

Data processing agreement

This data processing agreement is applicable to all processing of personal data that Thingsdata, registered with the Chamber of Commerce under number 66044561, (hereinafter: '**Controller**') has performed by another party contracted by it (hereinafter: '**Processor**') on the basis of the agreement concluded between these parties (hereinafter: '**the Agreement**').

Article 1. Purposes of processing

- 1.1. Processor hereby agrees under the terms of this Data Processing Agreement to process personal data on behalf of the Controller. Processing shall be done solely for the purpose of facilitating orders and payments for products or services of Controller, storing data in the 'cloud' for the benefit of Controller, and associated online services, managing financial administration and bookkeeping of Controller, offering and maintaining the online Customer Relationship Management service of Processor for Controller, providing customer service by phone with customers of Controller, providing Public Relations and marketing activities for Controller, the transmission of newsletters for Controller, managing the customer administration of Controller, and all purposes compatible therewith or as determined jointly.
- 1.2. The personal data to be processed by Processor for the purposes as set out in the previous clause and the categories of data subjects involved are set out in Appendix 1 of this Data Processing Agreement. Processor shall not process the personal data for any other purpose unless with Controller's consent. Controller shall inform Processor of any processing purposes to the extent not already mentioned in this Data Processing Agreement. Processor however is permitted to use personal data for quality assurance purposes, including surveys to data subjects and statistical research purposes regarding the quality of Processor's services.

Article 2. Processor's obligations

- 2.1. Regarding the processing operations referred to in the previous clause, Processor shall comply with all applicable legislation, including at least all data processing legislation such as the GDPR.
- 2.2. Upon first request Processor shall inform Controller about any measures taken to comply with its obligations under this Data Processing Agreement.
- 2.3. All obligations for Processor under this Data Processing Agreement shall apply equally to any persons processing personal data under the supervision of Processor, including but not limited to employees in the broadest sense of the term.

- 2.4. Processor shall inform Controller without delay if in its opinion an instruction of Controller would violate the legislation referred to in the first clause of this article.
- 2.5. Processor shall provide reasonable assistance to Controller in the context of any data protection impact assessments to be made by Controller.
- 2.6. Processor shall, in accordance with Article 30 GDPR, keep a register of all categories of processing activities which it carries out on behalf of the Controller under this data processing agreement. At Controller's request, Processor shall provide Controller access to this register.

Article 3. Transfer of personal data

- 3.1. Processor may process the personal data in any country within the European Union.
- 3.2. Transfer to countries outside the European Union is not permitted.
- 3.3. Processor shall report to Controller of the countries involved.

Article 4. Allocation of responsibilities

- 4.1. The authorised processing operations shall be performed by employees of Processor within an automated environment.
- 4.2. Processor is solely responsible for the processing of personal data under this Data Processing Agreement in accordance with the instructions of Controller and under the explicit supervision of Controller. For any other processing of personal data, including but not limited to any collection of personal data by Controller, processing for purposes not reported to Processor, processing by third parties and/or for other purposes, the Processor does not accept any responsibility.
- 4.3. Controller represents and warrants that the content, usage and instructions to process the personal data as meant in this Data Processing Agreement are lawful and do not violate any right of any third party.

Article 5. Involvement of sub-processors

- 5.1. Processor shall not involve any third parties in the processing under this Data Processing Agreement without the prior written permission of Controller, which permission may be made conditional.
- 5.2. In any event, Processor shall ensure that any third parties are bound to at least the same obligations as agreed between Controller and Processor. Controller has the right to inspect the agreements containing such obligations.

5.3. Processor shall ensure that these third parties shall comply with the obligations under this Data Processing Agreement and is liable for any damages caused by violations by these third parties as if it committed the violation itself.

Article 6. Security

6.1. Processor shall use reasonable efforts to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk for the processing operations involved, against loss or unlawful processing (in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed).

6.2. The security measures include, but are not limited to:

- a. Implementing appropriate access controls and authentication measures to prevent unauthorized access to personal data.
- b. Regularly updating and patching systems and software to address security vulnerabilities.
- c. Encrypting personal data during transmission and storage.
- d. Implementing firewalls, intrusion detection and prevention systems, and other security measures to reduce network risks.
- e. Training employees who have access to personal data on the importance of data protection and confidentiality.

6.3. Processor does not warrant that the security is effective under all circumstances. If any security measure explicitly agreed in this Data Processing Agreement is missing, then Processor shall use best efforts to ensure a level of security appropriate to the risk, taking 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.

6.4. Controller shall only provide personal data to Processor for processing if it has ensured that the required security measures have been taken. Controller is responsible for the parties' compliance with these security measures.

Article 7. Notification and communication of data breaches

7.1. Controller is responsible at all times for notification of any security breach and/or personal data breach (which are understood as: a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed as described in Article 4 (12) of the GDPR) to the competent supervisory authority and for communication of the same to data subjects. In order to enable Controller to comply with this legal requirement,

Processor shall notify Controller within a reasonable period after becoming aware of an actual or threatened security or personal data breach.

