Kepler Cloud Data Processing Addendum

This Data Processing Addendum (“DPA”) governs the rights and obligations arising when a company within the Kepler Technologies group of companies (“Kepler”, the “Processor”) provides a Service or an ancillary service to the entity that has entered into a legally binding agreement (the “Controller”) for Kepler Technologies’ hosting and data center services (the “Agreement”), which involves the processing of the Customer as the data controller’s Personal Data on behalf of Controller. This DPA, the Agreement and any appendices constitutes the Parties’ Agreement. This DPA applies on Agreements from 2024-04-25.

1. Scope

1.1. This Data Processing Addendum shall form an integral part of the Agreement and applies to all Processing activities performed by the Processor or any third party acting on behalf of the Processor (a “Sub-processor”) of Kepler Technologies AB’ services.

1.2. This DPA replaces any existing data processing agreement in place between the Parties. In case of any inconsistencies, this DPA will take precedence over the provisions of the Agreement. Upon the Controller’s written request, the Processor will provide the Controller with a signed version of this DPA.

1.3. When Kepler Process Personal Data in the course of providing the Service, Kepler will:

- Process the Personal Data as your Data Processor, only for the purpose of providing the Services in accordance with your documented instructions and as may be agreed with you.
- If Kepler is required by law to Process the Personal Data for other purposes, we will notify you, unless we are prohibited by law to do so.
- You acknowledge that Kepler acts as a service provider and is an independent Data Controller with regards to support, security of our systems and the Service and improvement of service performance and operation of service infrastructure. Our privacy practices and how we use Personal Data can be read in our Privacy Notice, available on our website.

2. Definitions

2.1. “Appropriate Technical and Organisational Measures”, “Controller and Processor”, “Controller and Processor”, “Data Subject”, “Non-adequate Country”, “Personal Data”, “Personal Data Breach”, “Processing”, “Sub-Processor” shall have the meaning given to it in the relevant Data Protection Laws;

2.2. “Data Protection Laws” means

a) in EU countries, the General Data Protection Regulation (Regulation (EU) 2016/679) (the GDPR);

b) in non-EU countries, any similar or equivalent laws, regulations or rules relating to Personal Data;

c) any enforceable guidance and codes of practice issued by any local regulatory authority responsible for administering Data Protection Laws; and/or

d) any amendments, re-enactments or changes to the items described in (a) to (c) above, from time to time.

2.3. “Service” shall mean the service and other ancillary services provided by the Processor concerning the Processing of Controller’s Personal Data as described in the Agreement.

2.4. “SCCs” refers to the standard contractual clauses for the transfer of Personal Data to processors established in third countries, set forth in the European Commission Decision of 4 June 2021, or any such standard contractual clauses amending or replacing the SCCs.

3. The rights and obligations of the controller

3.1. The Controller is responsible for ensuring that the Processing of Personal Data takes place in compliance with the GDPR (see Article 24 GDPR), the applicable Data Protection Laws and this DPA.

3.2. The Controller has the right and obligation to make decisions about the purposes and means of the processing of the Personal Data.

3.3. The Controller shall be responsible, among other, for ensuring that the Processing of Personal Data, which the Processor is instructed to perform, has a legal basis and a valid purpose.

4. The obligations of the Processor

4.1. The Processor undertakes to Process Personal Data in accordance with this DPA and the Controller’s written instructions solely for purposes of providing the services under the Agreement. Personal Data may not in any way be Processed for any other purposes.

4.2. The nature and purpose of the Processing, the type of Personal Data and the categories of Data Subjects covered under this DPA are specified in Appendix 1, Controller’s Instructions to the Processor.

4.3. The Processor shall without undue delay, provide access to the Personal Data it has in its possession and make requested rectifications, erasures, restrictions or transfers of the Personal Data. Necessary measures to prevent recovery of Personal Data shall be taken after the Controller or the Processor has deleted Personal Data.

4.4. The Processor shall immediately inform the Controller if, in its opinion, an instruction infringes on Data Protection Laws. The Processor understands that the Processor is not required to provide legal advice to the Controller regarding the responsibilities of the Controller.

4.5. The Processor shall assist the Controller in its contacts with the supervisory authority. The Processor may not disclose Personal Data or any information on the Processing of Personal Data without explicit instructions from the Controller.

4.6. If a Data Subject requests information from the Processor concerning the Processing of Personal Data, the Processor shall forward the request to the Controller and assist the Controller in responding to such requests in accordance with Data Protection Laws.

4.7. The Processor shall assist the Controller by appropriate technical and organisational measures, taking into account the nature of the Processing.

4.8. The Processor shall take steps to ensure that any person who performs work under the supervision of the Processor and who has access to the Personal Data, only processes the Personal Data in accordance with the Controller's instructions, unless otherwise required by Data Protection Laws.

4.9. The Processor shall assist the Controller in ensuring compliance with the Controller's obligations under Data Protection Laws, e.g. insofar as this is possible, assist with security measures, fulfil data subject requests, data protection impact assessments ("DPIA") (including prior consultation), and in situations involving a Personal Data breach, notify the Controller and assist the Controller in notifying the supervisory authority and the data subjects involved.

