

Data Processing Agreement

This Data Processing Agreement applies between you, hereinafter referred to as the “Customer” or “Controller” and Inriver AB, hereinafter referred to as “Inriver” or the “Processor”.

1. BACKGROUND

- 1.1. The Controller and the Processor have entered into a Master Subscription Agreement regarding the Inriver PIM Service and subsequent Order Forms (jointly hereinafter referred to as the "MSA") and may have entered into a Professional Service Agreement regarding implementation services (the "PSA"). The MSA and the PSA are jointly referred to as the "Main Agreements" and the Processor will through the service provided in accordance with the Main Agreements process Personal Data (see definition below) on behalf of the Controller.
- 1.2. The EU General Data Protection Regulation 2016/679 ("GDPR"), requires a written agreement between a controller and a processor in order to allow the processing of Personal Data by the processor on behalf of the controller. For this reason, the parties have agreed to enter into this Data Processing Agreement.

2. DEFINITIONS

- 2.1. **"Affiliate"** means any legal entity that is directly or indirectly controlled by or under common control of a Party.
- 2.2. **"Customer Data"** means all data, including all text, sound, video or image files and software that is provided to Processor by, or on behalf of, Controller through the Inriver PIM Service.
- 2.3. **"Data Protection Law(s)"** means the applicable law or any other (local) applicable regulations regarding data privacy, including but not limited to GDPR, UK GDPR including the Data Protection Act 2018 and California Consumer Privacy Act of 2018 (Cal. Civ. Code § 1798.100 et seq.), as amended by the California Privacy Rights Act of 2020 (Proposition 24).
- 2.4. **"Data Subject"** means what is stated in GDPR article 4 (1) regarding Data Subjects.
- 2.5. **"Personal Data"** means what is stated in GDPR article 4 (1) but does not include any data uploaded by the Controller to the Inriver PIM environment as product content which is not permitted.
- 2.6. **"Processing" or "to Process"** means what is stated in in GDPR article 4 (2).
- 2.7. **"Services"** has the meaning provided in the Main Agreements and include the PIM Service provided by Inriver as well as related Professional Services.
- 2.8. **"Sub-processor"** means any third party engaged by the Processor, or its Sub-processor, to Process Personal Data on behalf of the Controller as described in GDPR article 28.

3. DATA PROCESSING

- 3.1. This Data Processing Agreement is agreed upon on behalf and for the benefit of the Controller and its Affiliates. Where in this Data Processing Agreement reference it made to the Controller, this shall also mean any Affiliate of the Controller. The Controller is entitled to enforce this Data Processing Agreement for itself and on behalf of any of its Affiliates. Furthermore, Affiliates of the Controller are entitled to

enforce this Data Processing Agreement as if these Affiliates are parties to this Data Processing Agreement.

- 3.2. Processor agrees to comply with Data Protection Laws applicable to its provision of the Services. However, Processor is not responsible for compliance with any laws or regulations applicable to Controller or Controller's industry that are not generally applicable to information technology service providers. Processor does not determine whether Controller's data includes information subject to any specific law or regulation.
- 3.3. Controller must comply with all Data Protection Laws applicable to its use of Services including laws related to biometric data and confidentiality of communications. Controller is responsible for determining whether the Services are appropriate for storage and processing of information subject to any specific law or regulation and for using the Services in a manner consistent with Controller's legal and regulatory obligations. Controller is responsible for responding to any request from a third-party regarding Controller's use of the Services. To the avoidance of doubt, this Data Processing Agreement applies only to the Processing of data in environments controlled by Processor or its Sub-processors. This includes data sent to Processor through Services but does not include data that remains on Customer's premises or in any Controller selected third party operating environment.
- 3.4. The Processor shall only Process the Personal Data in accordance with the instructions stated in this Data Processing Agreement, and the Controller may only submit information to Processors, including to the Inriver PIM Service, in accordance with this instruction, unless otherwise expressly agreed in writing by the Parties. The Processor shall without delay inform the Controller if it comes to the Processor's attention that, in its opinion, any of the written instructions of the Controller infringes Data Protection Law. The Processor shall have no independent say in relation to the Personal Data that it Processes. The Processor shall not Process the Personal Data for its own or any third party's benefit or purposes, or for other purposes, unless otherwise required by Data Protection Law. If required to do so under Data Protection Law and to the extent Processor is aware, the Processor shall inform the Controller of these relevant requirements before any processing takes place. Controller authorises Processor to create aggregated statistical non-personal data from data containing pseudonymised identifiers (such as usage logs containing unique and pseudonymised identifiers) and to calculate statistics related to Customer Data.
- 3.5. The Controller must prior to requesting any Processing of Personal Data make sure that the written instructions to the Processor include the relevant category of Personal Data as well as the relevant category of Data Subjects (as defined in the GDPR).
- 3.6. The Processor shall enable the Controller to access, rectify, erase, restrict and transmit the Personal Data Processed by the Processor. The Processor shall comply with any instruction related to the above without undue delay. If the Controller erases, or instructs the Processor to erase, any Personal Data held by the Processor, the Processor shall ensure that the Personal Data is erased so that it cannot be recreated by any party.
- 3.7. The Processor shall notify the Controller without undue delay regarding any contacts with a supervisory authority, of significance for, the Processing of Personal Data carried out on behalf of the Controller.
- 3.8. The Processor shall assist the Controller in its contacts with any supervisory authority, including, upon the Controller's instruction, by providing any information requested by the supervisory authority. For the avoidance of doubt, the Processor may not disclose Personal Data or any information on the Processing of Personal Data without explicit instructions from the Controller unless required by law. If the assistance required by Controller constitutes extensive additional work for Processor, Processor may charge the

Controller a reasonable fee for such additional work after the approval of such additional extensive work and fees by Controller in writing.

- 3.9.** If a Data Subject requests information from the Processor concerning the Processing of Personal Data, the Processor shall forward the request to the Controller and assist the Controller in responding to such request as obliged by Data Protection Law. The Processor shall assist the Controller by appropriate technical and organizational measures, taking into account the nature of the Processing and the functionality of the Services. The Controller will be responsible for responding to any such request.
- 3.10.** The Processor shall solely disclose Personal Data to those personnel, other persons engaged by the Processor and/or subcontractors who necessarily need (access to) the Personal Data for the performance of the obligations under the Main Agreements, and for the remainder keep the Personal Data confidential, unless otherwise required under Data Protection Law. The Processor shall impose adequate contractual obligations regarding confidentiality and security upon its personnel and other persons engaged by the Processor which have been authorised to Process Personal Data.
- 3.11.** The Processor shall assist the Controller in ensuring compliance with the Controller's obligations under Data Protection Laws, e.g. assist with security measures, data protection impact assessments (including prior consultation), and in situations involving Data Breach (as defined in Section 6.1). If the assistance required by Controller constitutes extensive additional work for Processor, Processor may charge the Controller a reasonable fee for such additional work after the approval of such additional extensive work and fees by Controller in writing. Controller is solely responsible for making an independent determination as to whether the technical and organisational measures for the Services meet Controller's requirements including any of its security obligations under Data Protection Laws. Controller acknowledges and agrees that the security practices and policies implemented and maintained by Inriver provide a level of security appropriate to the risk with respect to its Customer Data and Personal Data. Controller is responsible for implementing and maintaining privacy protections and security measures for components that Controller provides or controls.
- 3.12.** The Processor shall maintain a record of Processing activities carried out on behalf of the Controller.

4. INSTRUCTIONS FOR THE PROCESSING OF PERSONAL DATA

- 4.1.** The Controller instructs the Processor to Process the following on behalf of the Controller.
- 4.1.1.** The Personal Data will be Processed for the following purposes:
- i. Data needed for accounts required for managing the Services provided under the Main Agreements.
 - ii. Data to supervise the usage of the Services provided under the Main Agreements.
- 4.1.2.** The Personal Data Processed contains the following categories of Data Subjects:
- i. Controller's employees.
 - ii. Employees of any third party contracted by Controller.
- 4.1.3.** The Personal Data Processed contains the following categories of Personal Data:
- i. Name, login information and other account information and the usage of the Services provided under the Main Agreements.
- 4.1.4.** The Personal Data will only be accessed by the following groups of personnel of or other persons engaged by the Processor:
- i. Inriver's employees within cloud operations, product support and product development; and

- ii. Employees and contractors of subcontractors engaged within cloud operations, product support and product development.

4.1.5. The Personal Data Processed will be subject to the following basic Processing activities:

- i. Create, update and delete accounts in the Services provided under the Main Agreements; and
- ii. Record and store the usage of the Services provided under the Main Agreements.

4.1.6. The Personal Data will be Processed with the following duration:

- i. During the use of the Services provided under the Main Agreements.

5. SECURITY

- 5.1. The Processor shall implement appropriate technical and organisational security measures to protect the Personal Data in accordance with Data Protection Laws. The Processor shall regularly review its technical and organisational security measures and update them where necessary in accordance with such laws and regulations.

6. DATA BREACHES

- 6.1. The Processor shall maintain adequate procedures designed to detect and respond to any accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data ("Data Breaches"), including procedures for preventive and corrective actions, and to avoid recurrence of any Data Breaches. These procedures shall be established by the Processor in such a manner that both the Processor and the Controller will be able to meet their notification and documentation duties in relation to Data Breaches under Data Protection Law.

