Americas / APAC HQ
542A Amherst Street
Nashua, NH 03063
USA
+1 603 594 0249
www.episerver.com

EMEA HQ
Torsgatan 11
Box 7007
103 86 Stockholm, Sweden
+46 8 55 58 27 00
www.episerver.com
556208-3435

Appendix – Episerver Security Appendix

This Appendix is made and entered into between Customer and **Episerver ("Episerver")** as part of the Master Services Agreement.

The Parties have now therefore made and entered into this Appendix to the Master Services Agreement to be considered as an integral part of the Agreement. Terms defined in the Agreement, including the Episerver End User Service Agreement ("EUSA"), which are capitalized terms, shall apply within this Appendix. Terms defined in this Appendix shall only apply to Episerver Customer-Centric Digital Experience Platform Service(s).

1. Customer Data

As used in this Appendix "**Customer Data**" shall have the same meaning as set forth in Section 3.3 of the EUSA.

2. Security Measures and Audit Rights

Episerver undertakes in respect of all Customer Data that at all times it shall implement appropriate technical and organizational measures to protect any Customer Data processed by it against unauthorized and unlawful processing and against accidental loss, destruction, disclosure, damage, or alteration. This shall include, as a minimum, the following:

a. Episerver shall maintain, enforce, and comply with a written data security program (the "**Program**") with respect to its processing of Customer Data that is at least equal to applicable commercially reasonable industry practices and standards, including but not limited to ISO 27001. The Program's policies and procedures shall contain administrative, technical, and physical safeguards, including without limitation: (a) guidelines on the proper disposal of Customer Data after it is no longer needed to carry out the purposes of the Agreement; (b) access controls on electronic systems used to maintain, access, or transmit Customer Data; (c) access restrictions at physical locations containing Customer Data; (d) encryption of electronic Customer Data; (e) testing and monitoring of electronic systems, including but not limited to penetration and vulnerability testing; and (f) procedures to detect actual and attempted attacks on or intrusions into the systems containing or accessing Customer Data. Episerver shall review the Program and all other Customer Data security precautions regularly, but no less than annually, and update and maintain them to comply with applicable laws, regulations, technology changes, and generally accepted industry standard practices.

b. Episerver shall take all reasonable measures to: secure and defend all locations, equipment, systems and other materials and facilities employed in connection with the Services against "hackers" and others who may seek, without authorization, to disrupt, damage, modify, access or otherwise use Episerver's systems or the information found therein.

c. Episerver shall only give its employees access to Customer Data and systems containing Customer Data on a need to know basis and according to the principle of Least Privilege (as defined by US-CERT), provided such individual is subject to a reasonable written nondisclosure agreement with Episerver protecting such data.

d. Episerver will keep accurate records and accounts pertaining to the performance of the Software Services. Upon no less than ninety (90) days' prior written notice, and no more than once per calendar year (unless required by government authorities), Customer may audit Episerver's records relating to its performance under this Agreement, provided Customer warrants that the audit(s) (i) if performed onsite, will only occur at Episerver facilities; (ii) are at the sole cost of Customer, including costs incurred by Episerver to participate in the audit; and (iii) will not interfere with other customers, partners or agents ability to provide services, or support otherwise provided for; and (iv) Customer shall not violate (or cause Episerver to violate) any third-party non-disclosure agreements in place between such third-party and Episerver.. Customer may, but is not obligated to, perform security audits, which shall, at Customer's option, cost and request, include penetration, vulnerability, and security tests, of its own environment. Certification of independent third party security audits including vulnerability and penetration tests of any Episerver systems and their housing facilities and operating environments which include Customer Data may be provided to Customer upon request following approval by Episerver's DPO or other designated person. If any audit or test referenced above or in Episerver's Program uncovers deficiencies or identifies suggested changes in Episerver's performance of the Services, Episerver shall exercise reasonable efforts promptly to address such identified deficiencies and suggested changes.

e. Episerver shall conduct or have conducted contemporaneous backups of Customer Data and perform or cause to be performed periodic backups of Customer Data and store such backup Customer Data in a commercially reasonable location and manner. On written notice from Customer, Episerver shall provide Customer with a copy of the backed up Customer Data inline with its backup policy and Service Level Agreement agreed to with Customer.

f. Episerver shall comply with its Service Level Agreement and Master Services Agreement terms in respect of remedies entitled to Customer in the event of Episerver's failure to comply with its obligations in this Section 2.

3. Security Breaches

Episerver shall notify Customer within 48 (forty-eight) hours of becoming aware of any confirmed actual accidental, unauthorized, or unlawful destruction, loss, alteration, or disclosure of, or access to Customer Data ("**Security Breach**"). Episerver shall implement, maintain, and follow a program for managing Security Breaches. Episerver shall also provide Customer with a detailed description of the Security Breach, the type of data that was the subject of the Security Breach and (to the extent known to Episerver) the identity of each affected person(s), as soon as such information can be collected or otherwise becomes available, as well as all other information and co-operation which Customer or law enforcement may reasonably request relating to the Security Breach. Episerver agrees to take action immediately, at its own expense (to the extent Episerver was the sole cause of the breach), to investigate the Security Breach and to identify, prevent, and mitigate the effects of any such Security Breach and to carry out any recovery or other action necessary to remedy the Security Breach.

4. Public Communications

Episerver may not issue or make available to any third party any press release or other communication concerning a Security Breach solely concerning Customer without Customer's prior approval unless required by applicable law or regulatory authorities. Episerver will not display or use Customer's corporate identity graphics or Customer's name unless specific written approval has been obtained from the Public Relations department of Customer. This prohibition includes, without limitation, the use of Customer's name or logo in customer lists, media releases, or public announcements.

5. Personally Identifiable Information

To the extent that Episerver processes personally identifiable information about individuals located in the European Economic Area ("**EEA**") and/or Switzerland, which Episerver stores or otherwise obtains access to outside of the EEA and/or Switzerland, in a country that is not recognized as providing an adequate level of data protection, the parties agree that this Appendix incorporates by reference the European Commission Standard Contractual Clauses for the Transfer of Personal Data to Processors Established in Third Countries (2004/915/EC) ("**EU Model Clauses**") (https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32010D0087) where Episerver shall be the "data importer," and Customer shall be the "data exporter," and the description of the transfers in Appendix 1 and technical and organizational security measures in Appendix 2 to the EU Model Clauses shall be as described in the Agreement and this Appendix. Episerver shall comply with any other applicable laws or regulations governing the processing of personally identifiable information.

6. Entire Agreement

This Appendix and the Agreement together constitute the entire agreement between the parties with respect to the subject matter of this Appendix and supersede and extinguish any prior drafts, agreements, undertakings, understandings, promises or conditions, whether oral or written, express or implied between the parties relating to such subject matter.

Order of Precedence - In the event of a conflict between this Appendix and the Agreement the terms of the Agreement shall control.

This Appendix is entered into and becomes a binding part of the Agreement as of the date last signed below.

Episerver	**Customer:**
Signature:	Signature:
Print name:	Print name:
Title:	Title:
Date and place:	Date and place: