Personal Data Processing Agreement

Directo (registry code 10652749; seat at Mõisa 4, Tallinn, 13522 Estonia) and the **Client** have concluded an Agreement for the use of Directo business software and related services (hereinafter the **Services**). In connection with the performance of the Agreement, Directo may process certain personal data on behalf of the Client. This Personal Data Processing Agreement (hereinafter the **DPA**) forms an integral part of the Agreement and the purpose of the DPA is to ensure lawful and purposeful processing of personal data in compliance with the requirements of the EU General Data Protection Regulation (2016/679) (hereinafter the **GDPR**) and Estonian personal data protection laws.

1. DEFINITIONS

1.1 Unless indicated otherwise, all the terms used herein are defined in the GDPR.

1.2 **Data subject** means an identified or directly or indirectly identifiable natural person whose personal data are processed by the Parties under the Agreement.

1.3 **Personal data** means any personal information of an identifiable Data Subject. The Personal Data processed by Data Processors under the DPA are further defined in Section 4 of this DPA.

1.4 **Data Controller** means the controller of Personal Data who determines the purpose and scope of processing of the Personal Data. The Client shall determine which Personal Data and to what extent they wish to have processed in connection with the use of the Services. When using the Services, the Client is the Data Controller.

1.5 **Data Processor** means a processor of Personal Data who processes Personal Data only on behalf of and according to the instructions of the Data Controller in compliance with the Agreement and this DPA. In connection with the Services, Directo processes Personal Data on behalf of the Client and is therefore a Data Processor when providing the Services.

1.6 **Sub-processor** is a processor engaged by the Data Processor.

2. GENERAL OBLIGATIONS OF THE DATA CONTROLLER

2.1 **The basis for processing**. The Data Controller shall ensure that there is an appropriate basis for processing by itself and the Data Processor. The Data Controller shall make available to the Data Processor and insert/transmit to the Data Processor's Services and systems only Personal Data for which the Data Controller has a valid basis for processing.

2.2 **Obligation to provide information**. The Data Controller shall ensure compliance with the obligation to provide information regarding the Personal Data processed under the Agreement in accordance with Articles 13 and 14 of the GDPR, including, if appropriate, by providing information on processing carried out by the Data Processor.

2.3 **Processing in compliance with the GDPR**. The Data Controller warrants that it will process Personal Data in accordance with the requirements of the GDPR and will provide the Data Processor instructions for Personal Data processing in strict accordance with the requirements of the GDPR.

2.4 **Instructions and contacts**. The Data Controller shall provide instructions for Personal Data processing in a format which can be reproduced in writing.

The Client's contact is set out in the Main Terms.

Directo's contact is dpo@directo.ee.

3. GENERAL OBLIGATIONS OF THE DATA PROCESSOR

3.1 **Data Processor's compliance with the GDPR**. The Data Processor shall comply with and shall use only Sub-processors who comply with the requirements of the GDPR. The Data Processor shall comply with the following conditions:

3.1.1 **Processing in compliance with the Agreement and the DPA**. The Data Processor shall process Personal Data only to the extent and in the manner necessary for the provision of the Services set out in the Agreement and this DPA and in accordance with the instructions which the Data Controller may provide from time to in a format which can be reproduced in writing;

3.1.2 **Confidentiality.** The Data Processor shall keep the Personal Data confidential and shall not use or disclose them for any purpose other than permitted by this DPA or the Agreement. Responding to the Data Subject's or the authorities' enquiries relating to Personal Data shall not constitute a breach of confidentiality;

3.1.3 **Appropriate technical and organisational measures.** The Data Processor shall implement appropriate technical and organisational measures to protect Personal Data against unauthorised or unlawful processing, accidental loss or destruction or damage;

3.1.4 **Assisting the Data Controller**. The Data Processor shall reasonably assist the Data Controller in relation to any request and/or enquiry, investigation or assessment relating to the processing of Personal Data, including the preparation of a data protection impact assessment and cooperation in case of a breach (see Section 8.3). The Data Processor may charge a fee for the assistance provided in accordance with the applicable price list, except in cases where such assistance is required due to acts or omissions of the Data Processor and/or its Sub-processor(s) in breach of the requirements of the Agreement or this DPA;

3.1.5 **Data Subjects' enquiries.** The Data Processor shall inform the Data Controller of any enquiries received from Data Subjects and shall forward them and, where necessary (if the enquiry relates to the Data Processor's systems and the Data Controller does not have all the necessary information), assist in responding to them;

3.1.6 **Return and/or deletion of Personal Data.** Upon the Data Controller's request, the Data Processor shall return to the Data Controller or delete all the Personal Data in the Data Processor's domain, possession or control, except where retention of a copy is mandatory under the law. Such return and/or deletion shall be effected within a reasonable period.

