Qdrant Solutions GmbH

Cloud Data Processing Agreement

THIS CLOUD DATA PROCESSING AGREEMENT ("**CDPA**") IS ENTERED INTO BETWEEN QDRANT SOLUTIONS GMBH, CHAUSEESTR. 86, 10115 BERLIN, GERMANY ("**QDRANT**") AS A PROCESSOR AND THE CUSTOMER MENTIONED AS SUCH IN THE ORDER (**"CUSTOMER"**) AS THE CONTROLLER CONCERNING THE PROCESSING OF PERSONAL DATA IN THE CONTEXT OF THE PERFORMANCE OF THE AGREEMENT CONCLUDED BETWEEN QDRANT AND THE CUSTOMER PURSUANT TO THE QDRANT CLOUD TERMS AND CONDITIONS (**"CLOUD SERVICE AGREEMENT"**).

QDRANT AND THE CUSTOMER MAY EACH HEREINAFTER BE REFERRED TO INDIVIDUALLY AS A "**PARTY**" OR COLLECTIVELY AS THE "**PARTIES**".

THIS CDPA FORMS AN INTEGRAL PART OF THE CLOUD SERVICE AGREEMENT BETWEEN THE PARTIES. THE TERMS AND CONDITIONS OF THIS CDPA ARE LEGALLY BINDING FOR THE PARTIES UPON CONCLUSION OF THECLOUD SERVICE AGREEMENT.

THE TERMS AND CONDITIONS OF THIS CDPA SHALL APPLY *MUTATIS MUTANDIS* IF THE CUSTOMER PROCESSES PERSONAL DATA FOR CLIENTS OF THE CUSTOMER AS A PROCESSOR AND USES QDRANT AS A SUB-PROCESSOR.

IN THE EVENT OF ANY CONFLICT BETWEEN THE PROVISIONS OF THIS CDPA AND THE CLOUD SERVICE AGREEMENT, THIS CDPA SHALL PREVAIL.

§ 1 General Responsibilities of the Parties

(1) **Controller and Processor.** The provision of the services agreed in the Cloud Service Agreement (the "**Services**") by Qdrant requires the processing of data provided or made available to Qdrant by the Customer in the course of the cooperation. If and to the extent that such data consists of or contains personal data within the meaning of the applicable data protection laws ("**Data Protection Laws**"), in particular the EU General Data Protection Regulation ("**GDPR**"), the provisions of this CDPA shall apply to their processing by Qdrant. The Parties acknowledge and agree that the Customer is the sole controller in relation to such personal data as between the Parties and that Qdrant does not acquire any rights of its own in such personal data but may and will process them solely in its capacity as a processor for the Customer.

(2) **Responsibility of the Customer.** Within the scope of the cooperation, the Customer will transmit, make available or otherwise make accessible to the Customer personal data. The Customer agrees and understands that Qdrant will not monitor Customer personal data or Customer's use of any such personal data, unless the Customer submits an explicit written request to Qdrant to access its personal data. In any other case, only the Customer knows which data comprise the personal data. As between the Parties, it is, therefore, the sole responsibility and liability of the Customer to ensure that personal data is collected and transmitted, provided, or otherwise made accessible to Qdrant in compliance with applicable Data Protection Laws and, in particular, (a) to always observe the principles relating to processing of personal data including,

without limitation, the principles of purpose limitation and data minimization; (b) to have a legal basis for its processing; and (c) to properly inform data subjects of the collection and processing of their personal data, including their transfer to Qdrant.

(3) **Responsibility of Qdrant.** As a processor, Qdrant will process personal data of the Customer on behalf of the Customer exclusively in accordance with the provisions of this CDPA and the documented instructions of the Customer. If Qdrant is required by the law of the EU or an EU Member State to which Qdrant is subject to process personal data for other purposes, Qdrant shall inform the Customer before such processing takes place, unless the law requiring such processing prohibits Qdrant from informing the Customer because of an important public interest. Qdrant shall ensure and regularly check that in its area of responsibility the processing of the Customer's personal data is carried out in accordance with the provisions of this CDPA, with the applicable Data Protection Laws and in particular with the GDPR.

