Technical and Organisational Measures

Author: Georg Chapman

Date: January 2025

Version Number: 1.0

Contents

Executive Summary

Keyloop are dedicated to interconnecting the digital landscape, and safeguarding sensitive information is not just a regulatory requirement. For us, it is a foundation for building trust with customers, partners, and stakeholders.

Our approach to security is rooted in fostering digital trust, ensuring that all stakeholders can confidently interact with our systems, services, and platforms. By leveraging industry best practices, regulatory compliance frameworks, and implementing advancements in security technologies, we proactively address the ever-changing cyber threat landscape and maintain a resilient security posture.

Keyloop prioritises transparency, accountability, and innovation in our security practices, we aim to exceed expectations and inspire confidence in our ability to deliver our operations securely. This document outlines our unwavering commitment to upholding the highest standards of digital trust and security.

Purpose & Scope

This document outlines the Technical and Organisational Measures (TOMs) implemented by Keyloop for secure and compliant processing of Personal Data. These measures aim to ensure an appropriate level of security, including the ongoing confidentiality, integrity, availability and resilience of data processing systems and services. It takes into account the rights of data subjects and the requirements of applicable data protection legislation.

The measures outlined in this document are applicable to all standard Keyloop service offerings and systems.

These Technical and Organisational Measures are listed in the Privacy Hub which provides further information regarding the way in which Keyloop processes Customer Personal Data. Unless otherwise defined in this document, terms used in this document shall have the meanings given to them in the Standard Terms and Conditions or Data Processing Addendum, each being available at https://www.keyloop.com/legal-documentation.

These measures do not apply where the Customer is responsible for security and privacy either at law or as outlined in the Standard Terms and Conditions or Data Processing Addendum. Customer is responsible for implementing and managing security and privacy measures for components that do not form part of Keyloop services offerings and systems.

Confidentiality

1. Physical Access Control

Keyloop implements suitable measures to prevent unauthorised persons from gaining access to our data processing facilities and equipment. This shall be accomplished by:

- Establishing secure areas, such as data centres and server rooms within Facilities to ensure physical separation of areas hosting Personal Data
- Protecting and restricting access paths through electronic access control systems
- Limiting physical access to data centres, server rooms, and other secure areas to authorised personnel based on job responsibilities
- Logging, monitoring, and tracking all access to data centres where Personal Data is hosted
- Monitoring premises with CCTV cameras, with recordings retained in compliance with legal and operational requirements
- Implementing a visitor management process, including supervision by authorised personnel for visitors in secure areas
- Installing alarm systems to detect unauthorised access to managed facilities and secure areas
- Carrying out maintenance and inspection of supporting equipment in secure areas using only authorised personnel or approved third parties where appropriate
- Equipping facilities with measures to prevent unauthorised physical access to data processing systems, such as locked server cabinets

Keyloop also ensures that third-party data centres or cloud infrastructure providers used in the delivery of Keyloop services meet the above minimum standards.

2. Logical Access Control

Keyloop implements an authorisation and authentication framework including, but not limited to, the following elements:

- Individual and identifiable user accounts with access rights granted following the Least Privilege Access Principle
- Access management processes to create, modify and delete accounts implemented
- Access rights to IT systems and applications are removed upon termination of employment or contract
- Access to IT systems and applications is protected by appropriate authentication mechanisms based on the characteristics and technical options of the system or application
- Privileged access rights to IT systems, applications, and networks are only granted to individuals who need it under the least privilege principle, with Privileged Access Management, Password Management, and Secrets Management tools being utilised
- Access rights to IT systems and applications are reviewed and updated on a regular basis
- Password policy implemented including requirements for password complexity, minimum length, password age, maximum number of erroneous login attempts and password history
- Wherever available, Multi-Factor Authentication is also implemented
- Policy to lock user terminal when leaving the workplace is implemented
- Automatic time-out of user terminal if left idle

3. Data Access Control

Keyloop implements measures to prevent unauthorised persons from accessing Personal Data that includes:

- Restricting access only to authenticated and authorised individuals
- Ensuring that access to Personal Data is restricted to the minimum level necessary for the task or role
- Logging of access to applications, including actions such as entering, modifying, and deleting data
- Remote access is only permitted via VPN or secure access protocols with appropriate authorisation and authentication

