Document Information

Document Title	Data Security Measures
Owner	CEO
Status	APPROVED
Classification	Confidential – External
Version	2.0.EU
Date	19 September 2023
Next Review	10 January 2024

Version	Change	Initials	Date
1.0	Created for new organization	SXF	25 Aug 2023
1.1	Initial edits after peer review	CS	8 Sep 2023
2.0	Confidential External Approved (CEA)	JY	19 Sep 2023

Approvals

Version	Role	Initials	Date
1.0	Classified Draft only		
2.0	CEO	JY	19 Sep 2023

INTRODUCTION

This document outlines the specific data security protection measures implemented by ForeNova in accordance with the German security and compliance standard, TOMs (Technische und Organisatorische Maßnahmen). The measures are described from both organizational and technical perspectives to ensure comprehensive data security.

2. ORGANIZATIONAL SECURITY MEASURES

2.1 Data security Organization

ForeNova attaches great importance to the data security that:
2.1.1 establish and maintain a data governance framework that defines roles, responsibilities, and accountability for data security;
2.1.2 appoint a data protection officer responsible for supervising and managing data security affairs;
2.1.3 establish a data security team responsible for daily data security management and incident response.

2.2 Risk Management

ForeNova has established a risk management mechanism and fully utilizes its own risk management services to control data security risks. For instance:
2.2.1 conduct regular risk assessments to identify potential vulnerabilities and threats to data security, and develop and implement risk mitigation strategies based on the identified risks;
2.2.2 establish incident response and management procedures to handle data breaches effectively;
2.2.3 conduct attack and defense drills to proactively identify potential data security risks and take appropriate measures to manage these risks.

2.3 Personnel Security

2.3.1 All ForeNova employees are subject to a background check to ensure that their background meets the requirements of laws and regulations before joining ForeNova;
2.3.2 Non-disclosure Agreement (NDA) will be signed to ensure that all the new employees are aware of their data confidentiality obligation;
2.3.3 ForeNova conducts regular data privacy and security training for employees to enhance awareness and compliance with data protection policies;
2.3.4 The system permissions for departing employees will be promptly revoked and they will be requested to return all company assets.

2.4 Physical Security

ForeNova has chosen a globally trusted data center service provider that has achieved several security certifications and implemented multiple security measures to ensure the physical security of its data center.
Compliance The data center complies with physical security controls in alignment with standards and regulations such as ISO27001, SOC 2 Type II, EU Code of Conduct and many more quality, ICT, and cybersecurity standards.

Access Control The data center implementing 24/7 on-site security personnel, video surveillance, biometric authentication systems and secure perimeter fencing to ensure only authorized personnel can access the data center facilities;
Reliability and Resilience The data center ensures uninterrupted service and data protection through redundant power systems, devices, backup generators, and multiple network connections.

2.5 Data Classification

ForeNova implements data classification and labeling policies to ensure appropriate handling and protection of sensitive data.

2.6 Compliance Management

ForeNova has formed a privacy compliance group comprised of legal and information security engineers and business department representatives. This group is responsible for promptly identifying and reviewing relevant data privacy protection laws and regulations.

3. TECHNICAL SECURITY MEASURES

3.1 Access Control

ForeNova implements a robust access control mechanism to ensure that only authorized personnel can access and process data. This access control mechanism includes:
3.1.1 implement an access control process that assigns user privileges based on the principle of least privilege and need to know;
3.1.2 enforce strong password policies and encourage multi-factor authentication for all user accounts;
3.1.3 maintains detailed logs and audit trails of user activities within the system. This allows for monitoring and identification of any unauthorized access attempts or suspicious behavior;
3.1.4 regularly review and update user access rights and revoke access promptly when necessary.

3.2 Network Security

ForeNova adopts advanced technologies and solutions to prevent the risk of data breaches caused by network security. These include at minimum:
3.2.1 deploy advanced next generation firewalls, intrusion detection and prevention systems to detect and block unauthorized access and cyber-attacks in real time;
3.2.2 adopt network segmentation to protect against unauthorized access and external threats;
3.2.3 deploy a zero-trust solution that opens a minimum of services and ports to the internet and minimizes network exposures;
3.2.4 regularly update and patch security devices, applications, and components to address known vulnerabilities and weaknesses.

