

ANNEX II – DATA PROCESSING AGREEMENT

This Annex, or data processing agreement, describes the obligations of the parties, including those under applicable privacy, security and data protection legislation, in relation to the processing and security of Customer Data as defined below (hereinafter, the "DPA"). This Annex shall take effect on the date of commencement of the provision of the Services and shall supersede any terms previously applicable to the processing and security of Customer Data.

For the purposes of integrating this Annex into the Agreement myReach is considered as the Processor and the Customer is considered as the Controller which shall be governed by Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, (hereinafter, the "GDPR"), its implementing regulations and the Swiss Data Protection Act and its Ordinance (hereinafter, the "FDPA") (collectively "Applicable Data Protection Laws").

1. Purpose

- 1.1. The purpose of this DPA is to define the conditions under which the Processor, as Data Processor, shall process the Controller's Personal Data necessary for the proper performance of the Services provided to the Controller, as described in the Agreement.
- 1.2. The nature of the Services implies for the Processor the need to carry out the following processing activities: collection, recording, conservation, transmission to the Controller and erasure or destruction of personal data, to the extent necessary for the adequate provision of the Services.

2. Term

- 2.1. This DPA shall be effective during the time necessary to render the Services to the Controller. Nonetheless, the Parties agree that all clauses of the present DPA which are expressly or implicitly intended to continue in force after its termination shall continue in force and binding the parties in accordance with the relevant clause.

3. Purpose of the processing

- 3.1. The Controller's Personal Data shall be processed only to carry out the provision of the Services. Where the Processor deems necessary to process personal data for a different purpose, it shall obtain the previous written authorisation from the Controller. Failure to obtain such authorisation shall impede the operation of said processing.

4. Categories of the data subjects and of the personal data.

- 4.1. The categories of data subjects to whom the personal data processed under this DPA concern are Customers.
- 4.2. The categories of personal data to be processed under this DPA are any Customer Data provided to myReach while provisioning the Cloud Services.

5. Obligations of the Controller.

- 5.1. In order to permit the provision of the Service, the Controller undertakes to make available to the Processor all the personal data and/or information necessary for the appropriate operation of the processing activities.

6. Obligations of the Processor.

- 6.1. The Processor undertakes to:
 - 6.1.1. Comply with the duty to inform and to obtain consent under the instructions of the Controller where the provision of the Services implies collection of personal data on

behalf of the Controller and when such collection implies that the Processor shall comply with the referred duty to inform.

- 6.1.2. Processes the personal data only to carry out the provision of Services and under documented instructions from the Controller (unless required to conduct complementary processing activities by an applicable regulation).
- 6.1.3. Where the personal data are processed in the systems or facilities of the Processor, it shall guarantee the implementation of appropriate technical and organisational measures in order to achieve a level of security adequate to the risk, taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing.
- 6.1.4. In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed, or unauthorised communication or access to said data.
- 6.1.5. Process the Controller's Personal Data applying the security measures determined by the Controller where the processing is operated in the Controller's systems or facilities.
- 6.1.6. In order to subcontract third-party services that imply access and/or processing of personal data, the Processor shall notice the Controller in reasonable advance so that it will be able to object to such subcontracting. Otherwise, the engagement of a subcontractor shall be authorised and the subcontractor shall have to become contractually bound to the same data protection obligations as those established in this DPA for the Processor. In any case, access to personal data by companies and professionals engaged by the Processor within its internal organizational scope in order to provide general or maintenance services is authorised, provided that such tasks have not been arranged by the Processor for the purpose of subcontracting from a third party all or part of the Services provided to the Controller. The Processor shall maintain an up-to-date list of the subcontracted third parties with access to personal data engaged in the processing of Personal Data. This list shall be accessible to the Controller through the following hyperlink: <https://myreach.io/terms-and-conditions/subprocessors>. The Processor shall ensure that the list remains accurate and promptly update it to reflect any changes.
- 6.1.7. Delete or return all the personal data to the Controller, at the choice of the latter, after the end of the provision of Services, and to delete all existing copies unless storage of the personal data is required by law.
- 6.1.8. Assist the Controller in ensuring compliance with its legal obligations relating to the security of processing, communication of data security breaches of which it becomes aware, data protection impact assessment and prior consultation.
- 6.1.9. Assist the Controller in the fulfilment of its obligation to respond to requests from data subjects for exercising of their rights and to inform without delay of any request sent directly to the Processor.
- 6.1.10. Comply with its obligation to notify personal data security breaches to the Controller as provided in the provisions of the Applicable Data Protection Laws.
- 6.1.11. Maintain a record of processing activities carried out on behalf of the Controller.
- 6.1.12. Cooperate, on request, with the correspondent Data Protection Agency in the performance of its tasks.

7. International data transfers

- 7.1. the Processor shall not process the Controller's Personal Data outside the European Economic Area including Switzerland (EEA) or in a country which does not ensure an adequate level of security, unless a frame of adequate protection under the current legislation can be guaranteed by means of the application of binding corporate rules, standard data protection clauses adopted by the Commission or where the relevant transfer has been authorised by the competent Supervisory Authority.