4.10. The Processor shall maintain a record of all Processing activities carried out on behalf of the Controller. Upon the Controller's request, the Processor shall make a readable transcript available to the Controller in a generally readable electronic format, including as a minimum the following information:

a) the name and contact details of the Controller and, where applicable, the joint controller, the Controller's representative and the data protection officer;

b) the purposes of the Processing;

c) a description of the categories of Data Subjects and the categories of Personal Data;

d) the categories of recipients to whom the Personal Data have been or will be disclosed to;

e) where applicable, transfers of Personal Data to a third country including the identification of that third country and suitable safeguards employed to ensure an adequate level of protection of the Data Subject;

f) a general description of the technical and organisational measures employed to ensure an appropriate level of security;

g) where possible, the envisaged time limits for erasure of the different categories of Personal Data;

h) where possible, a general description of the technical and organisational security measures taken.

5. Security

5.1. The Processor shall implement appropriate technical and organisational security measures to protect Personal Data in accordance with Data Protection Laws. The Processor shall observe relevant codes of conduct, industry best practice, and guidelines issued or approved by supervisory authorities where applicable.

5.2. The Processor shall notify the Controller without undue delay after the Processor has become aware of any accidental or unlawful destruction, loss, alternation, unauthorised disclosure of, or access to, Personal Data.

5.3. Confidentiality. The Processor is responsible for ensuring that Processor's and its Sub-Processors' personnel who Process Personal Data for which the Controller is the Controller shall maintain secrecy, have received suitable training on Personal Data and are bound by non-disclosure agreements. The obligation of confidentiality shall remain in force even after this Data Processor Agreement has otherwise ceased to be in force. Otherwise, what is stated in the Service Agreement shall apply to the Processor's obligation of confidentiality.

5.4. Restricted access. The Processor is responsible for ensuring that only the personnel of the Processor and the Sub-Processor who need the Personal Data to fulfil the Processor's commitment under the Service Agreement shall have access to the Personal Data.

6. Sub-Processors

6.1. Use of Sub-Processors. The Processor may engage Sub-Processors for the Processing of Personal Data. The Processor is responsible for ensuring that all Processing of Personal Data performed by a Sub-Processor is governed by a written agreement with the Sub-Processor that corresponds to the requirements of this Data Processor Agreement. The Processor is fully liable for the performance of any Sub-Processors Processing of Personal Data.

6.2. Change of Sub-Processor. The Processor has the right to change a Sub-Processor or engage other appropriate and reliable Sub-Processors, provided that the rules in this Section are applied. Before engaging a new Sub-Processor, the Processor shall notify the Controller in writing of the new Sub-Processor, and upon receipt of the notice, the Controller has a right to object to the new Sub-Processor in writing within ten (10) days from receipt of the Processor's notice. Such objections shall not be deemed valid unless the Controller can prove a reasonable cause.

6.3. Resolution of objections. If the Controller has objected to a Sub-Processor, the Parties shall discuss various activities to resolve the reason for the Controller's objection together. If the Parties cannot agree on any solution within a reasonable period of time, which shall not exceed thirty (30) days, the Controller may terminate the agreement by notifying the Processor in writing. During the termination period, the Processor is not allowed to transfer any Personal Data to the Sub-Processor.

7. List of Sub-Processors. Upon the Controller's acceptance of this DPA, the Controller has pre-approved the existing sub-processors as listed on the Processor's website. During the term of the Agreement, the Processor shall maintain an updated list of all Sub-Processors who process Personal Data in connection with the Agreement and shall send a copy of the list to the Controller upon the Controller's request. Transfer of Personal Data outside of the EU/EEA

7.1. As the main rule, we will process your data in Sweden and within the EU and EEA.

7.2. If, however, the Processing carried out by the Processor includes the transfer of Personal Data to a country outside of the EU/EEA not granted an adequacy decision, the Processor shall enter into a supplementary agreement containing the then current European Commission's Standard Contractual Clauses ("SCC"), in so far as the SCC provides a lawful transfer mechanism. The Processor shall, upon the Controller's request, provide the Controller with a copy of such a signed SCC agreement. If, and to the extent that, this DPA and the SCC are inconsistent; the SCC provisions shall prevail. Obligations of the Data Importer/Processor in case of Government Access Requests. Besides entering into the new SCCs the Processor must review any legality issues and adopt appropriate ways of data minimization and additional safeguards.

7.3. The Parties undertake to monitor developments concerning regulatory pronouncements or any court rulings and, if necessary, to make adjustments to the Processing of Personal Data and this DPA insofar as this can serve the requirements for a legally secure data transfer to a third country.