3.3 Security Operations

3.3.1 ForeNova use our own security operation solution named “Component + Platform + Service” to manage detection and response;

3.3.2 ForeNova deployed our own security components such as NovaCommand and NovaGuard to integrate with our security operations platform, NovaMDR, enabling timely detection and identification of possible threats and taking appropriate response measures;
3.3.3 ForeNova own professional security operation expert team provide 24/7 security operation monitoring and incident response.

3.4 Data Lifecycle Management

ForeNova takes security and compliance measures to manage data throughout its lifecycle, including:

3.4.1 Data Acquisition

Data acquisition complies with laws and regulations by only collecting the necessary personal data for the business and obtaining explicit consent from customer;

3.4.2 Data Transmission

The secure transmission protocol TCP at network layer, TLS at session layer and HTTPS at application layer is used to ensure the security of data transmission；

3.4.3 Data Utilization

The use of data is restricted, only authorized personnel for business needs have access to sensitive data, and the presentation of sensitive data will be desensitized；
All access and operation logs are recorded and audited；
Utilizing UEM sandbox technology to ensure that access to production environment data takes place within the sandbox, preventing data from being stored on personal endpoint devices and mitigating the risk of data leakage.

3.4.4 Data Storage

Strong encryption algorithm (AES-256) is used to protect personal data in storage, and copies of all important data are kept for emergencies；
Implement key management practices to safeguard encryption keys.

3.4.5 Data Extraction

The extraction of all production data is controlled through an approval process to ensure that the extraction of data meets business needs；
All the approval records will be kept ensuring that the extracted data is auditable and traceable.

3.4.6 Data Retention and Disposal

Establish and enforce data retention policies that align with legal and regulatory requirements;
Before the expiration of the service, ForeNova will notify the customer and negotiate with the customer about the data processing method after the expiration of the service;
Implement secure data disposal procedures based on the customer’s requirement, including the use of data destruction methods like encryption or physical destruction.

3.5 Vulnerability Management

3.5.1 ForeNova conduct periodic vulnerability scan and assess the security posture of systems, applications, and infrastructure;
3.5.2 ForeNova will promptly address identified vulnerabilities through patching or other mitigation measures;

3.5.3 ForeNova implement penetration testing to identify potential security weaknesses and ensure continuous improvement of security measures;
3.5.4 ForeNova follows a vulnerability management process and uses a vulnerability management platform to track and manage the discovery, disposition, validation, and closure of vulnerabilities throughout the process.

3.6 Incident Response Management
3.6.1 ForeNova established an incident response process that includes defined response organization, roles, personnel, and responsibilities to deal with incidents;
3.6.2 Incidents are defined into different levels and different ways of handling and reporting. ForeNova will regularly organize relevant personnel to discuss and learn about the incident response process, so that everyone is familiar with their responsibilities；
3.6.3 Prepare contingency planning and conduct regular incident response drills and simulations to test the effectiveness of the plan.
3.6.4 Conduct quarterly practical attack and defense drills to test the coordination of emergency response and continuously improve and optimize the emergency response process.

3.7 Backup and Recovery
ForeNova establish data backup and disaster recovery mechanisms that:
3.7.1 implement regular and automated data backup to ensure data availability and recovery in case of data loss/damage or system failures;
3.7.2 periodically test the backup and recovery processes to verify their effectiveness.

4. DUE DILIGENCE ON SUB-PROCESSORS

4.1 ForeNova maintain a security process to conduct appropriate due diligence prior to engaging sub-processors.
4.2 ForeNova will sign a data processing agreement with sub-processors that clearly defines the security responsibilities and obligations of the data processor, ensuring that data processing complies with legal requirements;
4.3 ForeNova conducts data security audits on sub-processors to ensure they adhere to ForeNova’s key information security policies and standards and no less protective than these measures.

In conclusion, ForeNova has implemented a comprehensive set of data security protection measures in accordance with the TOMs standard. The combination of technical and organizational measures ensures the safeguarding of sensitive data and compliance with applicable regulations and industry best practices. Regular evaluation, monitoring, and improvement of these measures are undertaken to maintain a high level of data security.