3.2 **Data processing contracts with Sub-processors**. The Data Processor shall ensure that Sub-processors are bound by a contractual obligation to comply with Personal Data processing requirements equivalent to those contained in this DPA.

4. CATEGORIES OF DATA SUBJECTS AND PERSONAL DATA

4.1 Unless the Parties have agreed otherwise, the categories of Personal Data processed are:

CATEGORIES OF DATA SUBJECTS	1) Data Controller's employees, including persons in a contractual relationship similar to employment; 2) individuals representing the Data Controller's cooperation partners; 3) Data Controller's customers and potential customers who are natural persons; 4) other categories of Data Subjects whose data the Data Controller transfers to the Data Processor or enters into the Data Processor's systems; 5) the categories of Data Subjects in companies belonging to the Data Controller's group.
CATEGORIES OF PERSONAL DATA	1) Names, contact details, ID code, date of birth, position, address; 2) employment-related information; 3) information on product purchases, use of the Services, etc.; 4) any other information that the Data Controller has provided to the Data Processor or entered into the Data Processor's systems; 5) any other information necessary for the performance of the Agreement with the Data Controller.
PURPOSES	1) Providing business software and related services.

5. SUB-PROCESSORS

5.1 **Right to use Sub-processors**. The Data Controller allows the use of Sub-processors on the condition that the Data Processor only uses Sub-processors who comply with the GDPR and other applicable data protection requirements. Furthermore, the Data Processor shall remain fully liable to the Data Controller for any acts and omissions of the Sub-processors. By signing the Agreement, the Data Controller agrees to the use of the following Sub-processors:

NAME AND REGISTRY CODE OF SUB-PROCESSOR	PURPOSE
Telia Eesti AS registry code 10234957, Estonia	Data hosting and administration services
IK Konsultatsiooniteenused OÜ registry code 12005988, Estonia	Implementation and consulting services
AR Konsultatsioonide OÜ registry code 12939478, Estonia	Implementation and consulting services
SIA Harrstone registry code 50203228761, Latvia	Integration developments
Askendo OÜ registry code 11201368, Estonia	Implementation and consulting services
FixSys OÜ registry code 12046604, Estonia	Implementation and consulting services

Vettermax OÜ registry code 14383387, Estonia	Implementation and consulting services
Arbaser OÜ registry code 12942049, Estonia	Implementation and consulting services

If the Sub-processors change, the Data Processor shall provide the new Sub-processors' details to the Data Controller at least in a format that can be reproduced in writing (e.g. by e-mail). If the Data Controller submits no objection to the use of the new Sub-processors within 3 working days and in a format that can be reproduced in writing, the Data Controller shall be deemed to have accepted the changes to the list of Sub-processors.

5.2 **Data Processor and Sub-processors**. The Data Processor shall be the Data Controller's sole point of contact for all matters within the scope of this DPA and shall ensure that its Sub-processor complies with the binding requirements of this DPA as it applies to the Data Processor, including that any Sub-processor used by the Data Processor complies with the confidentiality obligation on substantially the same (and no less restrictive) terms as those set out in this DPA.

6. ACCESS AND CONFIDENTIALITY

6.1 **Access**. The Data Processor shall ensure that access to the Personal Data for which the Data Processor is responsible is only granted to persons who need such access in accordance with the Agreement and this DPA, and to the extent necessary for the performance of their respective duties.

6.2 **Confidentiality**. The Data Processor shall ensure that all employees of the Data Processor:

(a) understand the confidential nature of Personal Data;

(b) are aware of the applicable data protection legislation and of the obligations and duties arising from this DPA.

7. DATA TRANSFERS

7.1 **Data processing takes place in the European Economic Area.** The parties shall not transfer Personal Data to any country outside the EEA that does not comply with data protection requirements. As an exception, the Data Processor or a Sub-processor may transfer Personal Data outside the EEA, but only if they have a lawful basis for doing so and the data recipient (i) is located in a country that ensures an adequate level of protection for Personal Data; or (ii) has concluded a contract containing the European Commission's standard clauses for the transfer of Personal Data to processors located outside the EEA.

