	03/02/2025	First Draft Created	N/A
1.0	Georg Chapman	05/02/2025	Final Draft for approval	Craig Duff

Appendix: Glossary of Terms

Term	Definition
Systems	Information and communications technology systems used in performing the Services including any software (including cloud software), middleware, hardware, applications, infrastructure, network, devices and peripheries which are used to process Keyloop data.