8. The Processor shall forward to the Controller if it receives from its sub-processors a legally binding request by a public authority under the laws of the country of destination for disclosure of Personal Data transferred under the SCCs. The Processor and its sub-processors shall, to the largest extent possible, refuse all requests that would include access to the Controller's data by a public authority that are not legally binding. The Processor shall forward the most possible amount of relevant information on the requests received from its sub-processors to the Controller.Audits

8.1. Performance of an audit. The Processor shall provide the Controller and Controller's independent auditors with access to such information and Processor's premises as may reasonably be necessary for the Controller to be able to verify that the Processor is fulfilling its obligations according to the DPA. The Controller may only conduct audits once a year, or, when a material violation of this DPA and Data Protection Laws are suspected for good reasons, to ensure that the Processor is complying with this DPA and Data Protection Laws. The Controller shall, within a reasonable period of time (at least thirty (30) days), notify the Processor before such an audit unless otherwise required by a government authority, or the Controller has reason to suspect that the Processor or a Sub-Processor is not fulfilling its obligations according to the DPA.

8.2. Costs. Each party shall be responsible for its own costs during an audit, and the Controller shall carry the cost of any third party appointed for the audit. If the audit, initiated due to suspected material violation, would demonstrate that no material violations have been made on Processor's part, the Controller shall bear the cost of the audit.

8.3. Audit results. The Processor shall be allowed within a reasonable time period to read and provide comments to the audit report before it is made final to resolve any potential misunderstandings or minor issues. If an audit has shown that the Processor or a Sub-Processor has not fulfilled its obligations according to the DPA, the Processor shall promptly manage and correct this. Such corrective action does not affect the Controller's other possible claims and rights under this DPA.

9. Commencement and Termination

9.1. This DPA shall become effective on the date of both Parties' signature.

9.2. This DPA shall apply for the duration of the provision of Personal Data Processing services. For the duration of the provision of Personal Data Processing services, the Agreement cannot be terminated unless other Agreement governing the provision of Personal Data processing services have been agreed between the Parties.

9.3. Upon termination or expiry of the services relating to the Processing, the Processor shall submit all Personal Data to the Controller on a medium as reasonably requested by the Controller. The Processor shall thereafter ensure that no Personal Data is remaining with the Processor or any of its Sub-processors. This DPA is applicable from the date of its execution and until all Personal Data is returned, erased or made anonymous in accordance with this section.

9.4. Within thirty (30) days of the Agreement's expiration, the Processor shall delete all Personal Data that the Processor Processed under the Agreement, including Personal Data managed in backups and the like unless otherwise agreed in writing. Before deletion, the Processor shall return all Personal Data that the Processor Processed under the Agreement upon the Controller's request.

10. Changes

10.1. The Parties agree that where the Data Protection Laws changes as a result of legislative, regulatory or judicial developments, thereby altering the Parties' legal rights and/or obligations, or impacting either party's ability to perform its rights and/or obligations under this DPA, the Parties will negotiate in good faith the terms of this DPA to comply with the new developments with the goal to continue the commercial relationship between the Parties. No change of this DPA shall be valid unless made in writing.

11. Applicable Law and Disputes

11.1. The DPA shall be applied and interpreted in accordance with the law stated in the Agreement. Notwithstanding this, the Parties must at all times process Personal Data in accordance with Data Protection Laws.

11.2. Any dispute, controversy or claim arising out of or in connection with this DPA, or the breach, termination or invalidity thereof, shall be finally settled in accordance with the dispute resolution provision in the Agreement.

Appendix 1
Controller's Instructions to the Processor regarding the Kepler Technologies Services

1. Scope of Processing

1.1. The Processor shall Process Personal Data hereunder exclusively within the scope of providing the Kepler Technologies the hosting and data center services in accordance with the Parties' Agreement.

2. Purpose of processing

2.1. The purpose of the Personal Data processing is to provide contracted Services offered by Kepler Technologies at any given time to offer the applicable service modules

- Data hosting,
- Storage,
- Trouble shooting,
- Communication in support matters,
- Partner & Sub-Processor Management

3. Categories of data subjects

3.1. The processing of Personal Data under the DPA applies to the following categories of data subjects:

- The Controller's employees (incl. current and former employees, trainees and interns, pre-hires and applicants)
- The Controller's business partners (Processors, and subcontractors incl. its employees)
- The Controller's customers and contacts
- The Controller's partner contacts ("Users")
- The Controller's users of Kepler's Services

4. Categories of Personal Data

4.1. The Kepler Technologies Service does not process any special category Personal Data (such as health data, biometric data, trade union memberships, ethnic origin etc.) If you are considering submitting this type of Personal Data, contact your Kepler Technologies representative.

5. Duration of Processing

5.1. The Processor shall process the Personal Data as necessary to provide the Services to the Controller during the term of the Agreement, subject to the terms of the Agreement.

5.2. The Processor shall delete, limit or restrict its processing upon the Controller's written instruction as possible and as soon as practically possible.

6. List of Preapproved Sub-processors

6.1. The Kepler's Service is based on the use of the following Sub-Processors, which may be updated from time to time:

Sub-Processor	Service Delivered	Location of processing	Necessary to provide the Services
Glesys AB	Connectivity resources, datacenter space, switching, and hardware resources for running our private and public cloud resources	Falkenberg and Stockholm Sweden	Yes
Slack	Communication resource, data aggregation and monitoring trough slack	EU (Ireland)	No