Deventura Data Processing Addendum (DPA)

Version: 1 July 2025

1. BACKGROUND AND PURPOSE

1.1 This Data Processing Addendum and its appendices ("**DPA**") are an integral part of the Deventura terms of service or separate service agreement, as the case may be (the "**Main Agreement**") in which the Processor undertakes to provide SaaS services (the "**Service**").

1.2 When used in this DPA, "**Processor**" shall refer to Deventura AB, and "**Controller**" shall refer to the commercial customer purchasing the Service. This DPA applies when the Customer renews or purchases a Service.

1.3 In the event of inconsistency between the Main Agreement and the DPA, the Main Agreement shall generally prevail, however this DPA shall prevail with respect to those terms and issues relating particularly to Processing of Personal Data.

1.4 In addition to the remuneration stipulated in the Main Agreement the Processor shall be entitled to reasonable and evidenced costs directly attributable to the obligations in section 4.11, which may be considered to be in addition and unreasonable to what is required in the Applicable Data Protection Law or where the Controller places higher or increased requirements for handling and control than those stipulated in Applicable Data Protection Law. This additional remuneration shall be based on an hourly rate of EUR 250 per hour.

2. DEFINITIONS

2.1 Except as set forth herein, words, abbreviations and expressions shall have the meaning as ascribed to them in the Main Agreement, unless the context requires otherwise, or it is explicitly stated below:

"**Applicable Data Protection Law**": the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the Processing of Personal data applicable in the country in which the Controller is established and/or applicable in the jurisdiction in which the Processor or any Sub-processors are established;

"**EEA**": The European Economic Area;

"**GDPR**": The European Parliament and the Council Regulation (EU) no 2016/679;

"**Personal Data**", "**Special Categories of Data**", "**Process/Processing**", "**Controller**", "**Processor**", "**Data Subject**" and "**Supervisory Authority**" shall have the same meaning as in GDPR;

"**Portal**": the Deventura portal to which the Controller has access;

"**Sub-processor**": any processor (subcontractor) engaged by the Processor who Processes Personal Data on behalf of the Processor in accordance with the instructions provided, the terms of this DPA and the terms of the written subcontract;

"**Standard Contractual Clauses**": the Standard Contractual Clauses for the transfer of Personal Data to data Processors established in third countries, laid down by the EU Commission (COMMISSION IMPLEMENTING DECISION (EU) 2021/914 as of 4 June 2021); and

"**Technical and Organisational Security Measures**" or "**TOMs"**: measures aiming at protecting Personal Data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the Processing involves the transmission of data over a network, and against all other unlawful forms of Processing.

3. CONTROLLER – PROCESSOR

3.1 The Controller determines the purpose and the means of the processing of Personal Data and is therefore defined as a data Controller. Consequently, the Controller is obligated to ensure that the processing of Personal Data under the Main Agreement is always in compliance with a legal basis in accordance with Applicable Data Protection Laws.

3.2 As set out in the Main Agreement, the Processor has undertaken to assist the Controller in processing Personal Data and is therefore deemed a data Processor.

4. GENERAL OBLIGATIONS OF THE PROCESSOR

4.1 The Processor shall, when Processing Personal Data in the context of the Main Agreement, comply with Applicable Data Protection Law (as amended or replaced from time to time).

4.2 The Processor shall further adhere to those routines and instructions for such Processing as communicated in writing by the Controller.

4.3 The Processor shall not Process Personal Data given access to or generated in the context of the Main Agreement for any purpose other than to perform its obligations pursuant to the Main Agreement. Accordingly, the Processor shall not use such Personal Data for its own purposes, except where Personal Data has first been irrevocably anonymized so that it no longer qualifies as Personal Data.

4.4 Without limiting the generality of the foregoing, the Processor does not have the right to process Personal Data in other categories or in any other way, for purposes or according to instructions other than those that follow from the Main Agreement or are specified in **Appendix 1** to this DPA. Should the Processor find that there are insufficient instructions to fulfil the assignment under the DPA or in the Main Agreement, the Processor must inform the Controller without undue delay. Should performance under the Main Agreement be affected the Processor shall inform the Controller thereof and await further instructions.

4.5 The Processor shall implement and maintain throughout the term appropriate Technical and Organisational Security Measures (TOMs) to ensure a level of security as required by Article 32 GDPR, to protect the Personal Data against unauthorized or unlawful Processing and against accidental or unlawful destruction or accidental loss, damage, alteration, unauthorized disclosure or access. In considering the appropriateness of the TOMs, Processor shall take into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and

freedoms of natural persons. The TOMs are subject to technical progress and further development. In this respect, the Processor is permitted to implement alternative adequate measures, as long as security is maintained. The latest TOMs shall be available on the Processor's website.

