Appendix 4 - Data Processing Agreement

PARTIES

1. Indivd AB, org. nr 559169-7072, Bankgatan 8, 852 31, Sundsvall (“Indivd” or “ Processor”); and
2. Customer, who’s name, company reg. no and address is stated in the Order Form (“Customer” or ” Controller”);

Indivd and Customer is each referred to as a “Party” and jointly as the “Parties”.

BACKGROUND

A) Indivd and the Customer have entered into a customer agreement (the “ Agreement”).

B) When performing the contractual obligations in the Agreement, it is anticipated that Indivd may Process Personal Data on behalf of the Customer. In doing so, Indivd acts as a Processor for Customer, who acts as a Controller. This Data Processing Agreement regulates the terms and conditions for such Processing.

C) If any provision of the Agreement conflicts with the terms of this Data Processing Agreement, the terms of this Data Processing Agreement shall take precedence to the extent its terms provide greater protection for Personal Data.

1. DEFINITIONS

In this Data Processing Agreement the following terms have the following meanings:

“**Processing**“, “ **Controller**“, “**Personal Data**“, “ **Processor**“, “**Personal Data**

Personal Data Breach“, and “**Data Subject**” shall have the same meaning as in 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 and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (“**GDPR**“);

“**Data Processing Agreement**” means this Data Processing Agreement and its appendices;

"**Applicable Laws**" means laws and regulations under EU law and relevant Member State laws that from time to time apply to the Parties (including Applicable Data Protection Laws);

"**Applicable Data Protection Laws**" means from time to time applicable legislation and regulations, including regulations issued by relevant supervisory authorities, protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the Processing of Personal Data, including in particular the GDPR; and

"Third Country" means a country which is not a member of the European Union (EU) or the European Economic Area (EEA).

When the context requires it, singular shall include plural, and vice versa.

2. GENERAL OBLIGATIONS FOR THE CUSTOMER

2.1. The Customer shall in its capacity as Controller ensure the compliance with the Applicable Data Protection Laws.

2.2 The Customer shall in accordance with Section 30 (1) in the GDPR provide the Processor records of processing activities that are required in order for the Processor to be able to comply with its obligation to maintain a record of processing activities in accordance with Section 30 (2) in the GDPR.

2.3 The Customer shall appoint a data protection officer and/or a representative if required by the Applicable Data Protection Laws and, where necessary, provide the Processor with the contact details to such person.

2.4 By entering into this Data Processing Agreement, the Customer confirms that the technical and organizational measures stated in Appendix 2 are considered adequate and sufficient in order to protect the Personal Data covered by this Data Processing Agreement and that the Processor gives sufficient guarantees in accordance with Section 28 (1) in the GDPR.

3. INSTRUCTIONS

3.1 The Controller instructs the Processor to process Personal Data only on behalf of the Controller and in accordance with the instructions by the Controller, as set out in this Data Processing Agreement and the Agreement. The Controller ensures that the instructions comply with the Applicable Data Protections Laws.

3.2 If the Controller leaves instructions that go beyond what is stated in this Data Processing Agreement and the Agreement, the following shall apply. In the event the implementation of actions required by the instructions entail costs for the Processor, the Processor shall inform the Controller thereof and

provide an explanation of why the actions entail costs. The Processor shall be required to implement the measures only on condition that the Controller confirms that the Controller shall bear the costs of the actions. The instructions must be submitted in writing.

3.3 The Processor shall notify the Controller if the Processor considers that an instruction regarding the Processing of Personal Data given by the Controller would be in a breach of Applicable Laws ("Challenged Instruction"). The Processor will not in such case be obliged to follow the Challenged Instruction unless the Controller maintains it and assumes full responsibility for the Challenged Instruction. In such case, the Processor shall take the measures required by the Controller provided that the measures do not concern (i) implementation of technical and organizational measures; (ii) Data Subject's rights; or (iii) appointing Sub-Processors. In case of disagreement, the Processor is entitled to seek guidance from a relevant supervisory authority. If such authority considers that the proposed measures are lawful, the Processor shall take them, in which case Section 3.2 applies with regard to the costs for such measures. The Processor's obligation to notify the Controller according the first sentence in this Section shall not apply to the extent the Processor is prevented from doing so in accordance with Applicable Laws.

