Data Processing Agreement
for contracts concerning the "pretix" ticket shop software

between

rami.io GmbH
Markgräfler Str. 16, 69126 Heidelberg, Germany
– Processor / Provider –

and

DEMO MUSTER SAMPLE
– Controller / Customer –

This document is a sample of the Data Processing Agreement and should not be signed and returned to us! Please access the personalized copy we prepared for you from within your pretix organizer account in the "Data Protection"-section.

§ 1 Subject matter

(1) The Processor (also referred to herein as the "Provider") processes data in the name of the Controller (also referred to hereinafter as the "Customer") by providing technical infrastructure for the execution of purchases.

(2) To accomplish this, the Processor provides a software product for use via the Internet in accordance with the General Terms and Conditions for contracts concerning the "pretix" ticket shop software version 1.6 dated March 26, 2021, Service Level Agreements (SLA) and technical specifications of pretix, as well as (if applicable) customer-specific contract amendments (together hereinafter referred to as the "Primary Contract"). The software is operated by the Processor in a computer center and made available to the Customer for use via the Internet (also referred to as the "Software as a Service" model).

(3) As part of its operations, the Provider processes personal data for the Controller within the meaning of Art. 4 No. 2 and Art. 28 General Data Protection Regulation (GDPR) with respect to the agreements of the Primary Contract, SLA and technical specifications which are referenced here.

(4) This supplemental agreement specifies the obligations of the parties concerning data protection arising under the Primary Contract. It applies to all activities in connection with the Primary Contract in which employees of the Provider or third parties engaged by the Provider are exposed to personal data of the Customer.

§ 2 Term

(1) The term of this supplemental agreement is based on the term of the Primary Contract.

(2) The Controller may terminate the contract at any time without notice if there is a serious breach by the Provider of data protection regulations or the provisions of this contract, if the Provider is unable or unwilling to comply with instructions given by the Controller or if the Provider refuses the exercise of

control rights on the part of the Controller in breach of contract. In particular, failure to comply with the obligations agreed in this contract and derived from Art. 28 GDPR constitutes a serious breach.

§ 3 Specification of processing

(1) The contractually agreed service will be provided exclusively within a Member State of the European Union or in a Contracting State to the Agreement on the European Economic Area. Any transfer of the service, or sub-parts thereof, to a third country requires the prior consent of the Controller and is only permitted if the special requirements of Art. 44 et seq. GDPR (e.g. Commission adequacy decision, standard data protection clauses, approved codes of conduct) are met.

(2) Type and purpose of data processing are primarily defined by the Primary Contract.

(3) In particular, the processing of data consists in collection, logging, storage, and evaluation of the data entered by the Controller and its customers, as well as transmission of this data to the Customer.

(4) Types of personal data:

a) Person data
b) Communication data (e.g. phone, e-mail)
c) Contract data (Contractual relationships, interest in products or contracts)
d) Customer history
e) Billing and payment data
f) Planning and controlling data
g) Informational data from third parties (e.g. from public directories)

(5) Specifically, the following data is processed:

a) Order data, in particular products ordered as well as email addresses and names. Depending on the Controller's settings, invoice addresses, delivery addresses or entries in form fields defined by the Controller will also be processed.
b) Visitor data for the online shop, in particular number of visitors and origin of visitors via certain links, as well as voluntarily collected email addresses from potential buyers for products that are currently not available.
c) Payment information depending on the method of payment chosen by the buyer, e.g. bank details. For online payment methods such as PayPal or credit card, the Controller must commission an external service provider to process the payment and the Provider only receives at most the data provided to the interface by the external service provider. As a rule, this includes names and account names but not complete credit card numbers, for example.
d) Technical data that is inherently generated when operating a publicly-accessible website (e.g. server logs). IP addresses and browser IDs are usually not stored as a rule, but rather only for diagnostic purposes in the event of a technical error.
e) Emails and metadata related to support cases or contact on the part of the Controller or its customers to the Provider's customer service.
f) Authentication data for the Controller's employees who are entitled to use the software.
g) Logs of software use by the Controller and its employees to ensure the transparency of entries.