- 6.2. Upon discovery or reasonable suspicion of a Data Breach, the Processor shall without undue delay take adequate recovery measures. Furthermore, the Processor shall provide all reasonable or requested feedback to the Controller and provide full effective support to the Controller and the (possibly) affected Data Subjects. The feedback and support should include at least:

6.2.1. a description of the preventive and corrective measures taken and to be taken, planned and recommended to minimise possible harm, including an emergency plan, and the expected resolution and work-around time;

6.2.2. the contact details of the authorised representative(s) of the Processor from whom the Controller may obtain immediate and regular updates on the status of the Data Breach; and

6.2.3. any other information that could help to minimise possible harm or damage of the organisation of the Controller and the privacy of the affected Data Subject(s).

- 6.3. The Processor shall provide the Controller also with all reasonable other assistance and share with the Controller also all other necessary or by the Controller requested information, so that the Controller will be able to notify, if applicable, the Data Subject(s) that was (were) (possibly) affected and/or the competent supervisory authorities of the Personal Data of the Data Breach in a timely manner. The Processor shall enable the Controller to demonstrate compliance with the Data Protection Law in relation to its Data Breach notification duties.

- 6.4. The Processor shall provide the Controller with all assistance necessary to document any Data Breaches in conformity with the obligations that rest upon the Controller under Data Protection Law and in a manner that enables the competent supervisory authorities to examine the compliance of the Processor and/or the Controller in relation to Data Breach notification duties under Data Protection Law.

- 6.5. The Processor shall undertake an internal review without undue delay after a Data Breach to determine and execute any appropriate corrective measures to avoid a recurrence or occurrence of a similar situation without prejudice to any audit rights of the Controller. Processor's notification to a Data Breach under this Section 6 is not an acknowledgment by Inriver of any fault or liability with respect to the Data Breach. Customer must notify Inriver promptly about any possible misuse of its accounts or authentication credentials or any security incident related to the Services.

7. SECURITY REPORTS AND AUDITS

- 7.1. The Processor must be able to verify its compliance with this Data Processing Agreement and Data Protection Laws and shall maintain adequate documentation verifying fulfillment of its obligations hereunder. The Processor shall evaluate the Processing activities and the security measures on a regular basis.
- 7.2. The Processor shall take appropriate measures in order to adequately recover the observed threats, weaknesses and other identified problems.
- 7.3. The Controller, or a third party approved by the Controller, may conduct audits to ensure that the Processor is complying with this Data Processing Agreement and Data Protection Law. The Processor shall, upon the Controller's request and without undue delay, provide necessary assistance and allow inspection of any relevant documentation. Each Party shall bear its own costs related to the audit.

8. SUB-PROCESSING

- 8.1. The Controller hereby gives the Processor a general consent to engage Sub-processors for Processing of Personal Data on behalf of the Controller. The Sub-processors engaged or that may be engaged by the Processor to which the Controller consents, the location of the Sub-processor and a description of the current Processing activities carried out by the Sub-processor are listed on Inriver's trust website (<https://trust.inriver.com/>). The Processor shall inform the Controller before transferring any Personal Data to a new Sub-processor through updates on the Trust-page which the Controller can subscribe to in order to receive automatic notifications. Following receipt of such information the Controller shall within 30 days notify the Processor if it objects to the new Sub-processor and may terminate the relevant Main Agreement and this DPA with a 60 days' notice period. If the Controller does not terminate the relevant Main Agreement and this DPA within 30 days from receiving the notification about the new Sub-Processor, the Controller shall be deemed to have accepted the Sub-processor. During the termination period, the Processor is not allowed to transfer any Personal Data to the new Sub-processor. If this Data Processing Agreement and the relevant Main Agreement have not been terminated by Controller in accordance with above, Personal Data may be transferred to the new Sub-processor. Inriver may also engage Sub-processors to provide certain limited or ancillary services on its behalf. Customer consents to this engagement and to Inriver Affiliates as Sub-processors. Such authorisation constitutes Controller's prior written consent to the subcontracting by Inriver of the processing of Customer Data and Personal Data to the extent such consent is required under Data Protection Laws.
- 8.2. The Processor shall enter into appropriate written agreements with all of its Sub-processors on terms which in all materially respects correspond to the obligations as set out in this Data Processing Agreement. The Processor shall remain fully liable to the Controller for the performance or non-performance of the Sub-processor's obligations.
- 8.3. Upon the Controller's request, the Processor is obliged to provide information regarding any Sub-processor, including name, address and the Processing carried out by the Sub-processor.

