Contract for order processing within the meaning of Art. 28 General Data Protection Regulation (GDPR)

between

Name: _____

Address: _____

referred to as “**Controller**"

and

XQueue GmbH
Christian-Pless-Str. 11-13, 63069 Offenbach am Main
Germany

referred to as "**Processor**".

Preamble

The controller has commissioned the processor in the contract already concluded (hereinafter “main contract”) to provide the services mentioned there. Part of the execution of the contract is the processing of personal data. In particular, Art. 28 GDPR sets certain requirements for such order processing. To meet these requirements, the parties conclude the following order processing agreement (hereinafter the “Agreement”), the fulfillment of which will not be remunerated separately unless this is expressly agreed.

§ 1 Definitions

(1) According to Article 4 Paragraph 7 of the GDPR, the controller is the body that alone or jointly with other persons responsible decides on the purposes and means of processing personal data.

(2) Pursuant to Article 4 Paragraph 8 of the GDPR, a processor is a natural or legal person, authority, institution or other body that processes personal data on behalf of the controller.

(3) According to Article 4 Para. 1 GDPR, personal data is all information that relates to an identified or identifiable natural person (hereinafter “data subject”); A natural person is considered to be identifiable if he or she can be identified directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more special characteristics that express the physical, physiological, genetic, psychological, economic, cultural or social identity of that natural person.

(4) Particularly sensitive personal data are personal data in accordance with Art. 9 GDPR, which reveal the racial and ethnic origin, political opinions, religious or ideological beliefs or trade union membership of those affected, personal data in accordance with Art. 10 GDPR about criminal convictions and offenses or related security measures as well as genetic data in accordance with Art. 4 Para. 13 GDPR, biometric data in accordance with Art. 4

Para. 14 GDPR, health data in accordance with Art. 4 Para. 15 GDPR and data on the sex life or sexual orientation of a natural person.

(5) Pursuant to Article 4 Paragraph 2 of the GDPR, processing is any operation or series of operations carried out with or without the aid of automated procedures in connection with personal data, such as the collection, recording, organization, structuring, storage, adaptation or Modification, reading, querying, use, disclosure by transmission, distribution or any other form of provision, comparison or combination, restriction, deletion or destruction.

(6) According to Article 4 Para. 21 GDPR, the supervisory authority is an independent government body established by a member state in accordance with Article 51 GDPR.

§ 2 Subject of the contract

(1) The processor provides the services specified in the main contract for the controller. The processor receives access to personal data, which the processor processes on behalf of the controller exclusively on behalf of and in accordance with the instructions of the controller. The scope and purpose of data processing by the processor arise from the main contract and any associated service descriptions. The controller is responsible for assessing the admissibility of data processing.

(2) The parties conclude this agreement to specify the mutual data protection rights and obligations. In case of doubt, the provisions of this agreement take precedence over the provisions of the main contract.

(3) The provisions of this contract apply to all activities that are related to the main contract and in which the processor and its employees or those authorized by the processor come into contact with personal data that originate from the controller or were collected for the controller .

(4) The term of this contract depends on the term of the main contract, unless the following provisions result in additional obligations or termination rights.

§ 3 Right to give instructions

(1) The processor may only collect, process or use data within the scope of the main contract and in accordance with the instructions of the controller; This applies in particular to the transfer of personal data to a third country or to an international organization. If the processor is required to carry out further processing by the law of the European Union or the Member States to which it is subject, it will communicate these legal requirements to the controller before processing.

(2) The instructions of the controller are initially set out in this contract and can then be changed, supplemented or replaced by the controller in writing or in text form with individual instructions (individual instructions). The controller is entitled to issue appropriate instructions at any time. This includes instructions regarding the correction, deletion and blocking of data.

(3) Instructions that go beyond the service agreed in the main contract are treated as a request for a change in service.

(4) If the processor is of the opinion that an instruction from the controller violates data protection regulations, it must immediately inform the controller of this. The processor is entitled to suspend the implementation of the relevant instructions until they are confirmed or changed by the controller. The processor may refuse to carry out an obviously illegal instruction.

§ 4 Types of data processed, circle of those affected

The scope, type and purpose of data processing are limited to the use of address data to send newsletters by email.

The subject of the processing of personal data is customer data from the controller.

Those affected by the handling of their personal data within the scope of this order are customers, business contacts and interested parties of the controller.

The types of data processed and the categories of data subjects result from Section 12 of this contract.