(6) Categories of data subjects:

a) Employees of the Controller
b) Customers of the Controller
c) Prospective customers and visitors to the Controller's online shop

§ 4 Rights and obligations and the Controller's authority to issue instructions

(1) The Controller is solely responsible for assessing the lawfulness of the processing pursuant to Art. 6 para. 1 GDPR and for safeguarding the rights of the data subjects pursuant to Art. 12 to 22 GDPR. Nevertheless, the Provider is obliged to immediately forward all such inquiries to the Controller, provided that they are obviously directed exclusively to the Controller.

(2) As a rule, the Controller places all orders, partial orders and instructions by means of appropriate configuration, installation and use of the software. Any further instructions, changes to the object to be processed and changes to procedures must be agreed jointly between the Controller and the Provider and specified in writing or by email. Verbal instructions must be confirmed immediately in writing or in a documented electronic format.

(3) The Controller shall immediately inform the Provider if it discovers errors or irregularities when examining the results of processing.

(4) The Controller is entitled - by appointment as a rule and without interruption of the Processor's business operations - to satisfy itself of compliance with the technical and organizational measures undertaken by the Processor and with the obligations set out in this contract both before the start of processing and then regularly thereafter in an appropriate manner. An employee of the Processor needs to be present all times during this process. The Controller may send a third-party in its place, as long as this third-party is not a competitor of the Processor. The Processor may charge the Customer for any efforts related to this.

(5) The Controller is obliged to treat confidentially all knowledge of business secrets and data security measures of the Provider it acquires within the scope of their contractual relationship. This obligation shall survive the termination of this contract.

§ 5 Persons authorized to issue instructions on behalf of the Controller; Recipients of instructions at the Provider

(1) Persons authorized to issue instructions on behalf of the Controller include all employees of the Controller for whom the Controller has set up personal access to the software provided.

(2) Recipients of instructions at the Provider include all employees of the Provider whose duties include written or electronic customer service. Susanne Kasper (email: datenschutz@rami.io, tel. +49 6221 3217713) is the data protection contact person.

(3) Instructions must be given by configuring the software accordingly, by email to support@pretix.eu or by mail to the address set out above. The instructions must be retained for their period of validity and subsequently for three full calendar years.

§ 6 Duties of the Provider

(1) The Provider processes personal data exclusively within the scope of agreements that have been reached and in accordance with instructions from the contracting Controller, unless it is obliged to process in another manner by the EU law or the law of a Member State to which the processor is subject (e.g. investigations by law enforcement or state security authorities); in such a case, the contract data process shall inform the Controller of the relevant legal requirements prior to processing unless the law in question prohibits such communication on account of an important public interest (Art. 28 para. 3, second sentence a) GDPR).

(2) The Provider may not use personal data provided for processing for any other purposes, in particular not for its own purposes.

(3) Within the context of processing personal data in accordance with the respective contract, the Provider warrants that all agreed measures will be carried out in accordance with the contract.

(4) The Controller's data will be processed with the data of other clients on common physical systems. It is therefore not possible to hand over or destroy specific data storage media but rather it is only possible to delete certain data on the relevant data storage media. The Provider shall ensure that each client may only access its respective data by means of authorization rules.

(5) The Provider is required to cooperate to the extent necessary when the Controller is giving effect to the rights of data subjects pursuant to Articles 12 to 22 GDPR, in the preparation of records of processing activities and in the case of required data protection impact assessments from the Controller and shall provide reasonable support the Controller to the extent possible (Art. 28 para. 3, second sentence e) and f) GDPR).

(6) The Provider shall notify the Controller immediately if it believes that an instruction given by the Controller violates applicable laws and regulations (Art. 28 para. 3, third sentence GDPR). The Provider is entitled to suspend execution of the instructions concerned until it they are confirmed or modified person responsible at the Controller following a review.

(7) The Provider is required to correct, delete or restrict the processing of personal data within the scope of the contractual relationship if the Controller so requests by means of an instruction and this does not conflict with the Provider's legitimate interests.

