

Episerver Processor Binding Corporate Rules Policy

1. Introduction and scope

- 1.1 The Policy. This Episerver Processor Binding Corporate Rules Policy (the “Episerver BCR”) establishes Episerver’s approach to compliance with Data Protection Laws and Regulations as it relates to transfers of personal data to third countries to and between members of the Episerver Group, and to third-party Sub-processors when acting as Processors and/or Sub-processors on behalf of and under the instructions of Customers. The scope of the Episerver BCR and Episerver Data Processing Agreement further includes the details of the data transfers, including the categories of Personal Data, the type of processing and its purposes, the types of Data Subjects affected and the identification of the recipients in the third country or countries.
- 1.2 Updates to the Episerver BCR. The Episerver BCR may be modified (for instance to take into account modifications of the regulatory environment or the company structure) but nonetheless imposes a duty to report changes without undue delay to all **Episerver** Group Members, to the Supervisory Authorities and to Customers.
- 1.3 Processing Changes. Where a change affects the processing conditions, notice and information will be given to Customer in such a timely fashion so Customer has the possibility to object to the change or to terminate the contract before the modification is made (for instance, on any intended changes concerning the addition or replacement of subcontractors, before the Personal Data is communicated to the new Sub-processor).
- 1.4 The Episerver Group entities as set forth in the Data Processing Agreement shall be bound by the Episerver BCR. For further information on the structure and contact details, please refer to the Data Processing Agreement for customers, the Data Processing Agreements for partners and vendors, and/or the Episerver intra-company Data Processing Agreements.
- 1.5 Definitions. Capitalized terms used herein shall have the same definitions as set forth in the Episerver Data Processing Agreement unless explicitly stated otherwise herein,

2. Description of Processing and data flows

- 2.1 Details of Processing. Refer to Exhibit 3 of the Data Processing Agreement.
- 2.2 Customer Application. It is up to Customer to apply the Episerver BCR to all Personal Data processed for processor activities and that are submitted to EU law (for instance, data has been transferred from the European Union), or all processing of data processed for processor activities within the group whatever the origin of the data. Customers and partners/vendors may apply the Episerver BCR by entering into an Episerver Data Processing Agreement. Any such processing conducted under an Episerver Data Processing Agreement shall apply the Episerver BCR.

3. Duty to respect and comply

- 3.1 Binding Nature. The Episerver BCR is legally binding on each member of the Episerver Group including their employees to respect the Episerver BCR. The Episerver Group and its employees shall comply with the Episerver BCR, process Personal Data only upon Customer’s instruction and shall have a duty to respect the security and confidentiality of Personal Data in accordance with Data Protection Laws and Regulations and the Data Protection Agreement. The Episerver Group and its employees are obligated to undergo regular training on such topics and are contractually bound through their employment (or contractor) agreements to adhere to such policies and principles.

4. Data Subject rights as third-party beneficiary

- 4.1 The Episerver BCR grants rights to Data Subjects to enforce the Episerver BCR as third party beneficiaries directly against the Episerver Group where the requirements at stake are specifically directed to Episerver Group in accordance with Data Protection Laws and Regulations. Data Subjects may enforce the following elements of the Episerver BCR directly against the Episerver Group:
 - 4.1.1 Duty to respect the instructions from Customer regarding the data processing including for data transfers to third countries (Art. 28.3.a, 28.3.g., 29 GDPR),
 - 4.1.2 Duty to implement appropriate technical and organizational security measures (Art. 28.3.c and 32 GDPR and section 11 of the Episerver BCR) and duty to notify any Personal Data breach to Customer (Art. 33.2 GDPR).
 - 4.1.3 Duty to respect the conditions when engaging a Sub-processor either within or outside the Group (Art. 28.2, 28.3.d, 28.4, 45, 46, 47 GDPR, section 9 of the Episerver BCR).

