ANNEX CONCERNING THE PROCESSING OF PERSONAL DATA, draft xx.x.20xx

1 Parties, background and purpose

This annex concerning the processing of personal data (”**Annex**”) is an inseparable part of the agreement (”**Agreement**”) signed between xxx (”**Provider**”) and Helsinki Partners Oy, Business ID 3209009-8 (”**Customer’’)** on the [date] of [month] 20xx concerning agreed services.

Depending on the context, the Customer may separately act as a joint registrar together with another data controller(s) and then the Customer and the other joint registrar(s) agree their mutual obligations pursuant to the currently applicable data protection legislation.

The purpose of this Annex is to enter into a binding data processing agreement between the Parties on the processing of personal data as required by the EU general data protection regulation 2016/679 and other data protection legislation applicable currently to the Agreement and the processing of personal data under this Annex and ensure the necessary level of privacy and data security of the personal data of the Customer (“**Customer Data**”) processed by the Provider. The Parties acknowledge and agree that in the event of a change in legislation or regulatory guidance, the terms of this Annex will be revised to reflect such change.

The types of personal data and the categories of data subjects, the duration, nature and the purpose of the processing and the guidance of the Customer are defined in the annex processing specification form (“**Annex A**”) unless it is agreed otherwise in the Agreement or it’s appendices e.g. orders.

The parties acknowledge that the service provided on the basis of the Agreement contains such information, the confidentiality of which may be e.g. critical to the safety and rights of the Customer and individuals, the operation of the Customer, the rights and obligations imposed by law, and compliance with instructions binding on authorities and individuals.

2 Relation to the Agreement and applicability

If the terms concerning the processing of personal data of this Annex and the Agreement are in conflict, the parties shall primarily comply with the terms of this Annex.

If the JIT 2025 General Terms and Conditions apply to the Agreement, this Annex shall apply mutatis mutandis in place of those corresponding terms and conditions. If the JIT 2025 Special Terms and Conditions for Services Delivered via a Data Network apply to the Agreement, this Annex shall apply mutatis mutandis in place of

those equivalent terms.

This Annex shall enter into force upon signature by the Parties. Signed and electronically provided Annex is as binding as original signed agreement.

The Annex remains in force and effective until the processing of personal data based on the Agreement and Annex is completed in full and terminates thereafter automatically.

If the Provider materially violates this Annex, the Customer shall have the right to terminate this Annex thirty (30) days after the Customer notified the Provider of the violation or when the Provider should have discovered the violation.

Upon expiration of the Annex, the Provider shall delete, destroy or return Customer's personal information as set forth in Section 5.

3 Definitions

Terms used in this Annex “controller”, “processor”, “data subject”, “personal data”, “personal data breach” and processing are equivalent to terms of the EU general data protection regulation 2016/679 (“**GDPR**”) and in national data protection legislation.

4 General requirements for the Provider concerning privacy and data security

The Provider shall have documented processes and operational models for risk management in its operations. The Provider is responsible for detecting and identifying privacy and data security risks and to prevent and minimize such risks.

The Provider shall have sufficient expertise and resources to carry out the privacy and data security measures defined in this Annex and other privacy and data security measures required by the Customer. The Provider shall, if necessary, work together with Customer’s privacy and data security personnel.

The Provider warrants that it will take technical, physical and organizational measures to ensure a high level of security of the processing of Customer Data and to protect Customer Data against unauthorized or illegal processing and against unintentional loss, destruction, damage, alteration or disclosure. These security measures must comply with applicable laws.

The Provider is responsible for ensuring that the confidentiality, availability or integrity of the Customer Data is not compromised due to the negligence of the Provider's personnel, incorrect working practices or other activities in violation of this Annex or the Agreement.

The Provider is responsible for ensuring at all times that the service it provides under the Agreement is fault-tolerant and that the Customer Data stored in the service can be quickly restored in the event of a physical or technical failure.

The Provider monitors developments and news related to information security that are relevant to the service. The Provider is actively preparing for and responding to new information security threats and threats.

The Provider shall, if necessary, assist the Customer, free of charge, unless otherwise agreed in writing, in carrying out the impact assessment pursuant to Article 35 of the GDPR and in carrying out the prior consultation pursuant to Article 36.

The Provider shall inform the Customer about the information security of the service referred to in the Agreement and other matters related to compliance by active

contacting the Customer and in such a way that the Customer is constantly aware of them.

5 Data protection and processing personal data

General. The Provider processes Customer Data on behalf of the Customer. For the purposes of this Annex, Customer Data means, and the subject of processing is, personal data that the Customer provides to the Provider to be processed in accordance with the Agreement and this Annex, and which relates to an identified or identifiable natural person (hereafter referred to as "**Data Subject**"). E.g. the data identifiable to employees, customers or other persons may be considered personal data.

The Customer is the controller of the Customer Data processed in the service, and the Provider is the processor of the same. The Provider shall not process the Customer Data for purposes other than the performance of the Agreement and this Annex. The Parties agree to abide by the legislation, regulations and official decrees, guidance and accepted practices of Finland and the European union.

Obligations of the Customer. As the controller, the Customer is responsible for ensuring that it has the necessary rights and it has acquired, for example, the necessary consents to process Customer Data and transfer Customer Data to the Provider. The Customer is responsible for drafting a record and informing otherwise the Data Subjects pursuant to the GDPR.

Purpose and means of processing. The Provider has the right to process Customer Data only in accordance with the Agreement, this Annex and the written guidance of the Customer and only insofar as it is necessary to deliver the Service pursuant to the Agreement. The Customer has the sole right to define the purpose and means of processing of personal data. The ownership to Customer Data shall with all respects belong to the Customer, and the Provider are not granted any rights to Customer Data except to process Customer Data pursuant to this Annex and the Agreement.

The Customer has the right to give the Provider instructions on the processing of Customer Data. The Provider shall immediately notify the Customer if it considers that the Customer's instructions violate the GDPR or other data protection legislation. The Customer has the exclusive right to determine the purpose and means of the processing of Customer Data.

Subcontractors. The Provider may not engage subcontractors in processing the Customer Data without Customer's prior subcontractor-specific or general written authorization. Additionally, the Provider must keep the Customer informed of all subcontractors and changes concerning them. The Customer has the right to deny the use of new subcontractors on reasonable grounds.

The Provider undertakes to sign written agreements with its subcontractors and the Provider shall ensure that the subcontractors will adhere to the terms of this Annex and other possible guidance of the Customer and data protection legislation. The Provider shall regularly supervise the actions of its subcontractors and shall be liable for the acts of its subcontractors as if they were the Provider's own.

The Customer has the right to revoke its consent to the Provider for the use of subcontractors for a justified reason. Cancellation must be made in writing to the Provider. The Provider must find a replacement subcontractor without delay if the use of a subcontractor is still necessary.

Transfers of personal data/Customer Data. Customer Data may not be stored, transferred, disclosed, altered, used or otherwise processed in real time, in an archive, backups or in any other form in a country outside of the EU/EEA without the prior written authorization of the Customer. The Parties shall in advance agree in writing of all transfers or processing of Customer Data outside of the EU/EEA. In the absence of adequacy decision by the EU Commission the standard contractual clauses ("**SCC**") approved by the European Union shall be primarily applied on all Customer Data transfers outside the EU/EEA. As an alternative for SCCs, other approved transfer mechanisms for transfer of Customer Data can be used. The Provider shall inform the used mechanism and the countries outside the EU or EEA before storing, transferring, transferring, disclosing, altering, using or otherwise processing Customer Data outside of EU/EEA, in order that the Customer can fulfill the controller obligations set out in the GDPR.

Requests of Data Subjects. The Provider must immediately forward all requests to inspect, rectify, erase, ban the processing of data or other requests received from the Data Subjects to the Customer. At the Customer's request, the Provider must support the Customer free of charge in carrying out the requests of the Data Subjects. The Provider shall ensure that it can carry out all the statutory requests of a Data Subject.

Inquiries of supervisory authorities. The Provider shall direct all inquiries by the data protection authorities or other authorities relating to Customer Data to the Customer and shall wait for further written instruction from the Customer. If nothing else is agreed in writing, the Provider is not allowed to represent the Customer or act on behalf of the Customer in relation to the authorities. The Provider assists the Customer to ensure the compliance with the GDPR articles 32-36.

Audit rights. At Customer's request the Provider is obligated to prove that it and its subcontractors adhere to the terms of this Annex, the Agreement, and other possible guidance of the Customer. By giving a prior 14 days' written notice, the Customer or a third-party auditor (however not a competitor of the Provider) on behalf of the Customer may annually whenever inspect the Provider's and its subcontractors' compliance with this Annex, the Agreement, and other possible guidance of the Customer. The Customer may perform the audit without the aforementioned prior notice if the Customer has reasonable grounds to suspect that the Provider has not complied with this Annex, the Agreement or the Customer's instructions. The Provider shall ensure that the Customer can perform the audit. The Provider undertakes to assist the Customer in carrying out the audit by the necessary means. The Provider shall have obligation to rectify the detected infringements and shortcomings without delay at its own expense. Each Party shall carry its own costs caused by the audits. The Customer or an auditor authorized by the Customer may revise the adequacy of the repairs made by the Provider. If an audit shows a material breach of this Annex, Agreement or other guidance of the Customer by the Provider,

it shall pay the external costs according to the invoice of the third-party auditor for the audit as well as for the subsequent inspection of the corrections.

Provider's Liability. The Provider shall be responsible for all obligations, acts and requirements (including reasonable legal expenses) that are caused to the Customer and its management, officers, personnel or contracting parties and Data Subjects for the processing of Customer Data or data subject's personal data because of the Provider's breach of applicable data protection laws, Agreement and this Annex or the written guidance of the Customer.

If the Provider breaches its privacy and data security obligations provided in the Agreement, this Annex or applicable legislation and the Customer, as a result, must pay reparations to a third party, or a supervisory authority fines the Customer or issues a punitive payment to the Customer, the Provider shall compensate the Customer for the reparations and payments, as well as compensate the Customer for the expenses due to the clarification of the matter and the defence against claims in full.

Erasure or return of Customer Data. During the term of the Agreement, the Provider may not erase Customer Data processed on behalf of the Customer without the Customer's express request. At the expiry of the Agreement the Provider shall return and/or delete all Customer Data to the Customer in the form defined in writing in the guidance of the Customer. If the Customer has not given guidance to the Provider within one (1) month from the expiry of the Agreement, the Provider shall without delay inquire the Customer in writing for guidance concerning the deletion and return of Customer Data. The Provider shall support the Customer to a requested extent in transferring the data free of charge unless otherwise agreed in writing between the parties. Thereafter the Provider shall ensure that the copies of the Customer Data in the possession of the Provider and its subcontractors shall be deleted and shall confirm the deletion to the Customer in writing. The Provider is not entitled to a separate charge for the deletion and/or return for Customer Data, unless otherwise agreed in writing between the Parties.

Personnel Security: The Provider shall maintain an up-to-date list of the access rights, admittance and authorizations of the persons involved in the provision of services under the Agreement.

In the situations specified in the Act on Security Clearances (726/2014), the Customer may request a security clearance referred to in that Act or, if necessary, a foreign security clearance of an equivalent level from employees of the Provider or its subcontractor(s) who process Customer Data or access systems containing Customer Data. The Provider is

responsible for obtaining the consent of the person subject to the safety case and commissioning the safety case. The Provider is responsible for the costs of the safety reports described above.

The Provider shall ensure that only those persons who need to process Customer Data have access to the Customer Data. This should be done, for example, with access control, access codes or other means that implement data protection. The Provider is responsible for ensuring that the persons who process Customer Data are bound by the obligation of professional secrecy with regard to the processing of Customer Data. Persons who have access to and process Customer Data shall only process.

6 Data security

Customer Data in accordance with this Annex, Agreement and the documented instructions and legislation provided by the Customer.

Security of the premises: The premises of the Provider and its subcontractors in which the Customer Data is stored, used or otherwise processed must be adequately protected by locking and other necessary measures to prevent unauthorized access to the premises and the protected personal data contained therein.

Service development: If the Provider changes or expands its information systems in use during the term of this Annex, the Provider is obliged to review the information security requirements of the information systems and notify the Customer of such change.

The Provider shall continuously develop the service in accordance with the Agreement in order to meet the requirements related to information security.

The Provider shall ensure an appropriate level of security, as may be required from time to time, by implementing technical and organizational data security measures required by the applicable data protection laws, this Annex and by the Agreement in order to protect the Customer Data. The technical options, special risks and sensitivity relating of the processed Customer Data and risks to the rights and freedoms of natural persons of varying probability and severity, as well as the Customer's instructions and possible updates to the instructions shall be taken into account when organizing security measures.

E.g. the following rules must be adhered to when processing Customer Data:

1) The Provider ensures that the personnel of the Provider and of its subcontractors shall commit themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

2) The systems and communications used to process the Customer Data shall be protected by appropriate and up-to-date data security solutions in line with industry best practices.

3) The Customer Data shall not be used for Provider´s own business or service development or other purposes of its own.

The Provider shall be responsible for regularly backing up of the Customer Data, unless otherwise agreed.

With respect to data security updates, admittance, access control and other similar data security practices, the policies defined or separately agreed in the Agreement or the Customer's security guidelines shall apply.

7 Managing data security incidents

The Provider shall notify the Customer of all actual and suspected security incidents with regard to Customer Data, such as security breaches, accidental or unlawful destruction or alteration, unauthorized disclosure or access to Customer Data, as well as other material disruptions or problems of the service that may affect the status and rights of Data Subjects, without undue delay and at the latest within 24 hours of being informed of such event or incident. The notification must describe the events, whose Customer Data or what Customer Data was concerned, and the volumes of affected Data Subjects or Customer Data.

The Provider shall investigate all causes for the breach and take appropriate actions to end the breach, mitigate the effects and prevent further similar breaches. The Provider must without delay document in writing the results of the investigation and the actions taken for the Customer to eliminate the security incidents and to limit and remedy their effects.

The Provider must work together with the Customer and ensure that the Customer has the documentation required by legislation and data protection authorities regarding data security incidents.

8 Revisions of this Annex

The Provider shall be obligated to inform the Customer in writing of all changes that may affect its ability or prospects to abide by this Annex and the written guidance of the Customer.

The Parties will agree on all additions and changes to this Annex in writing.

9 Signatures

Helsinki xx.xx.20xx.

Clarisse Berggårdh

CEO

Helsinki Partners Oy

[Name]

[Position]

[Company]