§ 2 Processing Details

(1) **Specification of Processing Details.** The details of the processing are specified in the following paragraphs. However, to the extent necessary for a particular Service, the Parties shall further specify the details of the processing in the Cloud Service Agreement or in a supplemental agreement to such Cloud Service Agreement. In consideration of the Customer's responsibilities as a controller, also the responsibility to request such further specification remains with the Customer. The foregoing shall apply without restriction if the processing under this CDPA involves special categories of personal data.

(2) **Nature, Purpose, and Object of the Processing.** Qdrant processes the personal data of the Customer for the provision of the Services as further described in the Cloud Service Agreement.

(3) **Duration of Processing.** Qdrant will generally process the personal data of the Customer for the duration of the Services according to the Cloud Service Agreement, unless otherwise agreed in writing.

(4) **Categories of Data Subjects.** The Customer may transfer, provide, or make available to Qdrant personal data, the scope of which is determined and controlled by the Customer, and such personal data may relate to the following categories of data subjects:

- the Customer staff,
- clients, contractors, business partners of the Customer or their respective employees,
- other persons whose personal data are transferred, provided or made accessible to Qdrant in the context of the cooperation.

(5) **Types of Personal Data.** Personal data of the Customer may include the following types of personal data:

- Master data,
- Communication data (for example, telephone number, e-mail),
- Employee data,
- Applicant Data,
- Contract data,
- Operating and machine data,
- any other data transmitted, made available or accessible to Qdrant in the context of the collaboration.

§ 3 Place of Processing; Transfer to Third Countries

(1) **Place of Processing.** Personal data of the Customer will be processed by Qdrant only on its own or its authorized sub-contractors' premises. The processing activities will therefore be carried out, subject to paragraph 2, (a) in the member states of the European Union, (b) in another state party to the Agreement on the European Economic Area or (c) in a third country for which an adequacy decision of the European Commission within the meaning of Art. 45 of the GDPR is available. In the cases of lit. (c), Qdrant will obtain appropriate instructions from the Customer before the transfer to such third country.

(2) **Transfer to Other Third Countries.** Processing of personal data of the Customer outside the EU/EEA is otherwise only permitted on a corresponding instruction of the Customer and only if the requirements of Art. 44 et seq. of the GDPR are fulfilled. Without prejudice to the foregoing, and in addition to any further obligations under applicable Data Protection Laws, Qdrant may enter into an agreement on the basis of the Standard Contractual Clauses issued by the European Commission on 4 June 2021 when transferring personal data to a recipient with a processing location outside to EU/EEA.

(3) **Customers Located in Third Countries.** Where the Customer itself is located outside the EU/EEA, the Parties hereby enter into an agreement on the basis of the Standard Contractual Clauses issued by the European Commission on 4 June 2021 as annexed to this CDPA as **Annex 1** to ensure compliance when transferring personal data to the Customer's location.

§ 4 The Customer's Instructions

(1) **General Instructions.** The Parties agree and the Customer understands that the provisions of this CDPA shall include the general instructions of the Customer valid at the time of the entry into force of this CDPA regarding the processing of personal data of the Customer in the context of the provision of the Services.

(2) **Special Instructions.** In accordance with Data Protection Laws, the Customer may at any time issue individual instructions regarding the processing of the Customer's personal data. Unless such individual instructions are required to comply with applicable Data Protection Laws, individual instructions which deviate from the provisions of this CDPA, or which impose additional requirements on Qdrant, require Qdrant's prior consent and shall be made in accordance with the change procedure agreed in the Cloud Service Agreement (if any).

(3) **Compliance with Data Protection Laws.** In the relationship between the Parties, the Customer shall ensure that any instruction regarding the processing of personal data of the Customer complies with Data Protection Laws and that the processing of personal data of the Customer in accordance with its instructions does not lead to Qdrant violating Data Protection Laws and in particular the GDPR. If Qdrant is of the opinion that a particular instruction violates applicable Data Protection Laws, it shall inform the Customer thereof without undue delay. Furthermore, Qdrant is entitled to suspend the execution of the instruction until the Customer confirms the instruction.