- 4.1.4 Duty to cooperate with and assist Customer in complying and demonstrating compliance with the law such as for answering requests from Data Subjects in relation to their rights (Art. 28.3.e, 28.3.f, 28.3.h of GDPR and Sections 10 and 11 of the Episerver BCR).
- 4.1.5 Easy access to the Episerver Binding Corporate Rules (Art.47.2.g GDPR and Section 8 of the Episerver BCR).
- 4.1.6 Right to complain through internal complaint mechanisms (Art.47.2.i of GDPR and section 5 of the Episerver BCR).
- 4.1.7 Duty to cooperate with the Supervisory Authority (Art. 31, 47.2.l of GDPR).
- 4.1.8 Liability, compensation and jurisdiction provisions (Art.47. 2.e, 79, 82 GDPR and Section 7 of the Episerver BCR).
- 4.1.9 National legislation preventing respect of BCRs (Art.47.2.m of GDPR and Section 10 of the Episerver BCR).
- 4.2 Customer Ceases Business. Data Subjects may enforce the Episerver BCR against Episerver AB as a third-party beneficiary in situations where the Data Subject is not able to bring a claim against Customer; because such Customer has factually disappeared or ceased to exist in law or has become insolvent, unless any successor entity has assumed the entire legal obligations of Customer by contract or by operation of law, in which case the Data Subject can enforce its rights against such entity. In such a case, Data Subjects shall at least be able to enforce the Episerver BCR against the Sub-processor.
- 4.3 Right to Redress. A Data Subject's third-party beneficiary rights, if applicable, shall cover judicial remedies for any breach of the rights provided in the Episerver BCR and the right to receive compensation for damages. In particular, Data Subjects shall be entitled to lodge a complaint before the Supervisory Authority (choice between the Supervisory Authority of the EU Member State of his/her habitual residence, place of work or place of alleged infringement) and before the competent court of the EU Member State (choice for the Data Subject to act before the courts where the controller or processor has an establishment or where the Data Subject has his or her habitual residence pursuant to Article 79 of GDPR). Where the Processor and the controller involved in the same processing are found responsible for any damage caused by such processing, the Data Subject shall be entitled to receive compensation for the entire damage directly from the Processor (Art. 82.4 GDPR).

5. Processor liability

- 5.1 Episerver's Data Processing Agreements with Customers include a reference to the Episerver BCR. In accordance with such Data Processing Agreement, Customers shall have the right to enforce the Episerver BCR against the Episerver Group, including judicial remedies and the right to receive compensation. The Episerver Group has appointed Episerver AB to accept responsibility for and agree to remedy the acts of other members of the Episerver Group and third-party Sub-processors for breaches of the Episerver BCR or of third-party Sub-processors for breaches of the corresponding provisions of the written agreements with members of the Episerver Group.
- 5.2 Episerver AB accepts responsibility for and agrees to take the necessary action to remedy the acts of other Episerver Group members established outside of EU or breaches caused by external Sub-processor established outside of EU and to pay compensation for any direct regulatory damages or fines resulting from a violation of the Episerver BCR. Further, Episerver AB will accept liability to a Customer as if the violation had taken place by it in the Member State in which such Customer entity is based instead of the Episerver Group Member outside the EU or the external Sub-processor established outside of EU. This Episerver Group member will not rely on a breach by a Sub-processor (internal or external of the group) of its obligations in order to avoid its own liabilities. Episerver AB will have the burden of proof to demonstrate that the Episerver Group Member outside the EU or the external Sub-processor is not liable for any violation of the rules which has resulted in the Data Subject claiming damages. Liability arising from such actions shall follow the liability provisions within Episerver's Data Processing Agreements, or other contractual agreements between the parties.

6. Data Subject access

- 6.1 Access for the Customer. The Data Processing Agreement ensures that the Episerver BCR is part of Customer's agreement. The Episerver BCR will be annexed to the Data Processing Agreement or a reference to it will be made with a possibility of electronic access. The Episerver BCR is published on the website of the Episerver Group or other appropriate means in a way easily accessible to Data Subjects.
- 6.2 Access for Data Subjects: The Episerver Group shall promptly notify a Customer if the Episerver Group receives a request from a Data Subject for access to, correction, amendment or deletion of that person's Personal Data. The

Episerver Group shall not respond to any such Data Subject request without Customer's prior written consent except to confirm that the request relates to that Customer. The Episerver Group shall provide Customers with cooperation and assistance within a reasonable period of time and to the extent reasonably possible in relation to any request regarding Personal Data to the extent Customers do not have access to such Personal Data through their respective uses of the Services, in accordance to the provisions in the Episerver Data Processing Agreement.

7. Compliance

- 7.1 Training. Appropriate training on the Episerver BCR will be provided to personnel that have permanent or regular access to Personal Data, who are involved in the collection of Personal Data or in the development of tools used to process Personal Data. Such training is done through the Episerver learning management system, which both inventories the content of the training and the trainee's sessions and results. This is done on an annual basis.
- 7.2 Complaint Handling Process. The Episerver compliance department is responsible for handling complaints related to compliance with the Episerver BCR. Data Subjects may lodge a complaint about processing of their respective Personal Data that is incompatible with the Episerver BCR by contacting the relevant Customer or Episerver at the email address compliance@episerver.com. The Episerver Group shall promptly communicate the complaint to Customer to whom the Personal Data relates. The complaint handling process is detailed for Customers in their service level agreement, with Data Subjects in the Episerver privacy statement, and further detailed within the Episerver Trust Center.
- 7.3 Policy Audit Program. Episerver Group has data protection audits on regular basis (by either internal or external accredited auditors) or on specific request from the Global Data Protection Officer, or local data protection officer or operational head at Episerver, to ensure the verification of compliance with the Episerver BCR. Such audit program covers all aspects of the Episerver BCR including methods of ensuring that corrective actions will take place. The result of such audit will be communicated to the privacy officer/function and to the relevant board of the Episerver Group. Where appropriate, the result may be communicated to the ultimate parent's board. Supervisory Authorities may also access to the results of the audit upon request and they have the authority/power to carry out a data protection audit of any Episerver Group member if required. Episerver combines the audits with the annual audit process for its ISO 27001 certification process, and where such data privacy impact assessment report deems that such an audit must occur. Records of such audits are stored within the Episerver AB entity.
- 7.4 Sub-processor Facilities. If a Customer requests that any processor or Sub-processor processing the Personal Data on behalf of that Customer be audited for compliance with the Episerver BCR, such audits will be carried out pursuant to the terms of the Agreement with Customer and/or the Data Processing Agreement as applicable. Customers shall reimburse the Episerver Group for any time expended by Episerver Group or its third-party sub-processors at Episerver Group's then-current professional service rates, which shall be made available to Customers upon request.
- 7.5 Monitoring. Episerver has appointed a Data Protection Officer in line with article 37 of GDPR with responsibility to monitor compliance with the Episerver BCR and has the highest management support in exercising this function. A team of local data protection officers assists the Global Data Protection Officer as appropriate. The Global Data Protection Officer reports directly to the highest management level (GDPR Art. 38.3). Episerver Group has appointed a network of privacy personnel responsible for overseeing and ensuring compliance with Episerver Group's data protection responsibilities at a local and global level, including compliance with this Episerver BCR, advising the highest level of management on data protection matters, liaising with data protection authorities and their investigations, handling data protection-related complaints, monitors and annually reports on compliance at a global level, and at a local level, local data protection officers can be in charge of handling local complaints from data subjects, reporting major privacy issues to the Global Data Protection Officer, and monitoring training and compliance at a local level. Each member of the Episerver Group is assigned such a network of privacy personnel who support Episerver Group's Data Protection Officer and benefit from the support of Episerver Group's top management.

8. Cooperation and accountability

- 8.1 Audit Cooperation. Episerver Group will cooperate with and accept to be audited by the Supervisory Authorities competent for the relevant Customer and to comply with the advice of these Supervisory Authorities on any issue related to those rules. Episerver Sub-processors agree to co-operate and assist Customer to comply with Data Protection Laws and Regulations to the extent reasonably possible such as its duty to respect the data subject rights or to handle their complaints, or to be in a position to reply to investigation or inquiry from Supervisory Authorities). This shall be done in a reasonable time and to the extent reasonably possible. Customers shall reimburse Episerver Group for any time expended by Episerver Group or its third-party sub-processors for such audit at the Episerver Group's (or third-party sub-processor's) then-current professional service rates, which shall be made available to Customers

upon their request. Before any such on-site audit commences, the requesting Customer and the Episerver Group shall mutually agree upon the scope, timing, and duration of the audit in addition to the reimbursement rate for which Customer shall be responsible and such audits will be performed pursuant to the terms of the Data Processing Agreement. All reimbursement rates shall be reasonable, taking into account the resources expended by Episerver Group or its third-party sub-processors.

- 8.2 **Customer Cooperation.** Upon Customer's request, and subject to appropriate confidentiality obligations, Episerver Group will make available to Customer information necessary to demonstrate compliance with their obligations as provided by Article 28.3h of GDPR and allow for and contribute to audits, including inspections conducted by Customer or another auditor mandated by Customer. Such audits will be performed pursuant to the terms of the Data Processing Agreement. In addition, the Processor shall immediately inform Customer if in its opinion, an instruction infringes GDPR or other Union or Member State data protection provisions.
- 8.3 **Records.** Episerver Group members will maintain a record of all categories of processing activities carried out on behalf of each Customer in line with the requirements as set out in Art. 30.2 GDPR. Such records of processing activities will be limited to the Software Services as initially provisioned by Episerver. However, for Customers implementation, including edits, modifications, Customer Data, custom development, Episerver may provide assistance for Customers to comply with the appropriate measures under GDPR to the extent reasonably possible. Customers shall reimburse Episerver Group for any time expended by Episerver Group or its third-party sub-processors for such audit at the Episerver Group's then-current professional service rates, which shall be made available to Customers upon their request. This record will be maintained in writing, including in electronic form and will be made available to the Supervisory Authority on request (Art.30.3 and 30.4 GDPR).
- 8.4 **Compliance Facilitation,** As Episerver initially provisions the Software Services, Episerver Group may also assist Customer in implementing appropriate technical and organisational measures to comply with data protection principles and facilitate compliance with the requirements set up by the Episerver Group in practice such as data protection by design and by default (Art. 25 and 47.2.d GDPR) to the extent commercially possible. Customers shall reimburse Episerver Group for any time expended by Episerver Group or its third-party sub-processors for such assistance at the Episerver Group's then-current professional service rates.
- 8.5 If an Episerver Group member has reasons to believe that the existing or future legislation applicable to it may prevent it from fulfilling the instructions received from Customer or its obligations under the Episerver BCR or the Data Processing Agreement, it will promptly notify this to Customer which is entitled to suspend the transfer of data and/or terminate the contract, upon giving reasonable notice to Episerver AB, the Data Protection Officer, or to the Supervisory Authority, as prescribed in the Episerver Data Processing Agreement.
- 8.6 Any legally binding request for disclosure of the Personal Data by a law enforcement authority or state security body shall be communicated to Customer unless otherwise prohibited (such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation). In any case, the request for disclosure should be put on hold and the Supervisory Authority competent for Customer and the competent Supervisory Authority for the Processor should be clearly informed about the request, including information about the data requested, the requesting body and the legal basis for disclosure being sought in the request (unless otherwise prohibited).
- 8.7 Where any local legislation, requires a higher level of protection for Personal Data it will take precedence over the Episerver BCR. In any event data shall be processed in accordance with the applicable law.

9. Data protection safeguards

9.1 The following principles will be observed by each Episerver Group member:

- 9.1.1 **Transparency, fairness, and lawfulness.** Episerver Group and Sub-processors will have a general duty to help and assist Customer to comply with the law (for instance, to be transparent about Sub-processor activities in order to allow Customer

to correctly inform the Data Subject);