- Data minimisation is embedded as a Privacy by Design principle throughout the Software Development Lifecycle (SDLC)
- Confidential documentation is securely shredded at facilities in accordance with industry standards by an approved third-party supplier
- Keyloop ensures that equipment and data storage media are erased and disposed in accordance with industry standards

4. Separation Control

Keyloop implements suitable measures to ensure that Personal Data collected for different purposes can be processed separately, which may include:

- Separation of production, testing, and development environments
- Implementation of access controls to restrict access to data based on an authorisation concept
- For shared systems, ensuring data is isolated between customers or tenants through logical or technical mechanisms
- Use of industry standard encryption for data at rest
- Implementation of network segmentation to isolate sensitive systems and data
- Privacy by Design principles are utilised during testing and development to ensure real data is not exposed in non-production environments

5. Pseudonymisation

Keyloop takes suitable measures to ensure that only authorised persons can access and read Personal Data, and that to the extent necessary, data is either anonymised or pseudonymised to minimise the risk of identification:

- Privacy by Design principles are embedded into the Software Development Lifecycle (SDLC) including Data Anonymisation and Data Minimisation
- Personal Data is pseudonymised where possible to reduce the exposure of sensitive information, ensuring that data cannot be attributed to a specific individual without additional information

- Pseudonymised data is stored separately from the key information required for re-identification, ensuring that access to the original data requires authorisation
- Specific internal regulations govern the use of cryptography for data both at rest and in transit

Integrity

6. Transmission Control

Keyloop implements 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:

- Continuous monitoring of IT systems, applications and relevant network zones to detect malicious and/or abnormal network activity which may include:
    - Endpoint Detection and Response (EDR) agents;
    - Firewalls (e.g., stateful firewalls and application firewalls);
    - Web Filtering; and
    - Security Information and Event Management (SIEM) systems.
- Documenting and updating network topologies and associated security requirements on a regular basis
- Administration of IT systems and applications by using industry standard encrypted connections
- Protecting the integrity of content and Personal Data during transmission by using industry standard network protocols
- Use of secure channels including Virtual Private Networks (VPNs) and secure data transfer protocols

7. Input Control

Keyloop implements 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:

- Comprehensive logging of data entries, modifications, and deletions
- Only authorised personnel can input or modify Personal Data, with user authentication mechanisms ensuring secure access
- Assignment of rights to enter, change and delete data based on an authorisation concept
- Restrictions on input capabilities to ensure data is processed only by users with the appropriate permissions
- Implementation of input validation mechanisms to prevent errors or injection of malicious data during data entry

Availability and Resilience

8. Availability Control

Keyloop implements and maintains suitable measures to ensure Personal Data is protected against accidental destruction or loss. This shall be accomplished by:

- Data centres in which Personal Data is stored or processed are protected against natural disasters, physical attacks or accidents through the following elements:
    - Heating, ventilation and air conditioning (HVAC) systems
    - Protection of power and telecommunications cabling to guard against interference, interception or damage
    - Implementation of appropriate alerting measures such as fire suppression, leak detection and smoke detectors
    - Use of uninterruptible power supplies (UPS) and, where necessary, emergency generators
    - Maintenance schedules to ensure continued availability and integrity

- Supporting equipment in IT areas and data centres such as cables, electricity, telecommunication facilities, water supply, or air conditioning systems are safeguarded against disruptions and unauthorised manipulation
- Keyloop maintains appropriate business continuity plans to uphold availability commitments, considering the size, scale and nature of the Keyloop organisation and the products we offer
- Implementing industry standard anti-malware solutions to protect Keyloop systems against malicious software

Keyloop also ensures that third-party data centres or cloud infrastructure providers used in the delivery of Keyloop services meet the above minimum standards.

9. Recoverability Control

Keyloop defines, documents and implements 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. This includes, but is not limited to, the following elements:

- Keyloop defines, documents and implements a backup concept for IT systems, including, but not limited to the following elements:
    - Backup storage media is protected against unauthorised access and environmental threats (e.g., heat, humidity, fire, flooding);
    - Defined backup intervals;
    - Defined retention periods; and
    - The restoration of data from backups is periodically tested.
- Redundant infrastructure and failover mechanisms to ensure high availability and continuous service
- Integration of recoverability measures with incident response processes to coordinate effective recovery efforts
- Backup data is encrypted and stored securely to prevent unauthorised access or loss
- Coordination of recoverability measures with Business Continuity Plans (BCP) to support seamless operations

Keyloop also ensures that third-party data centres or cloud infrastructure providers used in the delivery of Keyloop services meet the above minimum standards.