§ 5 Protective measures of the processor

(1) The processor is obliged to observe the legal provisions on data protection and not to pass on the information obtained from the controller's area to third parties or to suspend their access. Documents and data must be secured against access by unauthorized persons, taking into account the state of the art.

(2) The processor will design the internal organization within his area of responsibility in such a way that it meets the special requirements of data protection. He has taken the technical and organizational measures listed in Appendix 1 to adequately protect the data controller's data in accordance with Art. 32 GDPR, which the controller recognizes as appropriate. The processor reserves the right to change the security measures taken, while ensuring that the contractually agreed level of protection is not fallen short of.

(3) Persons employed by the processor to process data are prohibited from collecting, processing or using personal data without authorization. The processor will oblige all persons entrusted with the processing and fulfillment of this contract (hereinafter "employees") accordingly (obligation of confidentiality, Art. 28 Para. 3 lit. b GDPR) and with due care Ensure compliance with this obligation. These obligations must be worded in such a way that they remain in effect even after the termination of this contract or the employment relationship between the employee and the processor.

§ 6 Information obligations of the processor

(1) In the event of disruptions, suspected data protection violations or violations of the processor's contractual obligations, suspected security-related incidents or other irregularities in the processing of personal data by the processor, persons employed by the processor as part of the order or by third parties, the processor will immediately notify the controller , at the latest within 24 hours of the incident or irregularity. The same applies to audits of the processor by the data protection supervisory authority. The personal data breach notification shall contain at least the following information:

(a) a description of the nature of the personal data breach, indicating, where possible, the categories and number of individuals affected, the categories affected and the number of personal data sets affected;

b) a description of the measures taken or proposed by the processor to remedy the breach and, where appropriate, measures to mitigate its possible adverse effects;

c) a description of the likely consequences of the personal data breach.

(2) The processor immediately takes the necessary measures to secure the data and to reduce possible adverse consequences for those affected, informs the controller about this and requests further instructions.

(3) The processor is also obliged to provide the controller with information at any time to the extent that their data is affected by a violation in accordance with paragraph 1.

(4) If the controller's data is at risk from the processor through seizure or confiscation, through insolvency or composition proceedings or through other events or measures by third parties, the processor must inform the controller immediately, unless this has been reported to him by judicial or official authorities Order is prohibited. In this context, the processor will immediately inform all responsible authorities that decision-making authority over the data lies exclusively with the controller.

(5) The processor must immediately inform the controller of any significant changes to the security measures in accordance with Section 5 Paragraph 2.

(6) The processor must participate to an appropriate extent in the creation of the list of procedures by the controller. He must provide the controller with the required information in an appropriate manner.

§ 7 Control rights of the controller

(1) The controller can verify the technical

and organizational measures of the processor before commencing data processing and then regularly on a quarterly basis. For this he can z. B. Obtain information from the processor, have existing reports from experts, certifications or internal audits presented to you, or personally check the technical and organizational measures of the processor after timely coordination during normal business hours or have them checked by a knowledgeable third party, provided this is not done in one There is a competitive relationship with the processor. The controller will only carry out controls to the extent necessary and will not disproportionately disrupt the processor's operations.

(2) The processor undertakes to provide the controller, upon his oral or written request, within a reasonable period of time with all information and evidence that is necessary to carry out an inspection of the technical and organizational measures of the processor.

(3) The controller documents the control result and informs the processor. In the event of errors or irregularities that the controller discovers, particularly when checking the results of the order, he must inform the processor immediately. If the inspection reveals circumstances that require changes to the ordered procedural sequence to be avoided in the future, the controller will immediately inform the processor of the necessary procedural changes.

(4) At the request of the controller, the processor will provide the controller with a comprehensive and up-to-date data protection and security concept for order processing as well as persons authorized to access it.

(5) Upon request, the processor will provide the responsible party with proof of the employee's obligations in accordance with Section 5 Paragraph 3.

(6) The controller has appointed a data protection officer. The data protection officer of the processor is:

§ 8 Use of service providers

(1) The contractually agreed services are carried out using the service providers listed in Appendix 2 (hereinafter “sub-processors”).

The processor only commissions further sub-processors with the written consent of the controller.