(4) **Text Form.** Instructions from the Customer are always given in text form by the authorized persons of the Customer. Verbal instructions are to be confirmed by the Customer in writing or in text form. The Customer shall document all individual instructions issued within the scope of the cooperation and present them to Qdrant upon request. The Customer will use the

following communication channels for issuing instructions, the accessibility of which shall be ensured by Qdrant at all times during the term of this CDPA: **privacy@qdrant.com**
Qdrant shall inform the Customer in writing of any change in the aforementioned communication channels.

§ 5 Qdrant's Representations

(1) **Employees.** Employees of Qdrant: (a) who have access to personal data of the Customer have committed themselves to confidentiality or are subject to a corresponding legal duty of confidentiality; (b) will only process personal data of the Customer in accordance with the instructions of the Customer, unless otherwise required to do so in accordance with applicable Data Protection Laws; and (c) will be trained from time to time with regard to Qdrant's obligations under this CDPA, under Data Protection Laws and in particular under the GDPR.

(2) **Copies; Backups.** Qdrant may not make copies or duplicates of the Customer's personal data without the Customer's prior written consent. However, copies are exempt from this insofar as they are necessary to ensure proper data processing and the proper provision of the Services (including data backups), as well as copies that are necessary to comply with legal retention obligations.

(3) **Data Protection Officer.** Qdrant shall appoint a data protection officer if and to the extent the legal requirements for appointment are met. The contact details of such data protection officer will be provided to the Customer upon request.

§ 6 Technical and Organizational Measures

(1) **Implementation and Maintenance.** Qdrant shall implement the technical and organizational measures listed in **Annex 2** before the start of processing and maintain them during the term of this CDPA. These are data security measures to ensure a risk-adequate level of protection with regard to the confidentiality, integrity, availability, and resilience of the systems. The state of the art, the implementation costs and the nature, scope, and purposes of the processing as well as the varying likelihood and severity of the risk to the rights and freedoms of natural persons within the meaning of Article 32 (1) of the GDPR shall be taken into account.

(2) **Alternative Measures.** As the technical and organizational measures are subject to technical progress and technological development, Qdrant is permitted to take alternative and appropriate measures to keep the technical and organizational measures up to date, provided that the security level of the measures specified in **Annex 2** is not impaired. Qdrant shall document such changes and provide the Customer with a copy of the current list of technical and organizational measures upon request. Significant changes to the measures require the prior written consent of The Customer.

§ 7 Subcontracting

(1) **General Authorization; Pre-Approved Sub-Processors.** The Customer grants Qdrant a general authorization to appoint sub-processors, subject to the provisions of this § 7. The sub-processors that Qdrant has appointed at the effective date of this CDPA are listed in **Annex 3**. The Customer explicitly grants permission to the involvement of the sub-processors listed in **Annex 3** in the provision of the Services.

(2) **Qdrant's Liability.** Qdrant shall impose privacy, confidentiality and data security obligations on any sub-processor that are at least as stringent as those set forth in the present

CDPA. Where a sub-processor fails to fulfil its data protection obligations with respect to the processing of personal data, Qdrant shall remain fully liable to the Customer for the performance of that sub-processor's obligations.

(3) **Appointment of Sub-Processors.** Qdrant shall give the Customer prior written notice of the appointment of any new sub-processor. If, within thirty (30) days of receipt of that notice, the Customer notifies Qdrant in writing of any reasonable objection to the proposed appointment, the Parties shall negotiate in good faith a mutually acceptable alternative. If no such alternative is agreed within two (2) months of the objection, the Customer will have the right to terminate the Cloud Service Agreement to the extent it relates to Services which require use of the proposed sub-processor.

(4) **No Subcontracted Processing.** The Parties agree that auxiliary service providers of the Customer are not sub-processors within the meaning of the Data Protection Laws; this includes, in particular, transport services of postal or courier services, money transport services, telecommunication services, security services and cleaning services. However, the Customer will enter into customary confidentiality agreements with such service providers.

§ 8 Support for the Customer

(1) **Investigations by a Supervisory Authority.** Upon the Customer's written request, Qdrant shall assist the Customer in the event of an investigation by or inquiry from a regulatory or similar authority if and to the extent such investigation or inquiry relates to the Services. Qdrant will take all necessary steps requested by the Customer to assist the Customer in fulfilling its obligations in connection with any such investigation or inquiry. If an investigation or inquiry by a regulatory authority, including a supervisory or similar authority, involves Qdrant itself, Qdrant shall promptly notify the Customer thereof, to the extent permitted, and cooperate with such investigation or inquiry.