Procedures for regular review, assessment and evaluation

10. Governance Framework

Keyloop establishes a robust governance framework to oversee information security and data protection responsibilities, ensuring compliance with relevant laws and standards. This shall be accomplished by:

- Maintaining an Information Security Management System (ISMS) certified against the ISO 27001 framework, the ISMS is regularly reviewed and follows a continual improvement cycle to ensure ongoing alignment with best practices and evolving security requirements
- The ISMS is assessed by an independent third party at planned intervals or following significant business changes
- Maintaining an up-to-date set of policies and standards subject to annual review for both information security and data protection, such as a Global Data Protection Policy, Information Security Policy, and Acceptable Use Policy, to guide organisational practices
- Maintaining specific policies and procedures subject to annual review to ensure a uniform, consistent and cohesive approach to the collection, use, transfer, storage and destruction of Personal Data
- Operating dedicated internal cross-functional committees to regularly review matters related to information security and data protection
- Mandating that employees are responsible for adhering to organisational policies, standards, and procedures through Keyloop's Employee Code of Conduct
- Conducting assessments to verify compliance with internal policies, standards and procedures

11. Data Protection Management

Keyloop implements the following measures to ensure that our organisation meets the requirements of relevant data protection laws in accordance with our Data Protection Policy:

- Maintaining centralised documentation of all data protection policies and processes, ensuring they are accessible to all employees for consistent adherence
- Internal appointment of a Data Protection Officer (DPO)
- Delivery of annual data protection and privacy awareness training to all employees, ensuring they understand their responsibilities and best practices for handling Personal Data
- Regular inventory and monitoring of applicable data protection laws and regulations to ensure compliance across jurisdictions
- Processes to fulfil information obligations applicable data protection legislation, ensuring transparency in the collection and use of Personal Data
- Maintaining a Record of Processing Activities (RoPA)
- A formalised process for handling requests from data subjects, including access requests, correction, deletion, and data portability requests
- Review of the effectiveness of the TOMs is carried out at least annually with updates made as necessary
- Data Privacy Impact Assessments (DPIAs) are carried out for processing activities to identify and mitigate potential privacy risks
- Incorporating data protection aspects into the corporate risk management framework to identify and mitigate risks associated with Personal Data processing
- Ensuring that all employees are bound by confidentiality agreements to safeguard Personal Data
- All third-party suppliers, contractors and service providers with access to and/or processing Personal Data are required to sign Non-Disclosure Agreements (NDAs) or Data Processing Agreements (DPAs) as appropriate

12. Privacy by Design and by Default

Keyloop implements measures to ensure compliance with the principles of *Privacy by Design* and *Privacy by Default*. This shall be accomplished by:

- Embedding Privacy by Design and Privacy by Default principles into the Software Development Lifecycle (SDLC) program during the design and implementation of Keyloop software

- Maintaining a Data Privacy Impact Assessment (DPIA) process where Keyloop is determining the purposes for processing Personal Data
- Ensuring all new products, changes to current products and internal Keyloop tools and systems are subject to the DPIA process to assess and mitigate privacy risks
- Maintaining centralised documentation of all data protection policies and processes, ensuring they are accessible to all employees for consistent adherence
- Ensuring, by default, Personal Data is only processed to the extent necessary to provide the services and as outlined in the Agreement, in accordance with Data Protection Legislation

13. Risk Management

Keyloop implements a comprehensive risk management framework to identify, assess and mitigate potential threats to the security and privacy of Personal Data including, but not limited to, the following elements:

- Keyloop systematically identifies and documents potential risks to data security and privacy, considering both internal and external factors
- Conducting regular risk assessments using established methodologies to evaluate the likelihood and impact of identified risks on data and systems
- Implementing appropriate risk treatment measures, such as mitigating, transferring, accepting, or avoiding risks
- Developing and maintaining comprehensive risk mitigation plans, including clear action steps and timelines for addressing high-priority risks
- Continuously monitoring risks and evaluating the effectiveness of risk mitigation efforts, ensuring timely responses to emerging threats

14. Supplier Management

Keyloop implements measures to ensure that Personal Data processed on behalf of the client can only be processed in accordance with instructions. This is accomplished by:

- Ensuring third-party service providers comply with governance and security requirements through formal agreements and due diligence processes
- Conducting thorough due diligence and third-party risk assessments during the supplier onboarding process
- Requiring all suppliers processing Personal Data to sign Data Processing Agreements (DPAs) outlining their data protection obligations
- Maintaining a set of information security requirements which are incorporated into Supplier Terms and Conditions, ensuring suppliers adhere to Keyloop's standards
- Restricting access to Personal Data strictly to what is necessary for the provision of contracted services
- Ensuring suppliers notify Keyloop immediately in the event of a data breach or significant security incident
- Monitoring supplier compliance through periodic performance reviews, evaluations and due diligence checks
- Requiring secure deletion or return of Personal Data upon termination of the supplier relationship

Organisation

15. Human Resources Security

Keyloop implements the following measures in the area of human resources security:

- Employees and contractors with access to Personal Data are bound by confidentiality obligations
- Screening process ensures that employees are appropriately vetted to verify their suitability and trustworthiness for roles involving access to sensitive data and systems
- Annual Training and Awareness Programmes are implemented and maintained to educate employees on information security and data privacy principles
- Disciplinary Policy and process establishes clear consequences for violations of data protection and security policies

- Keyloop implements an offboarding process for employees during which they are reminded of their ongoing confidentiality obligations

16. Operations Security

Keyloop implements measures to manage, monitor and respond to security threats. This shall be accomplished by:

- Implementing industry standard anti-malware solutions to protect systems and applications against malicious software
- Keyloop continuously monitors its systems and networks using automated security tools such as Security Information and Event Management (SIEM) systems to detect and respond to potential threats
- Maintaining detailed security logs of all relevant activities
- Continuously analyses the respective systems and event logs for anomalies, irregularities, indicators of compromise and other suspicious activities
- Scanning systems and networks for security vulnerabilities on a regular basis
- Maintaining a process to update and implement vendor security fixes and updates on the respective IT systems and applications
- Maintaining a comprehensive Incident Response process that defines roles, responsibilities, and procedures for detecting, reporting, managing and mitigating security incidents or data breaches
- Establishing a formal change management process to control and perform changes to systems and applications

17. Incident Response Management

Keyloop maintains and implements an incident management process, including, but not limited to, the following measures which are intended to ensure that notification processes are triggered in the event of security incidents or data protection breaches:

- A formalised procedure for handling security incidents and data breaches
- Recording and documentation of security incidents and data breaches

- Involvement of the Data Protection Officer (DPO) during security incidents and data breaches as necessary
- Customer notification processes
- Resolution and recovery actions to minimise impact and restore normal operations
- Preventive measures to avoid recurrence of incidents

18. System Acquisition, Development and Maintenance

Keyloop implements and maintains software development, acquisition and maintenance processes including, but not limited to, the following elements:

- Keyloop identifies and documents information security and privacy requirements prior to the development and acquisition of new systems and applications as well as before making improvements to existing systems and applications
- Integrating security and privacy throughout the Software Development Lifecycle (SDLC), applying Security by Design, Privacy by Design and Privacy by Default principles
- Establishing a formal change management process to control and perform changes to developed applications
- Keyloop plans and incorporates security tests into the SDLC of systems and applications
- Keyloop implements a comprehensive security patching process that includes:
    - Monitoring of components for potential vulnerabilities (CVEs) through regular vulnerability scanning and penetration testing;
    - Assigning priority ratings to fixes based on severity and risk;
    - Prompt and timely implementation of the fix; and
    - Ensuring patches are downloaded exclusively from trusted and reputable sources.

Further Information

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

Keyloop may implement changes to these measures at any time without notice provided that such changes do not result in a material degradation of the overall level of security for Customer data. These measures shall be reviewed annually or where significant business or regulatory changes occur and updated where appropriate.

Document Control

CREATION DATE	January 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	16/01/2025	First Draft Created	N/A
1.0	Georg Chapman	22/01/2025	Final Draft for approval	Craig Duff

Appendix: Glossary of Terms

Term	Definition
Secure Area	A secure area is a physically defined space within Keyloop facilities where access is strictly limited to authorised personnel whose job roles necessitate entry.
Systems	Information and communications technology systems used by Keyloop in performing the Services including any software (including cloud software), middleware, hardware, applications, infrastructure, network, devices and peripheries which are used to process Customer Data.