(8) The Provider may only provide information concerning personal data to third parties after prior instruction or approval by the Controller. Such an instruction to share data with third parties is deemed expressly given in particular if the Controller activates and configures the functions of the software for communication with external service providers, e.g. payment service providers or newsletter service providers.

(9) The Provider agrees that the Controller is entitled - by appointment as a rule and without interruption of the Processor's business operations - to monitor compliance with data protection and data security regulations and contractual agreements to an appropriate and necessary extent either itself or via third parties commissioned by the Controller, in particular by obtaining information and inspecting the stored data and the data processing programs as well as through on-site inspections and audits (Art. 28 para. 3 second sentence h) GDPR). The Controller may send a third-party for this purpose, as long as the third party is not a competitor of the Processor.

(10) The Provider warrants that, where necessary, it will assist in these controls by allowing the necessary inspections. The Provider may demand payment for any expenses or efforts incurred in this connection.

(11) The Controller agrees that some of the Provider's employees may work from private homes (telecommuting or home office) and that some of them may have partial access to data for the purpose of error analysis. The Controller's data will not be permanently stored in private homes and the measures pursuant to Art. 32 GDPR must also be ensured in this case.

(12) The Provider confirms that it is aware of the relevant data protection rules contained in the GDPR with regard to contract data processing.

(13) The Provider undertakes to maintain confidentiality when processing the Controller's personal data in accordance with the respective contract. This shall continue to apply even after termination of the contract.

(14) The Provider warrants that it will familiarize the employees involved in the performance of the work with the data protection provisions applicable to them prior to commencement of the work and will undertake to maintain appropriate confidentiality for the duration of their work and after termination of their employment (Art. 28 para. 3, second sentence b) and Art. 29 GDPR). The Provider shall monitor compliance with data protection rules and regulations within its company.

(15) An in-house data protection officer has been appointed by the Provider, even if there is no legal requirement for such an appointment. The contact person for data protection questions is Susanne Kasper (Email: datenschutz@rami.io, Tel. +49 6221 3217713).

§ 7 Provider's notification duties in the event of processing disruptions and personal data breaches

(1) The Provider shall immediately inform the Controller of any disruptions, infringements by the Provider or by persons in its employ both of data protection laws and the specifications of the respective contract as well as of suspected personal data breaches or irregularities in the processing of personal data. This applies in particular regard to any reporting and notification obligations on the part of the Controller pursuant to Art. 33 and Art. 34 GDPR. The Provider warrants that it will adequately support the Controller, if necessary, in connection with its obligations under Articles 33 and 34 GDPR (Art. 28 para. 3, second sentence f) GDPR). The Provider may only provide notifications under Articles 33 or 34 GDPR for the Controller upon prior instruction according to Section 4 of this contract.

(2) Such notifications to the Controller are to be sent by e-mail to the primary contact address stored by the Controller in the software.

§ 8 Relationships with subcontractors

(1) A subcontractor relationship subject to a reporting obligation within the meaning of this section does not exist if the Provider commissions third parties as part of an ancillary service, such as external telecommunication services, postal and shipping services, maintenance, user service, or the disposal of storage devices. In these cases, the Processor is still obliged to take appropriate measures to ensure confidentiality and security of the processed data in these cases.

(2) Pursuant to Art. 28 para. 2 GDPR, the Controller agrees that the Provider in general may use subcontractors to perform its contractual duties.

(3) The Provider must ensure that it selects the subcontractor carefully, particularly taking into account the technical and organizational measures taken by the subcontractor within the meaning of art. 32 GDPR. The relevant test documents shall be made available to the Controller on request.

(4) Subcontractors in third countries may only be commissioned if the special requirements of Art. 44 et seq. GDPR (e.g. Commission adequacy decision, standard data protection clauses, approved codes of conduct) have been satisfied.

(5) The Provider is required to contractually ensure that the provisions agreed between the Controller and the Provider also apply to subcontractors. The contract with the subcontractor shall specify the details to such an extent that the responsibilities of the Provider and the subcontractor are clearly defined. If several subcontractors are used, this also applies to the responsibilities between such subcontractors.