(2) **Data Breaches.** Qdrant shall inform the Customer without undue delay if it detects a breach of the security measures agreed under this CDPA ("**Security Incident**"), in particular if such Security Incident has led or could lead to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to personal data of the Customer that Qdrant processes on behalf of the Customer under this CDPA. If, as a result of a Security Incident, the Customer has a legal obligation to provide information due to a risk to the rights and freedoms of natural persons (in particular, but not limited to, the information obligations under Articles 33, 34 of the GDPR), Qdrant will reasonably assist the Customer in fulfilling these information obligations upon request. Inasmuch as Qdrant is not at fault for the Security Incident, support shall be provided against a remuneration to be calculated in accordance with the Cloud Service Agreement.

(3) **Data Protection Impact Assessment.** Qdrant shall reasonably cooperate and assist the Customer, taking into account the nature of the processing and the information available to Qdrant, in any data protection impact assessments required with respect to the data processing for the Services under Art. 35 of the GDPR and in any regulatory consultations that the Customer considers itself obliged to undertake with respect to such data protection impact assessment under Art. 36 of the GDPR. Such assistance shall be made subject to a remuneration to be calculated in accordance with the Cloud Service Agreement.

(4) **Data Subject Requests.** Qdrant shall notify the Customer of any complaint, communication or request received directly from a data subject concerning his or her personal

data, without responding to such request, unless otherwise authorized by the Customer. Qdrant shall reasonably assist the Customer with any complaints, communications or requests it receives from a data subject, subject to a remuneration to be calculated in accordance with the Cloud Service Agreement.

§ 9 Return or Deletion of Personal Data

(1) **Return or Deletion.** Upon the Customer's written request during the term of the Cloud Service Agreement or upon termination or expiration of the Cloud Service Agreement, Qdrant shall either return or destroy the Customer's personal data as instructed by the Customer. If Data Protection Laws to which Qdrant is subject prevent Qdrant from returning or destroying all or part of the Customer's personal data, Qdrant warrants that it will ensure the confidentiality of such the Customer's personal data and will no longer actively process such the Customer's personal data, and that it will ensure the return or destruction of such the Customer personal data upon the Customer's request when the legal obligation to return or destroy the personal data is no longer in effect.

(2) **Deletion Reports.** Qdrant shall prepare a report on the deletion or destruction of the Customer's personal data, which shall be submitted to the Customer upon request.

§ 10 Audit Rights of the Customer

(1) **On-site Inspections.** The Customer is entitled to enter Qdrant's and its authorized sub-processors' business premises, in which personal data of the Customer are processed on behalf of the Customer, during normal business hours at its own expense, without unreasonable disruption of operations and while maintaining the business secrets of Qdrant and its authorized sub-processors, in order to verify compliance with this CDPA, applicable Data Protection Laws and in particular the GDPR. The Customer will inform Qdrant in due time (generally at least two weeks in advance) about all circumstances related to the performance of an audit.

(2) **Number of Audits.** As a rule, the Customer may conduct one audit per calendar year. This does not affect the right of the Customer to conduct further audits in case of special incidents.

(3) **Involvement of External Auditors.** If the Customer commissions a third party to carry out the audit, the Customer must obligate the third party in writing in the same way as the Customer is obligated to Qdrant on the basis of this CDPA. In addition, the Customer must oblige the third party to secrecy and confidentiality, unless the third party is subject to a professional obligation of secrecy. At Qdrant's request, the Customer shall provide Qdrant without delay with the confidentiality agreements concluded with the third party. The Customer must not appoint a competitor of Qdrant to carry out the inspection.

(4) **Audit Reports.** Without prejudice to the Customer's right to carry out on-site inspections, Qdrant may demonstrate compliance with this CDPA by complying with an approved code of conduct pursuant to Art. 40 of the GDPR, certification according to a recognized certification mechanism pursuant to Art. 42 of the GDPR and by submitting suitable, up-to-date certificates, reports or report extracts from independent bodies (e.g. certified accountant, auditor, data protection officer, IT security department, data protection auditors or quality auditors) or by a suitable certificate after an IT security or data protection audit - e.g. according to DIN ISO 27001 - ("**Audit Report**"), if and to the extent that the Customer can convince itself in a suitable manner of Qdrant's compliance with this CDPA by means of the Audit Report.

