

Data Processing Agreement

This Data Processing Agreement (the "**DPA**") has been entered into between Customer (as stated in the Service Agreement) (the "**Data Controller**" or the "**Controller**"); and CatalystOne Engage AB AB, reg. no. 559035-7678, Kungsbron 21, 111 22 Stockholm, ("**CatalystOne**", the "**Data Processor**" or the "**Processor**"); hereinafter each referred to as a "**Party**" and collectively as the "**Parties**".

1. BACKGROUND

- 1.1. The Controller has entered into an agreement with the Processor regarding the Processor's provision of services (the "**Services**") to the Controller (the "**Service Agreement**").
- 1.2. The Service Agreement entails that the Processor in the capacity as Data Processor processes Personal Data for which the Controller is the Data Controller according to 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**"). This DPA governs the Processor's Processing of Personal Data on behalf of the Controller, as well as the integrity level to be maintained during the Processing.
- 1.3. With regards to processing of Personal Data, this DPA shall take precedence over the Service Agreement and its annexes, unless otherwise expressly stated below.

2. DEFINITIONS

The following terms used in this DPA shall have the following meaning:

"Data Protection Laws" - means the General Data Protection Regulation (EU) 2016/679 ("**GDPR**"), and the binding decisions and regulations of the relevant regulatory authority, as well as additional local adaptation and regulation regarding data protection in the applicable membership country.

"Applicable Foreign Law" - means the foreign law and the rules regarding processing of personal data that apply to companies and employees who reside outside of EU and the European Economic Area (EEA).

"Response Data" - means the data subject's responses to questions asked by the Company using the Service. Although stored separately, the Response Data remains linked to a data subject through their account with the Processor. Therefore, the Response Data qualifies as Personal Data until either it is deleted from the data subject's account or the link between the Response Data and the account is removed. Subsequent to these actions, the Response Data becomes anonymous and loses its status as Personal Data.

"Affiliates" – means all companies that from time to time are part of the Controller's organization;

"Controller" – means the entity which solely, or together with others, determines the purposes and means of the Processing of Personal Data ("**Data Controller**" shall have the same meaning);

"Data Subject" – means the identified or identifiable natural person to whom Personal Data relates;

"GDPR" – means EU Regulation 2016/679 on the protection of individuals with regard to the Processing of Personal Data and on the free flow of such data and the repealing of Directive 95/46/EG (the Data Protection Directive);

"Personal Data" – refers to any information relating to a Data Subject, wherein the Data Subject is identified directly or indirectly with reference to an identifier such as name, email, phone number, ip-adress, work role, team ownership or any other identifiable data the Controller provide the Processor of the Data Subject;

"Processing" – means any operation or set of operations which is performed upon Personal Data, whether or not by automatic means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction ("Process", "Processes" and "Processed" shall have the same meaning);

"Services" – means all ongoing services that are described in the Service Agreement;

"Sub-processor" – means the subcontractor hired by the Processor or by any of the Processor's Sub-processors and who agrees to receive Personal Data from the Processor or from any of the Processor's Sub-processors with the sole intention of Processing the Personal Data after the transfer on behalf of the Controller in accordance with the Controller's instructions, the terms of this DPA, and the terms of a written Sub-processor agreement.

"Technical and organizational security measures" – means measures designed to protect Personal Data against accidental or illegal deletion, accidental loss, alteration, unauthorized disclosure or unauthorized access, in particular when the Processing involves transmission of data over a network, and against any other form of illegal Processing;

"Data Protection Agency" – means the Swedish Authority for Privacy Protection.

3. PROCESSING OF PERSONAL DATA

3.1. In order to fulfill the Parties' Service Agreement, the Controller approves and instructs the Processor to process on its behalf:

- a) Personal Data relating to the Controller's and/or the Controller's Affiliates' employees.
- b) The categories of Personal Data that may be processed include (but are not limited to): name, e-mail address, phone number, manager's name, organizational affiliation(s) within the Controller's organization (such as group, project and functional affiliation), birth date/age, gender, geographical location, and date of employment at the Controller.
- c) The Processor will as a main rule not process any special categories of personal data (as defined under the GDPR) nor other information more sensitive than those mentioned above.

3.2. The Processor shall Process Personal Data only for the following purposes:

- a) in accordance with the Parties' Service Agreement and this DPA to provide the Services under the Parties' Service Agreement, including any additional services;
- b) in accordance with the Controller's at any time applicable documented instructions;
- c) in order to communicate with the Data Subjects who contacts the Processor;
- d) in order to administer the Parties' Service Agreement and invoicing;
- e) in accordance with applicable Data Protection Law, and
- f) to comply with Applicable Foreign Law, but shall in such case inform the Controller of such requirements before processing the data.

3.3. The Processor undertakes to comply with the requirements that Article 28 of the GDPR obliges a Processor, including the requirement to keep proper documentation and records of its Processing of Personal Data under this DPA. Such documentation shall be presented to the Controller upon request.