9. TRANSFER OF PERSONAL DATA OUTSIDE THE EEA/US

- 9.1.** The transfer of data to a state which is not a member state of either the EU or the EEA may only occur after the specific conditions of Article 44 et seq. GDPR have been fulfilled. To the extent Controller is a US legal entity and has requested that all Customer Data is stored in the US, transfer outside the United States may only occur as needed to provide the Services.
- 9.2.** To the extent the Processor uses AI-systems that may result in Personal Data being accessed or processed from locations outside the EEA or the United States, such transfers shall only occur on the basis of appropriate safeguards under Article 46 of the GDPR including Standard Contractual Clauses (SCCs) adopted by the European Commission, or another applicable transfer mechanism. The Processor shall maintain a current record of such transfers and the applicable transfer mechanisms on the Inriver trust page (link set out in Section 8.1 above).

10. INDEMNIFICATION ETC

- 10.1.** If the Processor Processes Personal Data in breach of the Controller's lawful instructions, this Data Processing Agreement or any Data Protection Law, the Processor shall indemnify and hold the Controller harmless for any loss, cost or damage, including but not limited to claims by a Data Subject, financial penalties imposed by supervisory authorities or other competent authorities, due to the Processor's (or its Sub-processors') Processing of the Controller's Personal Data.
- 10.2.** If the Processor breaches Data Protection Laws as a result of the Controller's unlawful instructions or as a result of Controller's breach of this Data Processing Agreement or any Data Protection Law including without limitation failure to correctly specify relevant categories, the Controller shall indemnify and hold the Processor harmless for any loss, cost or damage, including but not limited to claims by a Data Subject, financial penalties imposed by supervisory authorities or other competent authorities, due to the Processor's (or its Sub-processors') Processing of the Controller's Personal Data.
- 10.3.** In case of claims by a Data Subject or financial penalties imposed by supervisory authorities or other competent authorities, the Controller shall: (a) notify the Processor promptly in writing of any such potential or pending claims or penalties; (b) use reasonable endeavors to reduce or avoid such claims or penalties; (c) allow the Processor to comment on any response, settlement, defense or appeal in relation to such claim; and (d) to a reasonable extent provide the Processor with information in relation to the same.
- 10.4.** The limitations of liability set out in the relevant Main Agreement shall apply also to this Agreement.

11. REQUESTS OF GOVERNMENTAL AUTHORITIES

- 11.1.** In case the Processor receives a request from a governmental authority relating to Personal Data, the Processor shall, prior to providing Personal Data, without delay inform the Controller thereof in writing, and provide the Controller with copies of all the correspondence it has received in this respect. The Processor shall only respond to such request in case of a specific legal obligation under Data Protection Law. The Controller may provide the Processor with reasonable instructions in this respect which the Processor shall follow, unless this would stand in the way of fulfilling the aforementioned legal obligation under Data Protection Law.
- 11.2.** To safeguard the protection of Personal Data, the Processor shall ensure that it will not provide more Personal Data to the competent governmental authority than necessary to meet the request of such governmental authority.

11.3. If the Processor receives a request from a competent governmental authority to provide Personal Data and such request does not allow the Processor to inform third parties, including the Controller, about the request and the possible subsequent provision of Personal Data, the Processor shall become data controller solely for carrying out this request. As soon as it is permissible, the Processor shall immediately inform the Controller about the request that was received and the provision of Personal Data, and provide the Controller with copies of all the correspondence received and sent in this respect.

12. TERM

12.1. Upon termination of the Main Agreements the Processor shall submit all Personal Data relevant for the terminated Main Agreement to the Controller on an appropriate medium and thereafter erase the Personal Data. The Processor shall, after a written request from Controller, provide the Controller with a statement in writing and a guarantee, and allow the Controller to verify, that the Personal Data will no longer be processed by the Processor or a Sub-processor engaged by the Processor.

12.2. This Data Processing Agreement is applicable from the date of its execution and until all Personal Data is erased in accordance with section 12.1

12.3. Any obligation arising from this Data Processing Agreement that by nature has post-contractual effect shall continue to be in effect after the termination of this Data Processing Agreement.

12.4. The Processor and the Controller shall herewith in advance consent to amendments to this Data Processing Agreement that due to changed circumstances are necessary to maintain compliance with any Data Protection Law or any required changes due to an opinion, order, warning or other decision or action by a competent supervisory authority.

13. GOVERNING LAW AND DISPUTE RESOLUTION

13.1. This Data Processing Agreement shall be governed by the laws designated by the Main Agreement if such jurisdiction is in the EU. If the Main Agreement designates a jurisdiction outside the EU, this Data Processing Agreement shall be governed by the laws of Sweden.

13.2. Any dispute, controversy or claim arising out of, or in connection with this Data Processing Agreement shall be subject to dispute resolution in accordance with the Main Agreement.