(5) **Remuneration.** If and inasmuch as Qdrant did not force an audit by fault, support during such audit shall be provided only against a remuneration to be calculated in accordance with the Cloud Service Agreement.

§ 11 Miscellaneous

(1) **Governing Law; Place of Jurisdiction.** This CDPA shall be governed by the same law as the Cloud Service Agreement, unless the Cloud Service Agreement is governed by the law of a third country outside the EU/EEA, in which case the law of the Federal Republic of Germany shall apply to this CDPA. Any disputes arising out of or in connection with this CDPA shall be subject to the exclusive jurisdiction of the court agreed between the Parties in the Cloud Service Agreement, unless the Parties have agreed in the Cloud Service Agreement that a court in a third country outside the EU/EEA shall have jurisdiction, in which case the competent courts in Berlin, Germany shall have exclusive jurisdiction over any disputes arising out of or in connection with this CDPA.

(2) **Written Form Requirement.** Amendments and supplements to this CDPA must be made in writing. This shall also apply to the written form requirement. If they do not comply with this form, they shall be invalid.

(3) **Severability Clause.** Should any provision of this CDPA be or become invalid, this shall not affect the validity of the remaining provisions. In such a case, the Parties shall be obliged to cooperate in the creation of regulations by means of which a result is achieved which comes as close as possible in legal terms to the invalid provision.

Annex 1
Standard Contractual Clauses

SECTION I

Clause 1

Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) for the transfer of personal data to a third country.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter 'entity/ies') transferring the personal data, as listed in Annex I.A (hereinafter each 'data exporter'), and

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A (hereinafter each 'data importer')

have agreed to these standard contractual clauses (hereinafter: 'Clauses').

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2

Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3

Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii) Clause 8.1 (b) and Clause 8.3(b)

(iii) n.a.;

(iv) n.a.;

(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e);

(viii) Clause 18.

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4

Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6

Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Clause 7

Docking clause

Clause 7 shall be omitted.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organizational measures, to satisfy its obligations under these Clauses.

8.1 Instructions

(a) The data exporter shall process the personal data only on documented instructions from the data importer acting as its controller.

(b) The data exporter shall immediately inform the data importer if it is unable to follow those instructions, including if such instructions infringe Regulation (EU) 2016/679 or other Union or Member State data protection law.

(c) The data importer shall refrain from any action that would prevent the data exporter from fulfilling its obligations under Regulation (EU) 2016/679, including in the context of sub-processing or as regards cooperation with competent supervisory authorities.

(d) After the end of the provision of the processing services, the data exporter shall, at the choice of the data importer, delete all personal data processed on behalf of the data importer and certify to the data importer that it has done so, or return to the data importer all personal data processed on its behalf and delete existing copies.

8.2 Security of processing

(a) The Parties shall implement appropriate technical and organizational measures to ensure the security of the data, including during transmission, and protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access (hereinafter 'personal data breach'). In assessing the appropriate level of security, they shall take due account of the state of the art, the costs of implementation, the nature of the personal data, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects, and in particular consider having recourse to encryption or pseudonymization, including during transmission, where the purpose of processing can be fulfilled in that manner.

(b) The data exporter shall assist the data importer in ensuring appropriate security of the data in accordance with paragraph (a). In case of a personal data breach concerning the personal data processed by the data exporter under these Clauses, the data exporter shall notify the data importer without undue delay after becoming aware of it and assist the data importer in addressing the breach.

(c) The data exporter shall ensure that persons authorized to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

8.3 Documentation and compliance

(a) The Parties shall be able to demonstrate compliance with these Clauses.

(b) The data exporter shall make available to the data importer all information necessary to demonstrate compliance with its obligations under these Clauses and allow for and contribute to audits.

Clause 9

Use of sub-processors

n.a.

Clause 10

Data subject rights

The Parties shall assist each other in responding to enquiries and requests made by data subjects under the local law applicable to the data importer or, for data processing by the data exporter in the EU, under Regulation (EU) 2016/679.