3.4. The Processor may not transfer Personal Data to a Third country unless permitted by section 5 below.

3.5. The Processor shall correct, block, erase, modify or delete Personal Data in accordance with the Controller's instructions. If the Controller has marked that Personal Data is to be deleted, such deletion must be done no later than 60 days thereafter.

3.6. The Processor shall, upon request, promptly assist the Controller with fulfilling the Controller's responsibilities in respect of the Data Subject's right of access and rectification under Article 15 and 16

of the GDPR, the right to request erasure under Article 17 of the GDPR as well as the right to oppose and restrict Processing under Article 18 of the GDPR.

- 3.7. Personal Data shall be deleted (erased) as soon as the purpose for which they were collected has been completed, unless other legal requirements stipulate that data must be saved for a certain time period. However, the Processor is entitled to retain and use anonymized Response Data as a basis for business and method development and statistics.
- 3.8. The Processor may not provide the Controller with Response Data other than in anonymized form.

4. SUB-PROCESSORS

- 4.1. The Processor may use or replace a third party or several third parties for the Processing of Personal Data under this DPA if the Processor has entered into a written agreement with the Sub-processor for the Processing of Personal Data, in which the Sub-processor is imposed in all material respects similar obligations as the Processor under this DPA.
- 4.2. The Processor shall ensure that the Controller is aware of what Sub-processors Process Personal Data by, without undue delay upon the Controller's request, providing correct and updated information about all Sub-processors, where the following information is specified for each Sub-processor:
 - a) definition of the Sub-processor, including its contact information, company form and geographical location;
 - b) what kind of service the Sub-processor is performing; and
 - c) where the Sub-processor is Processing the Personal Data covered by this DPA.
- 4.3. The Processor may not use a Sub-processor if that means that Personal Data will be transferred to a Third country unless the provisions in section 5 are met.
- 4.4. The Processor is fully responsible for the Sub-processor's Processing in relation to the Controller.
- 4.5. When the Processor intends to hire a new Sub-processor or replace an existing one, the Processor shall verify the Sub-processor's capacity and ability to meet their obligations in accordance with the Data Protection Legislation. The Processor shall notify the Controller in writing of
 - a) the Sub-processor's name, corporate identity number and head office (address and country), which type of data and categories of Data Subjects are being processed, and
 - b) where the Personal Data will be processed.
- 4.6. The Controller is entitled within thirty (30) days of the notice pursuant to item 4.5 to object to the Processor's hiring of a new Sub-processor and, due to such an objection, to cancel this Agreement to be terminated in accordance with the provisions of item 4.7 of this Agreement.
- 4.7. If the Controller objects to the Processor using a new Sub-processor, pursuant to item 12.6 of this Agreement, the Controller is entitled to terminate the Agreement with immediate effect.
- 4.8. Sub-processors are listed in the "List of Sub-Processors" available at catalystone.com/engage-legal/legal/sub-processors.

5. RESTRICTIONS ON THE RIGHT TO TRANSFER PERSONAL DATA TO A THIRD COUNTRY

- 5.1. The Processor does not own the right to transfer Personal Data to a Third Country, unless at least one of the following conditions are met:
 - a) the Data Subject has given his/her consent to the transfer,
 - b) any of the situations enumerated in Article 45, 46, 47 and 49 of the GDPR are present,

- c) an agreement for transfer of data (so called Data Transfer Agreement) containing the EU Commissions model clauses (2010/87/EU) has been entered into without any amendments or additions that contradict the clauses, which shall be displayed upon request of the Controller,
 - d) the Processor has established binding internal rules (so called Binding Corporate Rules) and the recipient of the Personal Data in the Third country is subject to these, or
 - e) The Processor has conducted self-certification and joined the EU-US Privacy Shield principles by registering on the U.S. Department of Commerce Privacy Shield list.
- 5.2. The Processor is responsible for the Sub-processor's Processing of Personal Data, as if the Processing is done by the Processor itself.
- 5.3. If transfer of Personal Data to a Third country becomes applicable, the Processor shall, prior to the transfer, ensure that provide documentation proving that the provision in clause 5.1 is executed or developed, as applicable, and upon request from the Controller provide such documentation for review subject to applicable confidentiality restrictions.

6. SECURITY

- 6.1. The Processor shall assist the Controller in complying with the security requirements of Processing by taking appropriate Technical and organizational measures to protect the Personal Data being processed as stipulated in Article 32 to 36 of the GDPR.
- 6.2. The Personal Data shall be protected by the Processor from destruction, modification, unlawful disclosure and unauthorized access. The Personal Data shall also be protected against any other form of unauthorized Processing. The Processor shall upon the Controller's request inform the Controller of the Technical and organizational measures taken to protect the Personal Data processed on behalf of the Controller.
- 6.3. The Processor shall provide and undertake technical and practical solutions to investigate suspicions that any unauthorized person has processed or have had unauthorized access to the Personal Data. In the event of a personal data breach, the Processor should inform the Controller of the event without undue delay after becoming aware of such breach.
- 6.4. If the Processor is missing instructions from the Controller that the Processor considers necessary to perform the Processing of Personal Data, or believes that the Controller's instructions in whole or in part conflict with the statutes, regulations and recommendations that the Processor shall comply with under this DPA, the Processor shall without undue delay notify the Controller about its opinion and await the instructions that the Controller considers necessary. If the Controller does not submit new instructions within a reasonable time, the Processor shall have the right to take reasonable and necessary security measures to comply with the Data Protection Rules at the Controller's expense.
- 6.5. The Processor is entitled to compensation for reasonable, substantiated and direct additional costs incurred as a result of altered or further instructions as described in clause 6.1 and 6.4 above. Such right to compensation shall not, however, apply to altered security requirements that the Processor shall fulfill without entitlement to compensation according to the Service Agreement.