(2) The processor is obliged to carefully select sub-processors based on their suitability and reliability. When engaging sub-processors, the processor must oblige them to comply with the provisions of this agreement. If sub-processors in a third country are to be involved, the processor must ensure that an appropriate level of data protection is guaranteed by the respective sub-processor (e.g. by concluding an agreement based on the EU standard data protection clauses with additional guarantees that the level of data protection in the third country corresponds to corresponds to the EU). Upon request, the processor will provide the controller with proof of the conclusion of the aforementioned agreements with its sub-processors.

(3) A subcontract relationship within the meaning of these provisions does not exist if the processor commissions third parties to provide services that are purely ancillary services. These include, for example: B. Postal, transport and shipping services, cleaning services, telecommunications services without any specific connection to services that the processor provides for the controller and security services. Maintenance and testing services constitute subcontracting relationships requiring approval, insofar as they are provided for IT systems that are also used in connection with the provision of services for the controller.

§ 9 Inquiries and rights of those affected,

(1) The processor supports the controller

with suitable technical and organizational measures in fulfilling his obligations in accordance with Articles 12-22 and 32 to 36 GDPR.

(2) If a data subject asserts rights, such as access to information, correction or deletion of his or her data, directly against the processor, the processor does not react independently, but rather refers the data subject immediately to the controller and waits for his instructions.

§ 10 Termination of the main contract

(1) After termination of the main contract, the processor will return all documents, data and data carriers provided to him to the controller or - at the request of the controller, unless there is an obligation to store the personal data under Union law or the law of the Federal Republic of Germany - delete them. This also applies to any data backups at the processor. The processor must provide documented evidence of proper deletion.

(2) The controller has the right to appropriately control the complete and contractual return or deletion of the data to the processor.

(3) The processor is obliged to treat the data he becomes aware of in connection with the main contract confidentially, even after the end of the main contract. This agreement remains valid beyond the end of the main contract for as long as the processor has personal data that was provided to it by the controller or that it collected for the processor.

§ 11 Final provisions

(1) The processor cannot invoke a right of retention in accordance with Section 273 of the Civil Code or other applicable laws with regard to the data to be processed under this agreement and the corresponding data carriers.

(2) Changes and additions to this agreement must be made in writing. This also applies to the waiver of this formal requirement. The priority of individual contractual agreements remains unaffected by this.

(3) If individual provisions of this agreement are or become wholly or partially invalid or unenforceable, this will not affect the validity of the remaining provisions.

(4) This agreement is subject to German law.

§ 12 Data

The following types of personal data are processed under this agreement.

Types of data:

In addition, the following **Categories of people** are affected:

Attachment 1: Data security concept / Technical & Organizational Measures (TOM)

Appendix 2: Subcontractor

Controller

Name:
_____

Position:
_____

Date:
_____

Signature:
_____

_____

Position:
_____

Date:
_____

Signature:
_____

Processor

Name:

Attachment 1

Data security concept

Data protection control measures in accordance with Art. 32 GDPR

As of August 8, 2023

If you have any questions about XQueue data protection and information security, please contact

heyData GmbH
Schützenstr. 5
10117 Berlin
support@heydata.eu

1 Introduction

This appendix summarizes the technical and organizational measures taken by the processor within the meaning of Art. 32 Para. 1 GDPR. These are measures with which the processor protects personal data. The purpose of the document is to support the processor in fulfilling its accountability obligations under Article 5 (2) GDPR.

2. Confidentiality (Art. 32 para. 1 lit. b GDPR)

2.1. access control

The following implemented measures prevent unauthorized persons from having access to the data processing systems:

- Securing building shafts
- Chip card/transponder locking system
- Video surveillance of entrances
- Logging of visitors (e.g. visitor book)
- Key regulation / key book
- Obligation to carry employee and guest ID cards
- Visitors only when accompanied by employees
- Careful selection of cleaning staff

2.2Access control

The following implemented measures prevent unauthorized persons from having access to the data processing systems:

- Authentication with user and password
- Use of anti-virus software
- Use of firewalls
- Use of VPN technology for remote access
- Blocking external interfaces (e.g. USB ports)
- Encryption of data carriers
- Automatic desktop lock
- User permissions management
- Creating user profiles
- Central password rules
- Logging of visitors (e.g. visitor book)
- Key regulation / key book
- General company policy on privacy or security
- Company policy for strong passwords
- Company Deletion/Destruction Policy
- Company policy on mobile device use
- General instructions to manually lock the desktop when leaving work

2.3. Access control

The following implemented measures ensure that unauthorized persons do not have access to personal data:

- Use of document shredders (with cross cut function)
- Destruction of data carriers at least in accordance with DIN 32757
- Physical deletion of data carriers before they can be reused
- Logging of access to applications (especially when entering, changing and deleting data)
- Use of an authorization concept
- The number of administrators is kept as small as possible
- Secure storage of data media
- Management of user rights by system administrators

2.4. Separation control

The following measures ensure that personal data collected for different purposes are processed separately:

- Separation of productive and test systems
- Logical controller separation (software side)

2.5. Pseudonymization (Art. 32 Para. 1 lit. a GDPR; Art. 25 Para. 1 GDPR)

Pseudonymization is the processing of personal data in such a way that it can no longer be attributed to a specific data subject without the use of additional information, provided that this additional information is kept separately and is subject to appropriate technical and organizational measures. For this purpose, the data is linked to unique pseudonyms before further processing and other personal data is removed. The following measures have been implemented:

- Sharing of data in anonymized or pseudonymized form

3. Integrity (Article 32 Paragraph 1 Letter b GDPR)

3.1. Transfer control

It is ensured that personal data cannot be read, copied, changed or removed without authorization when transferred or stored on data carriers and that it can be checked which people or bodies have received personal data. The following measures have been implemented to ensure this:

- WiFi encryption (WPA2 with strong password)
- Logging of accesses and retrievals
- Providing data over encrypted connections such as SFTP or HTTPS
- Use of signature procedures
- Sharing of data in anonymized or pseudonymized form
- Ban on uploading business data to non-company servers

3.2. Input control

The following measures ensure that it can be checked who processed personal data in data processing systems and at what time:

- Logging the entry, modification and deletion of data
- Manual or automatic control of protocols
- Traceability of entering, changing and deleting data through individual user names (not user groups)

4. Availability and resilience (Art. 32 para. 1 lit. b GDPR)

The following measures ensure that personal data is protected against accidental destruction or loss and is always available to the controller:

- Fire and smoke alarm systems
- Devices for monitoring temperature and humidity in server rooms
- Air conditioning in server rooms
- Protective socket strips in server rooms
- Uninterruptible power supply (UPS)
- Video surveillance in server rooms
- Alarm notification in the event of unauthorized access to server rooms
- Regular backups
- No sanitary facilities in or above the server room
- Separation of operating systems and data

5. Procedure for regular review, assessment and evaluation (Art. 32 Para. 1 lit. d GDPR; Art. 25 Para. 1 GDPR)

5.1. Data protection management

The following measures are intended to ensure that an organization that meets the basic data protection requirements is in place:

- Use of the heyData platform for data protection management
- Appointment of the data protection officer heyData
- Commitment of employees to data secrecy
- Regular training for employees in data

protection
- Maintaining an overview of processing activities (Art. 30 GDPR)
- Carrying out data protection impact assessments, if necessary (Art. 35 GDPR)

5.2. Incident response management

The following measures are intended to ensure that reporting processes are triggered in the event of data protection violations:

- Reporting process for data protection violations in accordance with Article 4 Paragraph 12 GDPR to the supervisory authorities (Article 33 GDPR)
- Reporting process for data protection violations in accordance with Art. 4 Paragraph 12 GDPR to those affected (Art. 34 GDPR)
- Involvement of the data protection officer in security incidents and data breaches
- Use of anti-virus software
- Use of firewalls

5.3. Data protection-friendly default settings (Art. 25 Para. 2 GDPR)

The following implemented measures take into account the requirements of the "Privacy by design" and "Privacy by default" principles:

- Training employees in "Privacy by design" and "Privacy by default"
- No more personal data is collected than is necessary for the respective purpose.

5.4. Order control

The following measures ensure that personal data can only be processed in accordance with the instructions:

- Written instructions to the contractor or instructions in text form (e.g. through an order processing agreement)
- Ensuring the destruction of data after completion of the order, e.g. by requesting appropriate confirmations
- Confirmation from contractors that they commit their own employees to data secrecy (typically in the order processing contract)
- Careful selection of contractors (especially with regard to data security)

Appendix 2

Current sub-processors

Surname	**Function**	**Server location**
Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Dublin, D04e5w5, Ireland	serverless computing environments, Platform-as-a-Service and Infrastructure-as-a-Service	EU
Hetzner Online GmbH Nuremberg data center	• Data center/cloud • Hosting Services	Industriestr. 25 91710 Gunzenhausen, Germany