Clause 11

Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorized to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

Clause 12

Liability

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.
(b) Each Party shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages that the Party causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter under Regulation (EU) 2016/679.
(c) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.
(d) The Parties agree that if one Party is held liable under paragraph (c), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.
(e) The data importer may not invoke the conduct of a processor or sub-processor to avoid its own liability.

Clause 13

Supervision

n.a.

SECTION III –
LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14
Local laws and practices affecting compliance with the Clauses

(where the EU processor combines the personal data received from the third country-controller with personal data collected by the processor in the EU)

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorizing access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorizing access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards;

(iii) any relevant contractual, technical or organizational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organizational

measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

Obligations of the data importer in case of access by public authorities

(where the EU processor combines the personal data received from the third country-controller with personal data collected by the processor in the EU)

15.1 Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimization

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and

to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16
Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority [for Module Three: and the controller] of such non- compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data collected by the data exporter in the EU that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall immediately be deleted in its entirety, including any copy thereof. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to

ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17

Governing law

These Clauses shall be governed by the law of a country allowing for third-party beneficiary rights. The Parties agree that this shall be the law of Germany.

Clause 18

Choice of forum and jurisdiction

Any dispute arising from these Clauses shall be resolved by the courts of Germany.

APPENDIX

EXPLANATORY NOTE:

It must be possible to clearly distinguish the information applicable to each transfer or category of transfers and, in this regard, to determine the respective role(s) of the Parties as data exporter(s) and/or data importer(s). This does not necessarily require completing and signing separate appendices for each transfer/category of transfers and/or contractual relationship, where this transparency can be achieved through one appendix. However, where necessary to ensure sufficient clarity, separate appendices should be used.

ANNEX I

A. LIST OF PARTIES

Data exporter(s): [Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union]

Name: Qdrant Solutions GmbH

Address: Chausseestr. 86, 10115 Berlin, Germany

Contact person's name, position and contact details: André Zayarni, Managing Director, privacy@qdrant.com

Activities relevant to the data transferred under these Clauses: Provision of the Services described in the Cloud Service Agreement, including the storage of Customer personal data on a cloud infrastructure

Signature and date: signed electronically upon conclusion of the Cloud Service Agreement

Role (controller/processor): processor

Data importer(s): [Identity and contact details of the data importer(s), including any contact person with responsibility for data protection]

Name: as stated in the Cloud Service Agreement

Address: as stated in the Cloud Service Agreement

Contact person's name, position and contact details: as stated in the Cloud Service Agreement

Activities relevant to the data transferred under these Clauses: uploading of Customer personal data to the Qdrant cloud infrastructure for the purpose of using the Services provided under the Cloud Service Agreement

Signature and date: signed electronically upon conclusion of the Cloud Service Agreement

Role (controller/processor): controller or processor

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

As set forth in the CDPA

Categories of personal data transferred

As set forth in the CDPA

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

As set forth in the CDPA

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).

Data may be transferred continuously throughout the term of the CDPA

Nature of the processing

As set forth in the CDPA

Purpose(s) of the data transfer and further processing

As set forth in the CDPA

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

For the duration of the Cloud Service Agreement

For transfers to (sub-)processors, also specify subject matter, nature and duration of the processing

n.a.