4.6 The Controller warrants that only personnel or contractors who require access to Personal Data to perform their work duties will have access to the Personal Data and that these personnel are subject to confidentiality undertakings regarding the Personal Data. The Processor shall only allow access to the Personal Data to personnel on a need-to-know basis and must always ensure that such personnel are bound by adequate confidentiality undertakings and are informed and aware of applicable data protection laws. The Processor must also ensure that the personnel only Processes Personal Data as instructed by the Controller unless other Processing is required by law.

4.7 The Controller retains the formal control of, and all ownership and rights to, the Personal Data Processed by the Processor and any Sub-processors hereunder. The Controller may require to receive the Personal Data at any time, and the Processor shall meet such request without undue delay in a suitable format.

4.8 The Processor shall inform the Controller as soon as possible in the event of attempted or successful unauthorised or unlawful access, destruction or change of Personal Data.

4.9 If the Data Subject, the Supervisory Authority or other third-party requests information from the Processor regarding Personal Data the Processor shall promptly refer such party to the Controller. The Processor is not entitled to disclose Personal Data or other information on the Processing without the explicit instruction from the Controller or if the disclosure is required by law.

4.10 The Processor shall inform the Controller of any contact with the Supervisory Authority without undue delay if the contact concerns or may affect the Processor's Processing of Personal Data. This undertaking shall only apply on Processing of Personal Data attributable to the Customer or which can affect the Customer. The Processor is not entitled to represent or speak on behalf of the Controller in relation to the Supervisory Authority.

4.11 Other than to the extent covered by the instructions from the Controller the Processor must not disclose Personal Data to third-parties, change the purpose or the means of the Processing, take measures or series of measures such as collect, record, process, change, block, erase or destroy Personal Data, multiply the data in the Controllers database or compile or merge the Personal Data.

4.12 The Data Subject has a right to request through the Controller a record of its Personal Data, data portability, request correction, blocking or potential erasure of the Personal Data that is covered by the DPA. Once the Controller has – to the extent necessary – confirmed the identity of the Data Subject who has made a request, the Processor shall be required to assist the Controller to such extent that these rights can be provided. The Processor is also obligated to assist the Controller in its duties on security in relation to the Processing, contact with the Supervisory Authority and potential breach, impact assessment regarding data protection and

prior consultation with the Supervisory Authority regarding the categories of Processing and the information available to the Processor.

4.13 All Processing must be made confidential, which means that the Processor, its employees and Sub-processors must not disclose any information to third-parties without the Controller's prior consent. The confidentiality undertaking does not apply if the information has been made available to the Processing on other ways than the fulfilment of the DPA or if it is publicly known. The confidentiality undertaking shall survive termination of the DPA.

4.14 Upon termination of the Main Agreement, the Processor must irrevocably anonymise all Personal Data that is stored or Processed by the Processor under the Main Agreement in such way that it is not possible to recreate, or instead return or erase all Personal Data as instructed by the Controller. The Processor must also delete all copies of Personal Data unless applicable law requires that the data is stored. Return or information on deletion of the Personal Data must be provided to the Controller within 90 days following termination of the Main Agreement, unless extended paid storage of Personal Data has been agreed upon (in which case this DPA shall continue to apply). Backups are gradually deleted during a fourteen-day period.

5. USE OF SUB-PROCESSORS

5.1 The Processor is hereby granted a general authorisation from the Controller to engage Sub-Processors, as long as the Processor ensures that Articles 28.2 and 28.4 of the GDPR are met and that the Sub-Processors provide adequate guarantees to implement appropriate TOMs to fulfil the requirement of this DPA and the Applicable Data Protection Law. Processor shall ensure that all Sub-Processors are bound by written agreements which impose corresponding obligations when processing Personal Data on behalf of Controller. Processor shall maintain an up-to-date list of Sub-processors on Processor's website. The Processor shall remain responsible towards Controller for any processing carried out by a Sub-Processor.

5.2 Processor is entitled to engage new Sub-Processors and to replace existing Sub-Processors. In this case, Processor undertakes to verify the new Sub-Processor's capacity and ability to meet its obligations in accordance with the Applicable Data Protection Law. The Processor shall inform the Controller - e.g. by e-mail, or within the Processor's SaaS platform - if the Processor intends to engage additional Sub-Processors or to replace Sub-Processors, and shall notify of a new Sub-Processor, which type of data and categories of Data Subjects are being processed and where the Personal Data will be stored. Controller is entitled within fourteen (14) days of the notice to object to the new Sub-Processor in writing. If Controller does not object within the given timeframe, the new Sub-Processor shall be deemed accepted. If Controller makes a legitimate objection and Processor does not accept the objection against Sub-Processor in question, the Processor shall be entitled to at its own discretion, either perform the service without the intended change in Sub-Processor, or, if the performance of the service without the intended change is unreasonable for the Processor, terminate the Main Agreement, including this DPA, by giving thirty (30) days written notice from Processor's receipt of Controller's objection.

5.3 Upon request from the Controller, the Processor shall provide Controller with a correct and up-to-date list of the Sub-Processors assigned to process Personal Data on behalf of

Controller, and the geographic location of the processing. Processor can fulfil the obligations under this paragraph by referring the Controller to the list maintained on the Processor's website or by sending the latest list to the Customer by email.

5.4 The Processor will impose equivalent data protection terms on the Sub-Processors that provide at least the same level of protection for Personal Data as those in this DPA, to the extent applicable to the nature of the services provided by such Sub-Processors. The Processor will remain responsible for each Sub-Processor's compliance with the obligations of this DPA and for any acts or omissions of such Sub-Processor that cause the Processor to breach any of its obligations under this DPA and the Applicable Data Protection Laws.

6. INTERNATIONAL DATA TRANSFER

6.1 In the event that Processor and/or Sub-Processors transfer Personal Data to a location outside of the EU/EEA or the UK, Processor and/or Sub-Processor shall ensure that such transfer complies with the Applicable Data Protection Laws. Under the terms of this DPA, such requirements in relation to certain countries will if suitable be fulfilled by entering into the EU's standard contractual clauses for the transfer of Personal Data to Processors established in third countries (Commission Implementing Decision (EU) 2021/914 of 4 June 2021), or – in the case of a third-country transfer outside the UK – the International Data Transfer Addendum to the EU SCCs, issued by the Information Commissioner and laid before Parliament in accordance with s.119A of the Data Protection Act 2018, or other applicable security mechanisms pursuant to sections 44 et seq. GDPR in order to secure the transfer. Processor is required to keep Controller informed of the grounds for transfer.

7. AUDITS

7.1 The Controller is entitled to verify, by himself or through an independent third party (who must not be a competitor of Processor) that the Processor complies with the terms of this DPA and Article 28(3) of the GDPR and the instructions provided by the Controller. After thirty (30) days' prior notification, Processor shall reasonably provide Controller with the assistance and provide the documentation required to carry out such control. Checks shall be made during the Processors normal office hours and shall be conducted so that the Processors operations are not disturbed. The cost of an audit shall be covered by the Controller.

7.2 The Processor may make the inspection conditional upon the signing of a confidentiality agreement to protect the data of other customers and information about Processor's TOMs, as well as Processor's business and trade secrets. The Controller shall ensure its personnel conducting such audit are subject to adequate secrecy obligations.

7.3 If the Parties agree that an audit is to be performed by external auditors, such external auditor is to be appointed by the Controller and approved by the Processor. Upon security audits performed by an external auditor, both Parties shall be entitled to receive a copy of the audit report.

7.4 If the audit reveals non-compliance with the DPA, the Processor shall notify the Controller immediately and without undue delay remedy such non-compliance.

7.5 The Processor shall procure that the Controller is similarly entitled to conduct audits in respect to the Sub-processors.

8. DATA BREACHES

8.1 The Controller must be notified without undue delay after a Personal Data Breach comes to the Processor knowledge. If the Processor can demonstrate that the Personal Data Breach is unlikely to result in a risk to the rights and freedoms of Data Subjects the Controller does not have to be notified.

8.2 The notification referred to in section 8.1 must at least (if relevant):

a) describe the Personal Data Breach including the categories and amount of the Data concerned and where feasible, names of the Data Subjects concerned;

b) provide information on the date and time of the Personal Data Breach;

c) describe the likely consequences and potential risk to the Data Subjects due to the Personal Data Breach;

d) describe the measures proposed or taken to address the data breach, including to re-establish the situation and to prevent the recurrence of the Data Breach;

e) include any other information required in order for the Controller to comply with Applicable Data Protection Law.

8.3 The Controller is responsible for notifying the relevant Supervisory Authority about the Personal Data Breach when applicable.

