Schedule B to Subscription and End User License Agreement

DATA PROCESSING AGREEMENT

This Data Processing Agreement (“Agreement”) is entered into by and between T.R. Björkbom-Trading Oy, a Finnish Corporation, with its principal place of business at Veneentekijäntie 8, Helsinki, Finland (“Processor”), and Processor’s respective client (“Controller”) having entered into Helm1 Subscription and End User License Agreement (“SaaS Agreement”).

The Processor and the Controller are each referred to individually as a "Party" and collectively as the "Parties".

Recitals

The Parties have entered into a SaaS Agreement under which the Processor provides the Controller with access to a software-as-a-service platform ("SaaS Service"). In connection with providing the SaaS Service, the Processor will process personal data on behalf of and under the instructions of the Controller.

In addition to acting as processor of the Controller's personal data, the Processor, in its capacity as a commercial service provider, independently determines the purposes and means of processing certain personal data of the Controller (including personal data of the Controller's authorized users and employees) for its own legitimate business purposes connected with the service provider–client relationship, including contract management, invoicing, customer support, communications, and service improvement. In relation to such processing, the Processor acts as an independent controller.

This Agreement is entered into to: (i) satisfy the requirement of Article 28(3) of the General Data Protection Regulation (EU) 2016/679 ("GDPR") for a binding written agreement governing the Processor's processing of personal data on behalf of the Controller.

This Agreement supplements and is incorporated into the SaaS Agreement. In the event of any conflict between this Agreement and the SaaS Agreement regarding data protection matters, this Agreement shall prevail.

NOW, THEREFORE, in consideration of the mutual covenants set out herein, and for other good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged, the Parties agree as follows:

1. DEFINITIONS AND INTERPRETATION

1.1 In this Agreement, the following terms shall have the meanings set out below. Terms not defined herein shall have the meanings ascribed to them in the GDPR.

a. "Applicable Data Protection Law" means the GDPR, any national law enacted pursuant to the GDPR, and any applicable supervisory guidance issued thereunder, each as amended or replaced from time to time.

b. "Controller Personal Data" means personal data of which the Controller is the controller and which is provided to, or accessed by, the Processor in connection with the SaaS Service, as further described in Annex 1.

c. "Data Subject" means an identified or identifiable natural person as defined in Article 4(1) GDPR.

d. "GDPR" means 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.

e. "Personal Data Breach" means a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed.

f. "Processor Own-Controller Data" means personal data processed by the Processor as an independent controller in the context of the service provider–client relationship.

g. "Processing" (and cognate terms) has the meaning given in Article 4(2) GDPR.

h. "SaaS Agreement" means the software-as-a-service subscription agreement between the Parties referenced in the Parties table above, including all order forms, schedules, and exhibits thereto.

i. "SaaS Service" means the software-as-a-service platform and related services provided by the Processor to the Controller under the SaaS Agreement.

j. "Standard Contractual Clauses" or "SCCs" means the standard contractual clauses for the transfer of personal data to third countries adopted by the European Commission pursuant to Article 46(2) GDPR, as currently in force.

k. "Sub-Processor" means any third party engaged by the Processor to carry out specific processing activities on its behalf with respect to Controller Personal Data.

l. "Supervisory Authority" means an independent public authority responsible for monitoring the application of the GDPR, as referred to in Article 51 GDPR.

m. “Technical and Organizational Measures" or "TOMs" means the security and data protection measures implemented by the Processor.

1.2 References to clauses, annexes, and schedules are to clauses, annexes, and schedules of this Agreement. Headings are for convenience only and shall not affect interpretation.

1.3 Where the context requires, the singular includes the plural and vice versa.

2. SCOPE

This Agreement governs Processor processing of Controller Personal Data by the Processor on behalf of and under the instructions of the Controller, where the Processor acts as a processor within the meaning of Article 4(8) GDPR.

3. NATURE, PURPOSE AND DETAILS OF PROCESSING

3.1 The details of the Processor Processing — including the subject matter, duration, nature and purpose of the processing, the type of personal data, and the categories of Data Subjects — are set out in Annex 1 to this Agreement.

3.2 The Processor shall process Controller Personal Data only for the purpose of providing the SaaS Service to the Controller in accordance with the SaaS Agreement and this Agreement, and only to the extent and in such manner as is necessary for that purpose, unless required otherwise by Union or Member State law to which the Processor is subject.

3.3 The Parties shall update Annex 1 if there is any material change in the processing activities, including where the Controller requests a new category of processing or new categories of Data Subjects, prior to such processing commencing.

4. PROCESSING INSTRUCTIONS

4.1 The Processor shall process Controller Personal Data in order to fulfill Prosessor’s obligations according to SaaS Agreement and this Data Processing Agreement. Furthermore, the Processor may may process such data on the documented instructions of the Controller, unless required to do so by Applicable Data Protection Law to which the Processor is subject. In such case, the Processor shall, to the extent permitted by law, inform the Controller of that legal requirement before processing.

4.2 If the Processor considers that any instruction from the Controller infringes Applicable Data Protection Law, the Processor shall promptly inform the

Controller. The Processor is not required to follow instructions that are manifestly unlawful.

4.3 The Controller represents and warrants that it has, and will maintain throughout the term of this Agreement, a lawful basis under Applicable Data Protection Law for instructing the Processor to process Controller Personal Data as contemplated by this Agreement.

5. PROCESSOR OBLIGATIONS

5.1 The Processor shall:

a. process Controller Personal Data only in as set out in Clause 4, except where required otherwise by Applicable Data Protection Law;

b. ensure that persons authorized to process Controller Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;

c. implement and maintain the Technical and Organizational Measures, taking into account the nature, scope, context and purposes of processing and the risks to the rights and freedoms of Data Subjects;

d. taking into account the nature of the processing, assist the Controller by appropriate TOMs insofar as this is possible in the fulfilment of the Controller's obligation to respond to Data Subject requests under Chapter III GDPR, as further set out in Clause 10;

e. assist the Controller in ensuring compliance with its obligations under Articles 32 to 36 GDPR (security, breach notification, DPIAs, and prior consultation), taking into account the nature of the processing and the information available to the Processor, as further set out in Clauses 7 and 8;

f. upon the choice of the Controller, delete or return all Controller Personal Data at the end of the provision of services relating to processing, and delete existing copies unless Union or Member State law requires storage of the personal data, as further set out in Clause 13; and

g. make available to the Controller all information necessary to demonstrate compliance with Article 28 GDPR, and allow for and contribute to audits and inspections by the Controller or an auditor mandated by the Controller, as set out in Clause 14.

6. CONFIDENTIALITY

6.1 The Processor shall ensure that access to Controller Personal Data is limited to those employees, contractors, agents, and authorized personnel of the Processor

and its Sub-Processors who have a strict need to know in order to perform the SaaS Service.

6.2 The Processor shall ensure that all such persons are subject to binding obligations of confidentiality with respect to Controller Personal Data, whether by contract, professional rules, or statutory obligation. Such obligations shall survive the termination or expiry of the relevant employment or engagement.

6.3 The Processor shall not disclose Controller Personal Data to any third party except: (a) to authorized Sub-Processors in accordance with Clause 9; (b) as required by Applicable Data Protection Law or other applicable law, in which case the Processor shall, where legally permitted, give the Controller prior written notice; or (c) with the prior written consent of the Controller.

7. SECURITY OF PROCESSING

7.1 The Processor shall implement and maintain the Technical and Organisational ensuring a level of security appropriate to the risk presented by the processing and the nature of the Controller Personal Data to be protected, in accordance with Article 32 GDPR.

7.2 In assessing the appropriate level of security, the Processor shall take into account, in particular, the risks presented by accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Controller Personal Data transmitted, stored or otherwise processed.

7.3 The Processor shall not reduce the level of security provided by the TOMs without the prior written consent of the Controller. The Processor shall keep the TOMs under review and update them in accordance with developments in technology and changes in the risk landscape.

7.4 The Processor shall ensure that any Sub-Processors engaged to process Controller Personal Data are subject to equivalent security obligations.

8. PERSONAL DATA BREACH NOTIFICATION

8.1 The Processor shall notify the Controller of a Personal Data Breach affecting Controller Personal Data without undue delay and, where feasible, no later than twenty-four (24) hours after becoming aware of the breach.

8.2 The notification shall, to the extent the information is available, include:

a. a description of the nature of the Personal Data Breach, including, where possible, the categories and approximate number of Data Subjects concerned and the categories and approximate number of personal data records concerned;

b. the name and contact details of the Processor's data protection officer or other contact point from which more information can be obtained;

c. a description of the likely consequences of the Personal Data Breach; and

d. a description of the measures taken or proposed to address the Personal Data Breach, including, where appropriate, measures to mitigate its possible adverse effects.

8.3 Where the information required in Clause 8.2 is not fully available at the time of initial notification, the Processor shall provide the information in phases as it becomes available, without undue further delay.

8.4 The Processor shall document all Personal Data Breaches, including those not required to be notified to a Supervisory Authority, in accordance with Article 33(5) GDPR. Such documentation shall be made available to the Controller upon request.

8.5 The Processor shall cooperate fully with the Controller in the investigation, remediation, and notification of any Personal Data Breach to Supervisory Authorities and Data Subjects, to the extent required by Applicable Data Protection Law.

8.6 The Processor shall not communicate to any Data Subject or to any third party, including any Supervisory Authority, about a Personal Data Breach affecting Controller Personal Data without the prior written consent of the Controller, unless required to do so by Applicable Data Protection Law.

9. SUB-PROCESSORS

9.1 The Controller grants the Processor general written authorization to engage Sub-Processors, subject to the conditions set out in this Clause 9.

9.2 The Processor shall inform the Controller of any intended changes concerning the addition or replacement of Sub-Processors by providing the Controller with written notice at least 7 calendar days prior to the intended change taking effect. The Controller may object to the addition or replacement of a Sub-Processor on reasonable data protection grounds within 5 calendar days of receiving notice. If the Controller objects and the Parties cannot resolve the objection within a further 7 days, either Party may terminate the SaaS Agreement and this Agreement on written notice.

9.3 Where the Processor engages a Sub-Processor, it shall impose on the Sub-Processor data protection obligations that offer at least equivalent levels of protection to those set out in this Agreement, by means of a binding written sub-processing agreement. In particular, the Sub-Processor shall be required to comply with the obligations applicable to the Processor under Article 28(3) GDPR.

9.4 The Processor remains fully liable to the Controller for the performance of Sub-Processors' obligations under the sub-processing agreement to the extent that those Sub-Processors fail to fulfil their data protection obligations.

10. DATA SUBJECT RIGHTS

10.1 Taking into account the nature of the processing, the Processor shall assist the Controller, by appropriate technical and organizational measures insofar as this is possible, in fulfilling the Controller's obligation to respond to Data Subject requests for the exercise of their rights under Chapter III GDPR, including rights of:

a. access (Article 15 GDPR);

b. rectification (Article 16 GDPR;

c. erasure (Article 17 GDPR);

d. restriction of processing (Article 18 GDPR);

e. data portability (Article 20 GDPR); and

f. objection (Article 21 GDPR).

10.2 Should a Data Subject contact the Processor directly with a request to exercise any of the rights listed in Clause 10.1 in relation to Controller Personal Data, the Processor shall promptly, and in any event within 5 business days, forward the request to the Controller and shall not respond to the Data Subject without the Controller's prior written authorization, unless required to do so by Applicable Data Protection Law.

10.3 Processor shall, upon request, provide the Controller with reasonable assistance in responding to any Data Subject request, including by extracting, rectifying, restricting, porting, or deleting Controller Personal Data within the SaaS Service, within the timeframes reasonably specified by the Controller.

11. DATA PROTECTION IMPACT ASSESSMENTS AND PRIOR CONSULTATION

11.1 The Processor shall provide the Controller with all reasonable assistance in relation to any data protection impact assessment ("DPIA") that the Controller is required or chooses to carry out pursuant to Article 35 GDPR, taking into account the nature of the processing and the information available to the Processor.

11.2 The Processor shall assist the Controller with any prior consultation with a Supervisory Authority required under Article 36 GDPR, providing such information as may be reasonably requested by the Controller or the relevant Supervisory Authority.

12. INTERNATIONAL TRANSFERS OF CONTROLLER PERSONAL DATA

12.1 The Processor shall not transfer, or permit the transfer of, Controller Personal Data to a country or territory outside the European Economic Area ("EEA") unless:

a. The European Commission has adopted an adequacy decision in relation to the destination country under Article 45 GDPR;

b. appropriate safeguards are in place in accordance with Article 46 GDPR, including Standard Contractual Clauses; or

c. one of the derogations in Article 49 GDPR applies and the Controller has provided its prior written consent.

12.2 The Processor shall inform the Controller of any circumstances that may affect the availability or validity of a transfer mechanism relied upon under Clause 12.1, including any relevant decisions, laws, or circumstances in the destination country that may impair the protection afforded to Controller Personal Data.

13. RETENTION AND DELETION OF CONTROLLER PERSONAL DATA

13.1 The Processor shall not retain Controller Personal Data for longer than is necessary to provide the SaaS Service or as otherwise instructed in writing by the Controller, subject to any mandatory retention requirements under Applicable Data Protection Law or other applicable law.

13.2 The Processor shall, in respect of Controller Personal Data, apply the retention periods set out in Annex 1.

13.3 Upon termination or expiry of the SaaS Agreement, or upon written request of the Controller at any time, the Processor shall, at the choice of the Controller and within 7 calendar days of receiving such instruction:

a. securely delete or destroy all Controller Personal Data (including all copies and backups) in its possession, custody, or control; or

b. securely return all Controller Personal Data to the Controller in a structured, commonly used and machine-readable format,

and in either case provide written certification to the Controller that it has done so, save to the extent that Applicable Data Protection Law or other applicable law requires continued storage of the Controller Personal Data.

13.4 The Processor shall ensure that Sub-Processors are subject to equivalent obligations regarding deletion and return of Controller Personal Data.

14. AUDIT RIGHTS AND INFORMATION

14.1 The Processor shall make available to the Controller, upon reasonable prior written notice of not less than 7 business days, all information reasonably necessary to demonstrate compliance with the obligations laid down in this Agreement and in Article 28 GDPR.

14.2 The Processor shall allow for and contribute to audits, including inspections, conducted by the Controller or an auditor mandated by the Controller, subject to the following conditions:

a. audits shall be conducted during normal business hours, subject to reasonable advance written notice;

b. the Controller shall bear all costs and expenses associated with the audit;

c. audits shall be conducted no more than once per calendar year, absent a reasonable cause related to a suspected breach of this Agreement or a Personal Data Breach; and

d. auditors must execute a confidentiality agreement acceptable to the Processor prior to conducting any audit.

14.3 The Processor may satisfy the audit requirements of this Clause, in whole or in part, by providing the Controller with up-to-date third-party audit reports or certifications (e.g. ISO 27001, SOC 2 Type II) that adequately address the subject matter of the requested audit.

14.4 The Processor shall promptly provide any information reasonably requested by the Controller, the Controller's data protection officer, or a competent Supervisory Authority in connection with any investigation into the processing activities under this Agreement.

15. PROCESSOR'S OWN-CONTROLLER PROCESSING

15.1 This Data Processing Agreement does not cover personal data the Processor processes certain personal data of the Controller's employees, representatives, and authorized users as an independent data controller. The processing of such data is governed by the Privacy Policy of the Processor forming an integral part of Subscription and End User License Agreement as schedule A, available on the Company's web site in www.helm1.com.

16. LIABILITY

16.1 Each Party shall be individually and independently liable for its own compliance with Applicable Data Protection Law in relation to the processing activities for which it is responsible under this Agreement.

16.2 Where both Parties have contributed to damage caused by processing in breach of Applicable Data Protection Law, they shall be jointly and severally liable in

accordance with Article 82 GDPR, subject to the right of each to be exonerated from liability to the extent they can prove that the damage is not attributable to them.

16.3 Each Party shall indemnify and hold harmless the other Party against any fines, penalties, claims, damages, costs, and expenses (including reasonable legal fees) arising from that Party's breach of its obligations under this Agreement or under Applicable Data Protection Law.

16.4 Any limitation of liability set out in the SaaS Agreement shall apply to this Agreement to the extent permitted by Applicable Data Protection Law, save that no limitation shall apply to a Party's liability for: (a) intentional or grossly negligent breaches; (b) fines or administrative penalties imposed by a Supervisory Authority; or (c) liability to Data Subjects under Article 82 GDPR.

17. TERM AND TERMINATION

17.1 This Agreement shall enter into force at the same time with the SaaS Agreement and shall remain in force for as long as the Processor processes Controller Personal Data pursuant to the SaaS Agreement, unless terminated earlier in accordance with this Clause.

17.2 This Agreement shall automatically terminate upon the termination or expiry of the SaaS Agreement, subject to any surviving obligations expressly provided herein.

17.3 Either Party may terminate this Agreement immediately by written notice if the other Party commits a material breach of this Agreement that is incapable of remedy, or fails to remedy a remediable material breach within thirty (30) calendar days of receiving written notice specifying the breach.

17.4 The following clauses shall survive the termination or expiry of this Agreement: Clause 6, Clause 13, Clause 16, Clause 17, Clause 18, and any other provisions which by their nature or express terms should survive.

18. GENERAL PROVISIONS

18.1 Governing law. This Agreement shall be governed by and construed in accordance with Finnish law, excluding its choice of law rules.

18.2 Dispute resolution. Any dispute, which may arise between the parties concerning this Agreement, shall be determined by Helsingin käräjäoikeus (District Court of Helsinki).

18.3 Entire Agreement. This Agreement, together with its Annexes and the SaaS Agreement, constitutes the entire agreement of the Parties with respect to the subject matter hereof and supersedes all prior discussions and agreements. In the

event of a conflict between the SaaS Agreement and this Agreement on data protection matters, this Agreement prevails.

18.4 Amendments. No amendment to this Agreement is effective unless made in writing and signed or otherwise agreed to by duly authorized representatives of both Parties.

18.5 Severability. If any provision of this Agreement is found to be invalid or unenforceable under applicable law, such provision shall be modified to the minimum extent necessary to make it valid and enforceable, and the remaining provisions shall continue in full force and effect.

18.6 Notices. All notices under this Agreement shall be in writing and delivered to the contact details set out in the Parties table, or such other address as a Party may designate by written notice to the other Party.

18.7 Counterparts. This Agreement may be executed in counterparts, each of which shall be deemed an original. Electronic signatures shall be valid and binding.

18.8 No Waiver. Failure by either Party to enforce any right under this Agreement shall not constitute a waiver of that right.

Annex 1 to Data Processing Agreement

T.R BJÖRKBOM-TRADING OY

RECORD OF PROCESSING ACTIVITIES PURSUANT TO ARTICLE 30 GDPR / hELM1

1. Processor

T.R. Björkbom-Trading Oy Ab (hereinafter "TRB")

Business ID	0723426-4
Address	Veneentekijäntie 8, Helsinki, Finland
Contact person for data protection matters	John Björkbom
Email	john.bjorkbom@bjorkbomtrading.fi
Telephone	+358 50 555 3536

2. Personal Data Processed and Data Subjects

TRB processes, on behalf of the Customer acting as Controller in connection with the hELM1 service, the following categories of personal data:

- name
- work email address
- role or user group
- user credentials and status of user credentials
- administrator credentials, administrator role, and status of administrator credentials
- access rights-related data
- login and log data

Categories of data subjects: The Customer's employees and contact persons using the website in various roles.

3. Purposes of Processing and Legal Basis

- Provision and maintenance of services
- Verification of identity
- Customer support
- Development of services
- Notification of new services and features

- Technical administration of the service
- Maintenance of information security
- Access control
- Support services
- Log data

Legal bases: Performance of a contract (customer relationship), compliance with legal obligations, legitimate interests, and consent.

4. Recipients of Personal Data

Personal data is transferred to the following processors:

IT service providers: Development, maintenance, and management of information systems.
Hosting service providers: Maintenance and development of services.

5. Transfers of Personal Data to Third Countries or International Organizations

Personal data is currently transferred outside the EU/EEA, in particular to cloud service platforms located in the United States. Appropriate safeguards are applied to such transfers, including standard contractual clauses and any necessary supplementary technical, organizational, or contractual measures in accordance with the GDPR. It is intended to modify the system in the near future so that the relevant services will be located within the EU.

6. Retention Periods for Personal Data

Personal data is retained as follows:

Website visitors' data (cookies): 12 months from the last activity.
Service users: 1 month from the date on which the customer has removed the person as a user of the service.

7. Security Measures for Personal Data

Personal data is protected by appropriate technical and organizational measures. Data is stored in an encrypted database on servers provided by third-party cloud service providers. Access to personal data is restricted to authorized employees and service providers who require the data for the performance of their duties and who are bound by a duty of confidentiality. Access to the internal network requires two-factor authentication.