Annex 2

Technical and Organizational Measures

1. Technical & Organizational Security Measures	Specify the Technical & Organizational Measures (TOMs) ensuring protection of Personal Data and, if applicable, adherence by the Provider to an approved code of conduct or to an approved certification mechanism	
1.1 Confidentiality		
Physical access control Measures to prevent unauthorized access to data processing facilities	x magnetic or chip cards x keys x electronic door openers x facility security services x entrance security staff	☐ personnel and visitor badges x visitor protocols x alarm systems x video/CCTV systems ☐ other:
Electronic access control Measures to prevent unauthorized use of the data processing and data storage systems	x (secure) passwords x automatic blocking/locking mechanisms x secure authentication process	x multi-factor authentication x intrusion detection and prevention system ☐ other:
Internal access control Measures to prevent unauthorized reading, copying, changes or deletions of data within the system	x rights authorization concept x documented assignment of rights and roles x need-based rights of access x restriction of writing and modification permissions	x logging of system access events x mobile device policy x clean desk policy ☐ other:
Isolation control Measures to ensure isolated processing of data, which are collected for differing purposes	x multi-client capability x separation in organizational / departmental boundaries x separation of testing and production environment	x physical separation of systems, databases and data carriers x sandboxing ☐ other:
1.2 Integrity		
Data transfer control Measures to prevent unauthorized reading, copying, changes or deletions of data during electronic transfer or transport	x encryption in rest x encryption in transit ☐ encryption of data carriers and storage media ☐ mobile device management	x virtual private networks (VPN) x electronic signatures ☐ other:
Data entry control Measures to verify whether and by whom personal data are entered into a data processing system, changed or deleted	x logging of access and modifications x verification of data sources (authenticity) x document management ☐ other:	
1.3 Availability and resilience		
Measures to prevent accidental or willful	x backup strategy ☐ uninterruptible power supply (UPS)	x repair strategies and alternative processes x fire and smoke detectors

destruction or loss and ensure rapid recovery	x virus protection x firewall x spam filter x reporting procedures and contingency planning x redundancy of hard- and software as well as infrastructure	x fire extinguishers ☐ water leakage detector ☐ rules of substitution for absent employees ☐ other:
1.4 Testing, assessment and evaluation		
Process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing	x documentation of business and operating procedures, data stocks, data flows and IT systems x process for regular monitoring, assessment and evaluation of data protection and information security measures x data protection management system x data protection by design and default process x incident response management system x information security management system ☐ information security certification (e.g. ISO 27001) ☐ other:	
1.5 Order or contract control		
Measures to ensure that no third-party data processing as per Article 28 GDPR takes place without corresponding instructions from Viatris	x clear and unambiguous contractual arrangements with service providers x obligation to data secrecy and confidentiality agreements with service providers x formalized order management x strict controls on selection of service providers x security pre-evaluation of service providers x supervisory follow-up checks of service providers	
1.6 Data protection controls		
Measures to ensure compliance with other data protection principles and requirements	x procedures for pseudonymization ☐ procedures for anonymization x automatic blocking and erasure routines x regular data protection and information security trainings for personnel (at least, once per year) x obligation to data secrecy for personnel x appointment of data protection officer x up-to-date record of processing activities x procedures for data subject requests x procedures for data protection incidents and personal data breaches ☐ other:	

Annex 3

Pre-Approved Sub-Processors

Qdrant uses the services of the following sub-processors for the provision of the Services and the processing of the Customer's personal data:

Name of sub-Processor	**Address**	**Task to be performed** *Please briefly explain processing activities*	**International transfer (if applicable)** *Please indicate to which country personal data is transferred if personal data is transferred to a country/recipient outside the EU/EEA*
AWS	Amazon Web Services EMEA SARL, 38 Avenue John F. Kennedy, L-1855 Luxemburg	Cloud platform provider.	
Auth0 (by Octa)	Auth0, Inc., 10800 NE 8th Street, Suite 600, Bellevue, WA 98004, U.S.A.	Authentication service provider. Stores the email and optional name (first, and last name) of the user.	EU-US Data Privacy Framework, Art. 45 of the GDPR
Google Cloud Platform	Google Cloud EMEA Limited 70 Sir John Rogerson's Quay, Dublin 2, Ireland	Cloud platform provider.	
Microsoft Azure	Microsoft Redmond, 1 Microsoft Way, United States	Cloud platform provider.	
Mailjet	Mailjet SAS 4, rue Jules Lefebvre, 75009 Paris, France	Transactional Email Provider	
Mailchimp	The Rocket Science Group, LLC 675 Ponce De Leon Ave NE Suite 5000,	Email Service Provider	EU-US Data Privacy Framework, Art. 45 of the GDPR

	Atlanta, GA 30308, United States		
Freshdesk	2950 S. Delaware Street Suite 201 San Mateo, CA 94403 USA	Support Ticket Tool	EU-US Data Privacy Framework, Art. 45 of the GDPR
Hubspot	25 First Street, Cambridge, MA 02141 USA	CRM System	EU-US Data Privacy Framework, Art. 45 of the GDPR