8.4 The Processor shall document any Personal Data Breaches. This documentation must enable the Supervisory Authority to verify compliance with this DPA, including without limitation the TOMs and Applicable Data Protection Law. The documentation shall only include information necessary for that purpose.

9. LIABILITY AND LIMITATION OF LIABILITY

9.1 Unless otherwise agreed in the Main Agreement, a Party in breach of this DPA shall be liable for documented and relevant damages suffered by the other Party. However, neither party shall be liable for indirect or consequential damages. The liability under the DPA for damages not covered by section 11 below shall be limited to the amount paid by the Controller under the Main Agreement during the 12 months preceding such breach.

9.2 The limitation of liability set out in section 9.1 shall not apply if the breach is caused by intent or gross negligence.

10. LIABILITY FOR DAMAGES IN CONNECTION WITH THE PROCESSING

10.1 In the event of compensation for damage in connection with Processing, through a judgment given or settlement, to be paid to a Data Subject due to an infringement of a provision in the

DPA, Instructions and/or applicable provision in Data Protection Law, Article 82 of the GDPR shall apply.

10.2 Fines pursuant to Article 83 of the GDPR or supplementary provisions under local law to the EU's data protection regulation shall be borne by the Party to the DPA named as recipient of such sanctions.

10.3 If either party becomes aware of circumstances that could be detrimental to the other party, the first party shall immediately inform the other party of this and work actively with the other party to prevent and minimise the damage or loss.

10.4 Regardless of the content of the Main Agreement, items 10.1 and 10.2 of this DPA take precedence to other rules on the distribution between the Parties of claims among themselves as far as the processing is concerned.

11. GENERAL NOTIFICATIONS

11.1 The Processor shall without undue delay notify the Controller in writing of:

(i) any request or complaint from a Data Subject. The Processor shall not respond to that request or complaint unless it has been authorized to do so. Responding to claims or complaints from a Data subject is thus the responsibility of the Controller; and

(ii) any request from any Supervisory Authority requiring access to or information regarding the Processor's and/or the Sub-processor' Processing of Personal Data covered by this DPA, including any legally binding request for disclosure of the Personal Data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation.

12. AMENDMENTS

12.1 The Parties may amend the DPA to such extent necessary to comply with Applicable Data Protection Law or to enable the Processing. Amendments enter into force within 30 days following written notification (email to suffice) to the other Party.

12.2 The Controller must be notified if the Service is changed in such way that new functionality is included which may result in other categories of Processing.

13. TERM AND TERMINATION

13.1 This DPA will stay in force as long as the Processor Processes or has access to Personal Data on behalf of the Controller in the context of the Main Agreement.

13.2 Upon expiration or termination, the Processor and any Sub-processors shall, at the choice of the Controller, return all the Personal Data and the copies thereof to the Controller or shall destroy all the Personal Data and certify to the Controller that it has done so, unless legislation imposed upon the Processor prevents it from returning or destroying all or part of the Personal

Data. In that case, the Processor warrants that it will guarantee the confidentiality of the Personal Data and will not actively Process the Personal Data anymore.

14. GOVERNING LAW AND LEGAL VENUE

14.1 Governing law and dispute resolution shall follow as set forth in the Main Agreement.

Appendix 1: Instructions on Processing covered by the DPA

Purpose	Categories of Personal Data	Type of Processing	Legal basis
To provide the Portal and the User Account.	• Name • Contact details (e.g. address, e-mail and phone number) • Position at employer or job title	• The creation and providing of the User Account. • Requesting, receiving and storing the Personal Data (as determined and decided by the Controller	• Performance of the user account agreement for use of the Portal. • Consent for Special Categories of Personal Data (in form of opt-in from end-users)
To prevent abuse of a service or to prevent and investigate crimes against the company.	• User-generated data (e.g. access and error logs).	• Prevent unauthorised use of the Portal. • Protecting and improving Deventura's IT environment against attacks and intrusion.	• Compliance with legal obligation (if any) or legitimate interest. If there is no legal obligation the process is still necessary to meet our legitimate interest in preventing abuse of our services or preventing and investigating crimes against us.
To deliver an individually adopted experience of the Portal.	• Name • IP address • Language settings • User-generated data (e.g. reading history)	• Simplification of your use of the Portal (e.g. by saving language selection and identifying device type).	• Performance of the user account agreement for use of the Portal.
To handle customer service issues.	• Name • E-mail address		• Performance of the user account agreement for use of the Portal.
To send newsletters and other periodical messages.	• E-mail address	• Receive news about Us and our Services. • Receive information about the operating system.	• Consent (in form of opt-in).