7.2. A notification under the previous clause shall be made only for actual breaches with severe impact.

7.3. The notification shall include at least the fact that a breach has occurred. In addition, the notification shall:

- describe the nature of the personal data breach including, where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
- describe the likely consequences of the personal data breach;
- include the name and contact details of the Data Protection Officer (if appointed) or a contact person regarding privacy subjects;
- describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

Article 8. Processing requests from data subjects

8.1. In the event a data subject makes a request to exercise his or her legal rights under the GDPR (Articles 15-22) to Processor, the parties shall jointly consult on how to handle the request. Controller shall however retain final responsibility on the request.

Article 9. Confidentiality obligations

9.1. All personal data that Processor receives from Controller and/or collects itself is subject to strict obligations of confidentiality towards third parties. Processor shall not use this information for any goals other than for which it was obtained, not even if the information has been converted into a form that is no longer related to an identified or identifiable natural person.

9.2. The confidentiality obligation shall not apply to the extent Controller has granted explicit permission to provide the information to third parties, the provision to third parties is reasonably necessary considering the nature of the assignment to Controller or the provision is legally required.

Article 10. Audit

10.1. Controller has the right to perform audits on Processor to verify unauthorised use of personal data by Processor personnel, and all issues reasonably connected thereto.

10.2. This audit may be performed in case a substantiated allegation of misuse of personal data has arisen.

- 10.3. Processor shall give its full cooperation to the audit and shall make available employees and all reasonably relevant information, including supporting data such as system logs.
- 10.4. The audit findings shall be assessed by Processor and implemented if and to the extent deemed reasonable by Processor.
- 10.5. The costs of the audit shall be borne by both parties.

Article 11. Liability

- 11.1. Parties explicitly agree that any liability arising in connection with personal data processing shall be as provided in the Agreement.

Article 12. Term and termination

- 12.1. This Data Processing Agreement enters into force upon signature by the parties and on the date of the last signature.
- 12.2. This Data Processing Agreement is entered for the duration of the cooperation between the parties.
- 12.3. Upon termination of the Data Processing Agreement, regardless of reason or manner, Processor shall - at the choice of Controller - return in original format or destroy all personal data available to it.
- 12.4. Controller is entitled to amend this Data Processing Agreement from time to time. Controller shall notify the Processor of amendments at least three months prior to their taking effect. Processor may terminate if the amendments are unacceptable to it.

Article 13. Applicable law and competent venue

- 13.1. This Data Processing Agreement and its execution are subject to Dutch law.
- 13.2. Any disputes that may arise between the parties in connection with this Data Processing Agreement shall be brought to the competent court for the place of business of Controller.

Appendix 1: Stipulation of personal data and data subjects

Data subjects and personal data of different purposes

Processor shall process the below personal data of the categories data subjects from different purposes (with retention period if specified) under the supervision of Controller, as specified in article 1 of the Data Processing Agreement:

Cloud storage of data

Leads and potential customers

- Telephone numbers
- Email addresses
- Visitor behaviour
- Names and addresses
- Financial data

Customers

- Telephone numbers
- Email addresses
- Names and addresses
- Financial data
- Visitor behaviour

Suppliers

- Email addresses
- Names and addresses
- Telephone numbers
- Financial data

Website visitors

- Visitor behaviour
- Telephone numbers
- Email addresses
- Financial data
- Names and addresses

Prospective employees

- Telephone numbers
- Resumes
- Email addresses
- (Portrait)photos
- Dates of birth
- Names and addresses

Customer Relationship Management

Customers

- Visitor behaviour
- Names and addresses
- Telephone numbers

- Email addresses
- Financial data

Send newsletters

Customers

- Email addresses
- Names and addresses

Customer and/or member administration

Customers

- Telephone numbers
- Email addresses
- Names and addresses
- Financial data

PR or Marketing

Customers

- Names and addresses
- Email addresses
- Financial data
- Telephone numbers

Accounting (financial administration)

Suppliers

- Names and addresses
- Telephone numbers
- Email addresses
- Financial data

Customers

- Names and addresses
- Financial data
- Telephone numbers
- Email addresses

Customer service or call center

Suppliers

- Names and addresses

- Telephone numbers
- Email addresses
- Financial data

Customers

- Financial data
- Telephone numbers
- Email addresses
- Names and addresses

Handling orders and payments for products or services of Controller

Suppliers

- Financial data
- Telephone numbers
- Email addresses
- Names and addresses

Customers

- Financial data
- Email addresses
- Names and addresses
- Telephone numbers

Controller represents and warrants that the description of personal data and categories of data subjects in this Appendix 1 is complete and accurate and shall indemnify and hold harmless Process for all faults and claims that may arise from a violation of this representation and warranty.