4. THE GENERAL OBLIGATIONS OF THE PROCESSOR

4.1 The Processor will Process Personal Data only in accordance with the written instructions issued by the Controller by way of this Data Processing Agreement and the Agreement.

4.2 Notwithstanding what is stated in Section 4.1 above, the Processor may Process the Personal Data to the extent it is necessary for the Processor in order to comply with legal requirements under Applicable Laws to which the Processor is subject. If so, the Processor shall inform the Controller of that legal requirement before the Processing, unless Applicable Laws prohibit the Processor from providing this information.

4.3 The Processor shall upon request by the Controller assist the Controller by providing with necessary information that the Processor has access to, in order for the Controller to be able to comply with its obligations to perform a data protection impact assessment in accordance with Section 35 GDPR and consult the supervisory authority in accordance with Section 36 of the GDPR, regarding the Processing of Personal Data that is conducted in accordance with this Data Processing Agreement. The Processor is entitled to compensation for the costs from the Controller for such measures. The

Processor's obligation to assist the Controller is limited to such information that the Controller otherwise has no access to.

5. SECURITY MEASURES

5.1 The obligation to implement technical and organisational measures to protect the Personal Data

5.1.1 The Processor shall implement appropriate technical and organisational measures in accordance what is provided in Appendix 2 to protect and safeguard Personal Data that is processed against Personal Data Breaches. The Processor shall have a right to change these measures on the condition that the changes do not result in a lower level of protection of the Personal Data and at least reach the level of protection that follows from the Applicable Data Protection Laws. In case the Controller requests that the Processor shall take technical and organizational measures that go beyond what is stated above in this Section 5.1.1, Section 3.2 shall apply to the cost allocation for such measures.

5.2 Access to Personal Data etc.

5.2.1 The Processor shall ensure that access to the Personal Data is limited to those employees of the Processor who need access to the Personal Data in order for the Processor to fulfill its obligations under this Data Processing Agreement and the Agreement as well as in order to perform their job duties.

5.2.2 The Processor shall ensure that all employees authorized to access and Process the Personal Data have committed themselves to confidentiality.

5.3 Personal Data Breach

5.3.1 In the event of a Personal Data Breach at the Processor, the Processor shall notify the Controller about the Personal Data Breach without undue delay after when the Processor became aware of such Personal Data Breach. Moreover, the Processor shall provide such information that follows from the information obligation in Section 33 (3) in the GDPR, that the Processor has access to and that the Controller cannot access by other means.

5.3.2 The notification to the Controller shall include the following Information:

5.3.2.1 a description of the nature of the Personal Data Breach including the categories and number of Data Subjects concerned and the categories and number of Personal Data records concerned;

5.3.2.2 the likely consequences of the Personal Data Breach; and

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

5.3.3 Where, and in so far as, it is not possible for the Processor to provide the above information in Section 5.3.2 above at the same time, the information may be provided in phases (without undue delay).

6. ACCESS TO INFORMATION

6.1 The Processor shall document the measures that the Processor has taken in order to comply with its obligations in this Data Processing Agreement. The Controller shall have a right to receive a copy of the latest version of such documentation.

6.2 Upon the Controller's request, the Processor shall show that is meets the requirements under Article 28 of the GDPR. The Parties agree that this may be done by providing a report prepared in accordance with standards that has been prepared by a third party ("**Report**").

