Americas / APAC HQ
542A Amherst Street
Nashua NH 03063
USA

+1 630 974 3000
www.episerver.com

EMEA HQ
Regeringsgatan 67
Box 7007
103 86 Stockholm, Sweden

+46 8 55 58 27 00
www.episerver.com
556208-3435

Episerver Technical and Organizational Measures

1.0 OVERVIEW

This document describes technical and organizational security measures and controls implemented by Episerver to protect the data customers entrust to us as part of the Episerver services. Episerver may change these measures from time to time to adapt to the evolving security landscape and, where required, will notify customers of these changes.

2.0 DEFINITIONS

Within this document, the following definitions apply:

- Customer - the party that consumes Services per agreement with Episerver.
- Episerver Software Services - the cloud-based software services provided by Episerver to Customer as defined in an order as part of Customer's subscription, each subject to the applicable EUSA.
- Customer Data - any information provided or submitted by the Customer that is processed by the Episerver services.
- Personal Data - any information relating to an identified or identifiable natural person.
- Personnel - Episerver employees and authorized individual contractors/vendors.
- Strong Encryption - the use of industry-standard encryption measures.

3.0 EPISERVER TECHNICAL AND ORGANIZATIONAL MEASURES

Episerver is committed to the protection of Personal Data and has implemented controls and measures to ensure compliance to laws and regulations, including the EU General Data Protection Regulation 2016/679 (GDPR).

4.0 ORGANIZATION OF INFORMATION SECURITY MANAGEMENT

The information security function reports directly to the Episerver CISO and employs full-time dedicated trained/certified security Personnel responsible for information security and data protection. An Information Security Policy that addresses the objectives for information security and data protection is established, approved by top management and disseminated to all Personnel. Information security and data protection training is required for all new employees and at least annually for all employees and contractors.

5.0 INFORMATION SECURITY MANAGEMENT SYSTEM

Episerver's information security management system (ISMS) is based on the ISO 27001:2013 standard. Information Security Objectives are aligned with the priorities of the business, and all identified risks are accounted for with recognition and control from top management. Using a Risk management framework to assess, treat, and manage all risks including Personal Data, Episerver has implemented appropriate controls from ISO 27002 to address the following critical areas:

- Information Security Policies
- Organization of Information Security
- Human Resources Security
- Asset Management
- Access Control
- Cryptography
- Physical and Environmental Security
- Operational Security
- Communication Security
- Systems Acquisition, Development, and Maintenance
- Supplier Relationships
- Information Security Incident Management
- Compliance

6.0 RISK MANAGEMENT

Episerver's risk management methodology represents a framework to identify, assess, treat, and monitor risks. Objectives for risk management shall be based on Episerver's ISMS scope, the Information Security Policy, information security objectives, and specific requirements. Objectives of the Risk Management Framework:

- Identify risks associated with protection of Personal Data
- Assess all risks using a consistent and proven methodology
- Treat and control risks to acceptable levels, based on Episerver's risk appetite and tolerance

- Monitor and review risks to ensure that treatment and controls are effective
- Improve the risk management function by resolving issues and discovering opportunities to increase the performance of the framework

7.0 PROTECTION OF EPISERVER PREMISE AND DATA PROCESSING FACILITIES

Episerver's data processing occurs at Episerver offices, secure data centers, and on secure, cloud service providers. Protection of the physical premises to all critical areas has been established and controlled. Protective measures have been implemented with security controls to prevent unauthorized persons from gaining physical access to data processing areas that may contain Personal Data. Measures include but are not limited to:

- Preventing access to unauthorized persons
- Formal visitor policies and procedures with identity management
- Access authorization for employees and approved vendors
- Use of authentication for identity and access management using appropriate measures
- Surveillance and monitoring using video cameras, logging, and key logging
- Security and safety alarm systems
- Protection against natural disasters and threats
- Facilities auditing to ensure compliance to applicable policies and standards

8.0 PROTECTION OF EPISERVER SYSTEMS

All Episerver assets, services, and systems that are used for data processing are protected against unauthorized persons from use, access, or harm. Measures include but are not limited to:

- Access based on principle of least privilege and implemented based on job roles
- All users require a unique identifier and have separate accounts linked to named persons
- Administrative and privileged accounts are designated and managed separately
- Logging of access for activities and events that may affect or alter data or data processing systems
- Use of modern firewalls and firewall services that are updated, maintained, tested, and monitored regularly
- Use of anti-virus and anti-malware applications and services that are updated regularly to properly detect and manage against vulnerable threats
- Established requirements and use for strong passwords, password expiry, multi-factor authentication, and digital certificates
- Ongoing and continuous monitoring and scanning for vulnerabilities and threats
- Systems and software updated with latest tested patches and updates to applicable critical systems
- Use of intrusion detection and intrusion prevention systems and services
- Regular third-party security assessments and penetration tests performed against networks

9.0 DATA PROTECTION

Personal Data and information that is processed or controlled by Episerver are protected against un-authorized access via security controls and rules. Further controls include the use of data encryption where feasible and where encryption serves an effective security measure. Only authorized persons with approved access are permitted to such data and limited to the scope and nature of the job duty and purpose of providing Episerver services. In addition, all third-parties as sub-processors for Episerver must have equivalent measures in place prior to access and use. Measures include but are not limited to:

- Episerver employees and contractors required to sign applicable confidentiality agreements
- Policies and procedures for employee onboarding, transfers, and leavers that govern access to Personal Data and data processing facilities, and all systems
- Role-based access using unique login account credentials based on job duties and the principle of least privilege
- Use of encryption with strong algorithms for all data at rest, data in motion, and data in transit where proven to be feasible and effective
- Logging of access to critical systems and services and protection of log data from compromise
- Information security and data protection awareness training for use and requirements for handling Personal Data
- Monitoring and regular reviews of logging information for account activities, including administrative and privileged accounts

Americas / APAC HQ
542A Amherst Street
Nashua NH 03063
USA

+1 630 974 3000
www.episerver.com

EMEA HQ
Regeringsgatan 67
Box 7007
103 86 Stockholm, Sweden

+46 8 55 58 27 00
www.episerver.com
556208-3435

10.0 DATA AVAILABILITY

Episerver protects Personal Data from damage, loss, or destruction from potential disasters and unforeseen threats. Measures include but are not limited to:

- Conducting regular backups as well as regular monitoring of the backup processes
- Ensuring there are specific requirements in all critical areas regarding performance, uptime, integrity of services, disaster recovery, data redundancy, and monitoring
- Comprehensive Business Continuity Management planning with aligning Disaster Recovery strategies
- Continuous monitoring of networks, storage solutions, systems, and services critical for processing of Personal Data
- On-call response to monitoring events relating to critical data handling
- Appropriate security controls for all systems and services for all states and events

11.0 DATA SEPERATION

Episerver ensures that each Customer's Data is processed separately. Measures include but are not limited to:

- Use of logical separation within multi-tenant architecture to enforce data segregation between customers
- Uniquely identifying Customer Data to ensure separation between Customer data set
- Limiting customer data using strong encryption keys

12.0 SECURITY INCIDENT MANAGEMENT

In the event of any security breach of Customer Data, Episerver ensures the effects of the breach are minimized and that the Customer is promptly informed. A formal Security Incident Management process is used along with protective supporting measures. Measures include but are not limited to:

- Separation of Incident Management and Security Incident Management processes to ensure exclusive handling and compliance regarding incidents involving Breach of Personal Data
- Use of an up-to-date incident response plan that includes responsibilities, how information security events are assessed, classified, managed, and responded to
- Training for staff of Security Incident Management processes and handling of security incidents involving Personal Data
- Testing of Security Incident response policies and procedures performing "table-top" exercises and utilizing lessons-learned from tests
- Ensuring notification to Customers without undue delay after becoming aware of the security breach
- Annual auditing and review of Security Incident Management policies and procedures, including Management Reviews for incident reporting

13.0 VENDOR AND SUPPLIER DATA PROCESSING

All third-parties used by Episerver for data processing have implemented measures to ensure data protection equal to that of the measures taken by Episerver. Additionally, the following measures have been added and include but are not limited to:

- A Data Processing Agreement (DPA) in support of the regulations upheld and required from Episerver, including those that permit transfer of data of European Union residents to the data processor
- Review of vendor and supplier audits or assessments as a data processor
- Critical reviews of data processor security and availability controls, service level agreements (SLA), and accountability for data processing
- Requiring wording within agreements to be unambiguous and clear as to the use, separation, ownership, and control of Personal Data

14.0 AUDITING

Episerver holds regular internal and external audits at planned intervals. Episerver requires all internal and external auditing activities to be performed by competent, certified auditors. Processes and data are audited for compliance to Episerver policies, standards, and regulations. An auditing program is in place at Episerver, which regularly audits information security and data protection systems.