- 9.1.2 Purpose limitation. Episerver Group and Sub-processors will process the Personal Data only on behalf of the Customer and in compliance with its documented instructions including with regard to transfers of Personal Data to a third country, unless required to do so by Union or Member State law to which the Processor is subject. In such a case, the Processor shall inform Customer of that legal requirement before processing takes place, unless that law prohibits such information on important grounds of public interest (Art. 28.3a of GDPR). In other cases, if the Processor cannot comply for whatever reason, it agrees to promptly inform Customer of its inability to comply, in which case Customer is entitled to suspend the transfer of data and/or terminate the contract, upon giving reasonable notice to Episerver AB, the Data Protection Officer, or to the Supervisory Authority, as prescribed in the Episerver Data Processing Agreement.
- On the termination of the provision of Software Services related to the data processing, Episerver Group and Sub-processors shall, at the choice of the Customer, delete or return all the Personal Data transferred to Customer and delete the copies thereof in accordance with the terms of Agreement and/or Data Processing Agreement. In that case, the Episerver Group and the Sub-processors will inform Customer and warrant that it will guarantee the confidentiality of the Personal Data transferred and will not actively process the Personal Data transferred anymore.
- 9.1.3 Data quality. Episerver Group and Sub-processors will help and assist Customer to comply with the law, in particular:
- 9.1.3.1 Episerver Group and Sub-processors will execute any necessary measures when asked by Customer, in order to have the data updated, rectified or deleted. Episerver Group and Sub-processors will inform each Episerver Group member to whom the data has been disclosed of any updating, rectification, or deletion of data.
- 9.1.3.2 Episerver Group and Sub-processors will execute any necessary measures, when asked by Customer, in order to have the data deleted or anonymised from the moment identification of the Data Subject is not necessary anymore. Episerver Group and Sub-processors will communicate to each entity to whom the data has been disclosed of any deletion or anonymisation of data.
- 9.1.4 Security. Episerver Group and Sub-processors will implement all appropriate technical and organizational measures to ensure a level of security appropriate to the risks presented by the processing as provided by Article 32 of GDPR. Episerver Group and Sub-processors will assist the Customer in ensuring compliance with the obligations as set out in Articles 32 to 36 of GDPR taking into account the nature of processing and information available to the Processor (Art.28-3-f of GDPR). Episerver Group and Sub-processors will implement technical and organisational measures which at least meet the requirements of Customer's applicable law and any existing particular measures specified in the Data Processing Agreement. Episerver Group shall inform Customer without undue delay after becoming aware of any Personal Data breach. In addition, Sub-processors shall have the duty to inform Episerver Group and Customer without undue delay after becoming aware of any Personal Data breach.
- 9.1.5 Data Subject rights. Episerver Group and Sub-processors will execute any appropriate technical and organizational measures, insofar as this is possible, when asked by Customer, for the fulfilment of Customer's obligations to respond to requests for exercising the Data Subjects rights as set out in Chapter III of GDPR (Art. 28.3e of GDPR) including by communicating any relevant information in order to help Customer to comply with the duty to respect the rights of the Data Subjects. Episerver Group and Sub-processors will transmit to Customer any Data Subject request without answering it unless authorized to do so.
- 9.2 Sub-processing within the Group. Data may be sub-processed by other Episerver Group members bound by the Episerver BCR only with the prior informed specific or general written authorization of Customer. A general prior authorization will be given at the beginning of the Software Services, including within the Episerver Data Processing Agreement, provided Customer will be informed by Episerver Group of any intended changes concerning the addition or replacement of a Sub-processor in such a timely fashion that Customer has the possibility to object to the change or to terminate the contract before the data are communicated to the new Sub-processor in accordance with the Data Processing Agreement.
- 9.3 Onward transfers to external Sub-processors. Data may be sub-processed by Sub-processors which are not members of Episerver Group only with the prior informed specific or general written authorization of Customer. If a general authorization is given, including within the Episerver Data Processing Agreement, Customers will be informed by Episerver Group of any intended changes concerning the addition or replacement of Sub-processors in such a timely fashion that Customer has the possibility to object to the change or to terminate the contract before the data are communicated to the new Sub-processor.
- 9.4 Adequate Protections. Where the Episerver Group member bound by the Episerver BCR subcontracts its obligations under the Data Processing Agreement, with the authorization of Customer, including within the Episerver Data Processing Agreement, it shall do so only by way of a contract or other legal act under Union or Member State law with the Sub-processor which provides that adequate protection is provided as set out in Articles 28, 29, 32, 45, 46, 47 of GDPR and which ensures that the same data protection obligations as set out in the Data Protection Agreement and in particular providing sufficient guarantees to implement appropriate technical and organization measures in such a manner that the processing will meet the requirements of GDPR (Art. 28.4 of GDPR).