8. NOTIFICATIONS AND INFRINGEMENTS

8.1 **Notifications to the Data Controller.** The Data Processor shall immediately notify the Data Controller, if the Data Processor:

8.1.1 receives an official enquiry or request relating to Personal Data processed under this DPA, unless the law prohibits the Data Processor to provide such notification;

8.1.2 receives a request from a third party, including a Data Subject, for the disclosure of Personal Data or information relating to the processing of Personal Data;

8.1.3 becomes aware or reasonably suspects that a Personal Data breach has occurred in the Data Processor's systems. The Data Processor shall generally notify of any Personal Data

breach without undue delay but not later than within forty-eight (48) hours of becoming aware of the breach. If all of the information required by this DPA and applicable legislation has not yet been obtained, the Data Processor shall provide the information available and shall update the notification to the Data Controller as soon as possible.

8.2 **Personal data breaches within the Data Processor's area of responsibility**. In the event of a Personal Data breach in the Data Processor's systems/in the Data Processor's area of responsibility, the Data Processor shall take reasonable remedial action without undue delay, including by notifying the Data Controller of the cause of the breach, conducting an investigation and, upon the Data Controller's request, submitting a report and proposals for remedial action.

8.3 **Cooperation in case of a personal data breach**. The Data Processor and the Data Controller shall cooperate to develop and implement a response plan for the event of a personal data breach. The Parties shall make all reasonable efforts to mitigate the effects of the Personal Data breach.

8.4 **Information on Personal Data breaches.** The Data Processor shall, without undue delay, provide the Data Controller the information on a Personal Data breach as required under Article 33(3) or Article 34(3) of the GDPR, if such information can be obtained from the Data Processor's and/or its Sub-processors' systems and is not directly available to the Data Controller.

9. SECURITY REQUIREMENTS

9.1 Data security and other measures

9.1.1 The Data Processor shall implement the technical, physical (e.g. locked storage of Personal Data, etc.) and organisational measures (confidentiality agreements with staff) needed to ensure the security of Personal Data processing.

9.1.2 When processing Personal Data, the Data Processor shall comply with the requirements of ISO 27001:2013 (Information Security Management System, ISMS) or equivalent requirements.

9.2 **Security audit.** Once a year, the Data Processor shall make available to the Data Controller all the information and shall allow the Data Controller or an auditor authorised by the Data Controller to carry out audits or checks necessary to verify compliance with the obligations laid down in this DPA, and shall provide assistance therefor. To exercise the right to audit, the Data Controller shall coordinate the time of the audit (with a minimum of 30 days' prior notice) and the scope of the audit with the data Processor. The Data Processor has the right to require the conclusion of a confidentiality agreement. Information disclosed to the Data Controller or its authorised representative in the course of an audit shall be confidential unless the information has been made publicly available by the Data Processor or can be retrieved from public registers. Information obtained in the course of an audit may not be used for any purpose other than performing the audit. Unless otherwise agreed in writing, the Data Controller shall be responsible for its authorised representative's compliance with the confidentiality obligation. The costs of an audit, including any direct costs incurred by the Data Processor, shall be covered by the Data Controller in accordance with the applicable price list.

10. LIABILITY

10.1 **Liability**. The Parties acknowledge and accept that each Party is responsible for its own processing of Personal Data. Directo's liability to the Client is limited in accordance with

the provisions of the Agreement, taking into account the applicable data protection legislation and the circumstances and scope of Personal Data processing.

11. TERMINATION

11.1 **Upon termination of the Agreement**, the Data Processor shall either return or destroy the Data Controller's Personal Data upon the Data Controller's request and within a reasonable period of time in accordance with the Agreement. The Data Processor shall not destroy or cease to process Personal Data which the Data Processor is required to process under the law.

11.2 **Right to terminate the Agreement upon refusal to use a substantial Sub-processor.** The Data Processor shall have the right to terminate the Agreement and this DPA immediately and without notice, if the Data Controller prohibits the use of a Sub-processor whose work is essential for the Data Processor's operations.

12. MISCELLANEOUS

12.1 **Invalid provisions**. The invalidity of any of the provisions of the DPA or a part thereof shall not affect the validity, lawfulness or enforceability of all the other provisions. If any provision of the DPA or a part thereof is invalidated, the Parties shall use their best endeavours to replace such provision or a part thereof by a provision which is similar in substance and intent, is lawful and follows the objectives of the DPA.

12.2 **Applicable law**. This DPA and any documents relating thereto are governed by and shall be interpreted in accordance with the laws of the Republic of Estonia.

12.3 **Jurisdiction**. Any disagreement arising from this DPA will be settled by negotiations. If no agreement is reached, the dispute will be settled in the Harju County Court.

12.4 **Headings**. The headings of the DPA have no legal force and are only intended to facilitate the reading of the DPA.