6.3 If further inspection measures than those stated above in Section 6.2 are required by the Applicable Data Protections Laws, the Controller may require an inspection at the site ("**Site Inspection**"). The following terms apply for Site Inspections:

(i) Site Inspections are limited to the resources and personnel at the Processor that are involved in the Processing of Personal Data covered by this Data Processing Agreement. This means that Site Inspections may not under any circumstances comprise other information regarding the Processor's business that is irrelevant for the Processors Processing of Personal Data on behalf of the Controller;

(ii) Site Inspections may not be conducted more often than once a year, unless otherwise required by the Applicable Data Protections Laws or as a consequence of a substantial Personal Data Breach that has affected the Personal Data that is covered by this Data Processing Agreement;

(iii) Site Inspections shall be conducted under office hours and in a manner that affects the Processor's business in the least possible way and in accordance with the Processor's security policies;

(iv) the Controller shall bear the costs that relate to the Site Inspections and preparing reports of the findings during Site Inspections;

(v) Site Inspection shall, when possible, be conducted by a third party chosen by both Parties. The Controller shall ensure that such third party undertakes a confidentiality undertaking regarding all information that the third party may get access to during the inspection and is liable to the

Processor for any breaches of the confidentiality undertaking by the third party. All costs that relate to an inspection shall be borne by the Controller, including any costs that the Processor has for the cooperation in such inspection.

(vi) Site Inspection shall be preceded by at least thirty (30) days written notice. Reports and reports from Site Inspections are considered the Processor's confidential information and shall not be disclosed to third parties unless required by Applicable Laws or if the Processor has consented thereto in writing.

7. USE OF SUB PROCESSORS

7.1 The Processor may engage outside sub-contractors, consultants or other third parties to Process Personal Data on behalf of the Controller ("Sub-Processors"). Any data processing agreement with a Sub-Processor shall impose corresponding and not less restrictive data protection obligations on the Sub-Processor than what follows from this Data Processing Agreement. The Sub-Processors listed in Appendix 1 at the time when the Agreement is entered into has been approved by Controller.

7.2 The Processor shall, in the event the Processor engages a Sub-Processor without undue delay provide the Controller with information corresponding to that stated in Appendix 1 in writing.

7.3 The Controller has a right to, with providing a cause within five (5) working days after the Processor has informed the Controller in writing about engaging a Sub-Processor, object against the Processor engaging the Sub-Processor. If the Controller has not objected within the stated time, the proposed Sub-Processor is deemed accepted. If the Controller objects to the Sub-Processor, the Processor has a right to choose one of the following alternatives: (a) refrain from engaging the Sub-Processor to process Personal Data covered by this Data Processing Agreement (b) take measures that reasonably eliminate the reason for the Controller's objection; or (c) temporarily or permanently cease to provide the part of the service/services that entail Processing of Personal Data by the Sub-Processor at hand. If none of these alternatives are feasible and the Controller maintains its objection after thirty (30) days has passed after the objection was made, each Party has a right to by giving a reasonable notice period terminate that part of the service/services that entails Processing of Personal Data by the Sub-Processor at hand.

7.4 The Processor shall, in addition to the information stated in Section 7.2 above, upon the Controller's request, provide information regarding the measures that have been taken to ensure that the Sub-Processor gives

sufficient guarantees to implement technical and organisational measures in a way that complies with the requirements in Applicable Data Protection Laws.

7.5 The Processor is liable towards the Controller for the Processing of Personal Data by the Sub-Processors covered by this Data Processing Agreement in accordance with Applicable Data Protection Laws.

8. LIABILITY

The terms and conditions regarding liability in the Agreement shall apply this Data Processing Agreement.

Administrative fines that have been imposed on one Party pursuant to Art. 83 of the GDPR, or Chapter 6 Section 2 of the supplementary Data Protection Act (2018:218) shall be borne by the Party on which such fines have been imposed.

9. DATA SUBJECTS' RIGHTS

9.1 The Controller shall be liable to assess if a Data Subject request is legitimate or not and provide the Processor with instructions regarding the scope of support that is required.

9.2 The Processor shall without undue delay inform the Controller about complaints and other notices from Data Subjects exercising their rights. However, the Processor shall not, unless the Controller has given the Processor sufficient instructions thereof, communicate with the Data Subject.

9.3 The Controller is responsible for handling in connection with the Data Subject exercising its rights under Applicable Data Protection Legislation.