7. AUDIT AND SUPERVISION

- 7.1. The Controller is entitled to, on its own behalf and at the expense of the Controller, or through a third party designated by the Controller (who shall not be a competitor to the Processor), follow up that the Processor fulfills the Controller's requirements for the Processing. In such follow-up, the Processor shall assist the Controller or the third party carrying out the audit with documentation, access to premises, IT systems and other assets necessary to follow up on the Processor's compliance with this DPA, provided, however, that such access does not imperil or can be reasonably assumed to imperil, an individual's anonymity or integrity. The Processor is entitled to offer alternative follow-up procedures, such as an audit conducted by an independent third party. In this case, the Controller shall be entitled to, but not obliged to, apply this

alternative follow-up procedure. If audits take place more than once per calendar year, the Processor is entitled to compensation for its reasonable costs for assisting with such audit.

- 7.2. The Processor shall also prepare the opportunity for the Data Protection Agency, or any other authority that is or may be of importance for Processing of Personal Data, to conduct consultation and on-premises supervision.
- 7.3. If the Data Protection Agency or other authority initiates review of the Controller's Processing of Personal Data or if an individual appeal against the Controller or the Processor in respect of such Processing and the matter concerns Processing that may be assumed to have been conducted by the Processor, the Processor shall, to a reasonable extent and against compensation for incurred costs, assist the Controller with documentation and other information regarding the Processing in order to enable the Controller to accommodate authorities in their audit and respond to their requirements.

8. DISCLOSURE OF INFORMATION

- 8.1. If the Data Subject, the Data Protection Agency, other supervisory authority or other third party requests information from the Processor regarding the Controller's Processing of Personal Data, the Processor shall refer to the Controller. The Processor may not disclose Personal Data or other information regarding the Controller's Processing of Personal Data without the prior written consent of the Controller. The Processor shall assist the Controller in the event that a Data Subject requests access to information that is recorded about him/her in the form of Personal Data or requests correction of such information.
- 8.2. The Processor shall, without undue delay, notify the Controller in writing regarding any contacts from the Data Protection Agency or any other supervisory authority that concern or may be of importance for the Processing of Personal Data. The Processor is not entitled to represent the Controller or act on the Controller's behalf against the Data Protection Agency or any other supervisory authority that concern or may be of importance for the Processing of Personal Data. In the event that the Processor by law or by authority injunction is required to disclose Personal Data, what is stipulated regarding confidentiality in clause 9.2 applies.

9. CONFIDENTIALITY

- 9.1. The Processor and the persons working under its management shall, in the Processing of Personal Data, agree customary confidentiality undertakings or be subject to an appropriate statutory professional secrecy.
- 9.2. The Processor may disclose Personal Data or information about its Processing without this being an act that violates this DPA if the Processor by law, regulations or authority injunction is required to disclose Personal Data. In such a case, the Processor shall immediately notify the Controller in writing of this, and, if possible, request that the requested Personal Data is subject to confidentiality upon disclosure.

10. AGREEMENT TERM, RELATION TO OTHER AGREEMENTS AND AMENDMENTS

- 10.1. This DPA is valid between the Parties as long as the Processor Processes Personal Data for which the Controller is the Data Controller. Upon termination of the Service Agreement, the Processor shall ensure that all Personal Data is deleted no later than 60 days thereafter.
- 10.2. The Processor undertakes to erase all Personal Data after the Processor's obligations under this DPA have been terminated, and delete any copies, unless the storage of Personal Data is required by law and as set out in 10.1 above.
- 10.3. If the underlying Service Agreement that entails that the Processor Processes Personal Data is terminated, and a new such agreement is reached without a new DPA has been entered into, this DPA shall also apply to the new agreement.

10.4. Amendments and additions to this DPA shall, in order to be valid, be made in writing and signed by both Parties.

11. GOVERNING LAW AND DISPUTE

11.1. The General Terms shall be governed, construed, and enforced solely in accordance with the laws applicable in Sweden.

11.2. Any dispute, controversy, or claim arising out of, or in connection with this DPA, or the breach, termination, or invalidity thereof, shall be finally settled by arbitration administered by the Arbitration Institute of the Stockholm Chamber of Commerce. The language to be used in the arbitral proceedings shall be English unless the Parties have agreed otherwise.