(6) In particular, the Controller must be entitled, if necessary, to have appropriate controls and inspections carried out, including on site, at the subcontractor, whether by itself or by a third parties acting on its behalf. The contract with the subcontractor must be set out in writing, which may also include in an electronic format (Art. 28 para. 4 and para. 9 GDPR).

(7) Passing on personal data to subcontractors is only allowed after all requirements from this paragraph and GDPR are complied with.

(8) At present, the subcontractors specified in Annex A by name, address and subject of the commission are engaged in the processing of personal data to the extent specified for the subcontractor concerned. The Controller declares its agreement to their commission.

(9) In all cases, the Provider shall inform the Controller in advance of any intended change in relation to the involvement or replacement of other contractors, giving the person responsible the possibility of objecting to such changes within a period of 14 days.

(10) In the event of an objection, the Provider may terminate the contract in accordance with the regular notice periods of the Primary Contract if continuation of the service is unreasonable without the intended change. In this case, the Provider must ensure that none of the Controller's data is transferred to the new subcontractor.

§ 9 Technical and organizational measures according to Art. 32 GDPR (Art. 28 para. 3, second sentence c) GDPR)

(1) A level of protection appropriate for the risks for the rights and freedoms of the natural persons affected by the processing shall be guaranteed for the specific contract data processing. To this end, the protective objectives of Art. 32 para. 1 GDPR, such as confidentiality, integrity and availability of systems and services and their resilience with regard to the type, scope, circumstances and purpose of processing, are taken into account in such a way that the risk is permanently mitigated by appropriate technical and organizational remedial measures.

(2) The technical and organizational measures undertaken by the Provider are described in Annex B.

(3) The Provider must carry out testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing as needed but at least once a year (Art. 32 para. 1 d) GDPR). The Controller must be informed of the results on request.

(4) The Provider shall inform the Controller immediately if the measures undertaken by the Provider do not meet the Controller's requirements.

(5) Measures undertaken by the Provider may be adapted to technical and organizational developments in the course of the contractual relationship, but may not fall short of the agreed standards.

(6) The Provider must inform the Controller electronically in a documented form of any significant changes with appropriate lead time.

§ 10 Obligations of the Provider after completion of the engagement, Art. 28 para. 3, second sentence GDPR

(1) After completion of the contractual work, the Provider must delete or have destroyed all data, documents and processing or usage results in its possession and in the possession of its subcontractors to the extent they relate to the contractual relationship as follows: Unless mandatory provisions of law provide otherwise, all personal data on the contractor's systems must be deleted immediately or anonymized such that association with a specific individual is not possible. The data may be retained for a period of up to three months in backups that cannot be modified or deleted to ensure the integrity of the backups. The backup copies are to be stored encrypted in a separate data center and automatically deleted after a maximum of three months.

(2) The deletion or destruction must be confirmed electronically to the Controller including the relevant date.

§ 11 Liability

(1) Reference is made to Art. 82 GDPR.

(2) Provisions regarding liability agreed between the parties in the Primary Contract also apply to contract data processing.

§ 12 Miscellaneous

(1) Subsidiary agreements must be in writing or electronically in a documented form.

(2) Agreements regarding technical and organizational measures as well as control and inspection documents (including those related to subcontractors) shall be kept by both contracting parties for their respective period of validity and subsequently for three full calendar years.

(3) The Provider is required to inform the Controller immediately in the event that property of the Controller or personal data of the Controller to be processed by the Provider are placed at risk due to actions undertaken by third parties (such as attachment or seizure), by insolvency or composition proceedings or by any other events.

(4) The invalidity of any individual provisions of this agreement is without prejudice to the validity of the agreement as a whole.

This document is a sample of the Data Processing Agreement and should not be signed and returned to us! Please access the personalized copy we prepared for you from within your pretix organizer account in the "Data Protection"-section.