9.4 The Processor shall upon the request assist the Controller with the following appropriate technical and organizational measures in connection with a Data Subject exercising its rights under Chapter III in the GDPR:

(i) In connection with a request of information the Processor shall provide the Controller with such information that is covered by Sections 13 and 14 in the GDPR to the extent such information is available for the Processor and the Controller does not have access to such information.

(ii) In connection with a request of right of access the Processor shall provide the Controller with such information that is covered by Section 15 in the GDPR to the extent such information is available for the Processor and the Controller does not have access to such information.

(iii) In connection with a request of rectification (Section 16 in the GDPR), erasure (Section 17 in the GDPR), restriction of processing (Section 18

in the GDPR), and data portability (Section 20 in the GDPR), the Processor shall, to the extent the Controller cannot take the measures requested by the Data Subject(s)assist the Controller to take such measures.

(iv) The Processor shall, on instructions for the Controller, notify the Sub-Processors that Process Personal Data covered by the request by the Data Subject to rectify, erase or restrict the processing (Section 19 in the GDPR) that such request has been made. The Controller undertakes to inform other recipients.

(v) In relation to the Data Subject's right to object processing in Section 21-22 in the GDPR, the Controller shall assess whether the objection is legitimate and how it is to be handled. In the event the Controller wishes to be assisted by the Processor, the Controller shall issue further instructions, whereby the routines described in Section 3.2 shall apply to the Processor's right to compensation for costs.

9.5 In the event the Controller requests that the Processor shall take technical and organisational measures in addition to what is stated in Section 5.1.1 for the purpose of handling the Data Subject's rights under this Section 9, the Section 3.2 shall apply to the costs for such measures.

9.6 Notwithstanding what is stated above in Section 9.5, the Processor is entitled to compensation for reasonable expenses due to a Data Subject exercising its rights as set out above.

10. RETURN OF PERSONAL DATA

10.1 Upon termination of the Agreement, the Processor shall return (and/or upon the Controller's written request in a secure and irreversible way delete or anonymise) all Personal Data which belongs to the Controller that the Processor and or any Sub-Processors have in its possession or control. This applies unless the Processor is required under Applicable Laws to continue to store the Personal Data. Unless the Controller has within thirty (30) days after the termination of the Customer Agreement instructed the Processor that the Controller wishes that the Processor returns or in secure way deletes the Personal Data, the Processor shall, provided that the Processor is not required to store Personal Data under Applicable Laws, without undue delay ensure that the Personal Data is deleted in a secure way.

11. TRANSFER AND PROCESSING OF PERSONAL DATA IN A THIRD COUNTRY

11.1 The Processor may transfer Personal Data processed on behalf of the Controller to a Third Country, provided that:

11.1.1 the Third Country provides an adequate level of protection for Personal Data in accordance with an adequacy decision issued by the EU Commission that covers the Processing of Personal Data;

11.1.2 the Processor ensures that there are appropriate safeguards in place in accordance with Applicable Data Protection Laws, e.g. standard data protection clauses adopted by the EU Commission under Applicable Data Protection Laws, covering the transfer and Processing of Personal Data; or

11.1.3 other exception exists under Applicable Data Processing Laws that covers the Processing of Personal Data.

11.2 For the avoidance of doubt, Personal Data may not be transferred to any Third Countries unless one of the conditions above in Section 11.1 applies.

12. TERM AND TERMINATION

This Data Processing Agreement will enter into force on the Agreement Date and is valid during the term of the Agreement or the longer period of time that the Processor or any Sub-Processor engaged by the Processor Processes Personal Data on behalf of the Controller.

14. AMENDMENTS

Additions and amendments to this Data Processing Agreement shall be in writing and duly signed by both Parties to be valid. Each Party may request amendments to this Data Processing Agreement that are justified by changes in Applicable Data Protection Laws.

15. APPLICABLE LAW

This Data Processing Agreement shall be governed by Swedish law, without the application of the choice of law rules, to the extent Applicable Data Protection Laws do not prescribe otherwise.

16. DISPUTES

Disputes arising out of this Data Processing Agreement shall be solved in Sweden to the extent Applicable Data Protection Laws do not stipulate otherwise.