Annex A: List of commissioned sub-contractors

(1) netcup GmbH, Daimlerstr. 25, 76185 Karlsruhe, Germany
Commissioned with server and computer center services for data processing and storage
Computer center locations: Nuremberg (Germany)

(2) Hetzner Online GmbH, Industriestr. 25, 91710 Gunzenhausen, Germany
Commissioned with server and computer center services for data processing and storage
Computer center locations: Nuremberg (Germany), Falkenstein (Germany)

(3) rapidmail GmbH. Augustinerplatz 2, 79098 Freiburg i.Br., Germany
Commissioned with email delivery services
Computer center location: Germany

(4) Strato AG, Pascalstraße 10, 10587 Berlin, Germany
Commissioned with server and computer center services for data processing and storage
Computer center locations: Germany

Annex B: General technical and organizational measures in accordance with Art. 32 GDPR

(1) Pseudonymization and encryption of personal data (Art. 32 para. 1 a) GDPR)
   a) All data is encrypted at all times when sent via public or private data networks according to the latest standards.
   b) Data backups are stored in encrypted form on systems that are physically and logically separated from both the productive system and the storage location of the keys.
   c) The Provider is provided with functions in the software to anonymize or pseudonymize stored data so that association with a specific individual solely using data stored by us is not possible.
   d) Data in the productive systems themselves are not encrypted, since the keys must be stored on the same system to ensure constant retrievability and this would provide no real security advantage.

(2) Confidentiality (Art. 32 para. 1 b) GDPR)
   a) Physical access control
      aa) Selection of subcontractor data centers of that are adequately protected against unauthorized access using appropriate locking systems, access control systems, visitor control, alarm system, video surveillance and other suitable measures
   b) System access control
      aa) Access to systems only with personal user ID and password. There are regulations in place for choosing secure passwords.
      bb) Workstations and laptops only with encrypted hard disk and time-controlled screen lock with re-login in case of inactivity
      cc) Active and configured firewall on all systems in use
      dd) Maintenance access to production systems is only possible by means of personal, secret keys
      ee) Two-factor authentication for employee access to the productive system
      ff) Logging of all logins to productive systems
      gg) Active and up-to-date virus protection software on all Windows-based systems
   c) Access control
      aa) User roles/group concept
      bb) Regular checks of user permissions

cc) Maintenance access to productive systems is only assigned to a minimum number of technical employees

dd) Normal employee access to the software does not include access to customer data by default; this must be temporarily activated. As part of this process, logs are kept of each system access.

ee) Paper shredder for document destruction

ff) A set of regulations for disposal of data-carrying devices is specified.

d) Separation control

aa) Company data (accounting, personnel administration, etc.) separated from customer data

bb) Logical separation of development and productive systems

cc) Physical separation of data backups and productive systems

(3) Integrity (Art. 32 para. 1 b) GDPR)

a) Transfer control

aa) Encrypted transmission of personal data within internal and external networks

bb) Identification / Authentication

b) Input control

aa) As a fundamental principle, employees of the Provider may only access, enter, modify or delete this data in order to comply with instructions given by the Provider or to diagnose a technical error.

bb) Logging during input, modification and deletion of relevant data

cc) Our staff is trained on privacy issues in regular intervals.

(4) Availability, resilience, recoverability (Art. 32 para. 1 b), c) GDPR)

a) Availability control

aa) All servers are located in data centers in Germany

bb) The subcontractors' data centers have appropriate protective measures (redundant power supply, over-voltage protection, protection against fire and water intrusion, etc.)

cc) Redundant IT infrastructure; the functionality of the core system can be maintained despite failure of any server

dd) Permanent automatic monitoring of correct functionality

ee) Automatic data backups in accordance with SLA attached to the Primary Contract

ff) Testing of restore/recovery

gg) Firewalls in use

(5) Regular testing, assessing and evaluating (Art 32 para. 1 d) GDPR)

a) Order supervision

aa) On request, the Provider offers a written contract that defines the purpose of data processing and contains a right to issue instructions.

bb) Employees of the Provider know the purpose of the data processing. They are provided written instructions on how to handle personal data.

cc) A data processing agreement is concluded between the Provider and any sub-contractors as needed.