APPENDIX 1

Categories of Data Subjects
Visitors in Customer Premises (as defined in the Order Form).

Categories of Personal Data
Personal data from People Counters.

Purpose(s) of the Processing
People Counter:

To gather personal data for anonymization and then analyze anonymized and aggregated data at group level in order to understand visitor behaviors and optimize the location.

Quality Assurance:

To ensure the quality of the collected Personal Data by comparing automated people counts with manual observations.

Processing Operations
Personal Data is anonymized, to be able to calculate statistics.

Location, and, where applicable, safeguard for third country transfers
Personal data is Processed in Europe.

Retention of Personal Data
People Counter:

The Personal Data is deleted instantly after Processing. Quality Assurance

Two (2)business days.

Contact details of the contact person at the Processor:
Fredrik Hammargården, privacy@indivd.com

SUB-PROCESSORS

Genesis Cloud GmbH Neuhauser Str. 17 80331 Munich Germany, contact@genesiscloud.com, Provide infrastructure for anonymization, hosting and creation of insights.

Categories of Data Subjects
Visitors in Customer Premises (as defined in the Order Form).

Categories of Personal Data
Personal Data from People Counters.

Processing Operations
People Counter (Standard and Premium)

Anonymization

Quality Assurance

Hosting

Location, and, where applicable, safeguard for third country transfer
The Personal Data will be Processed in Europe.

Retention of Personal Data
People Counter:

The Personal Data is deleted instantly after Processing.

Quality Assurance:

Two (2)business days.

APPENDIX 2

Technical and organisational measures

Anonymization
The following measures shall be implemented to address the anonymization of the personal data such as:

- use Indivd People Counter to anonymize personal data,
- personal data is never stored and,
- personal data is deleted instantly after processing.

Encryption
The following measures shall be implemented to address the encryption of the personal data:

- use secure code signing, symmetric encryption, asymmetric encryption and,
- provide security guidelines to the Processor to ensure they manage encryption of local network, people counter hardware, and transfer of personal data.

Confidentiality Of The Processing Systems And Of The Services
The following measures shall be implemented to address the confidentiality of the processing systems and of the Services:

- provide security guidelines to the Processor to ensure they manage confidentiality of local network, people counter hardware, and transfer of personal data,
- use access control mechanisms to prevent persons from gaining access to data processing systems with which personal data are processed or used without authorization,

- administer and monitor credentials with privileged access management (PAM),
- Data Breach Response Policy,
- ensure that data collected for different purposes can be processed separately.

Integrity Of The Processing Systems And Of The Services
The following measures shall be implemented to address the integrity of the processing systems and of the Services:

- provide security guidelines to the Processor to ensure they manage the integrity of the local network, people counter hardware, and transfer of personal data,
- protection by technical and organizational means regarding authorizations, protocols/logs including analyzing protocols, audits, automatic exclusion protocols, etc,
- Data Classification Policy,
- ensure that measures and activities are logged in a secure manner.

Availability Of The Processing Systems And Of The Services
The following measures shall be implemented to address the availability of the processing systems and of the Services:

- ensure that personal data are protected from accidental destruction or loss,

Resiliency Of The Processing Systems And Of The Services
The following measures shall be implemented to address the resiliency of the processing systems and of the Services:

- ensure that systems and services are designed in a way that they can handle punctual or constant high load of processing operations.

Ability to restore the availability and access to the personal data in a timely manner in the event of a physical or technical incident
The following measures shall be implemented to address the ability to restore the availability and access to the personal data in a timely manner in the event of a physical or technical incident:

- backup concept,
- cloud services.

Process For Regularly Testing, Assessing And Evaluating The Effectiveness Of Technical And Organizational Measures
The following measures shall be implemented to address the regularly

testing, assessing and evaluating of the effectiveness of technical and organizational measures:

- Information Security Policy
- Anonymization Policy,
- ensure development following Secure Software Development,
- use ISO/EIC 27001-27002 and ISO/EIC 27005 as frameworks for development,
- review by the data protection officer,
- external reviews, audits, certifications.