Data Processing Agreement - CMNTY Corporation (CMNTY)

Last modified: October 21, 2022

1. DEFINITIONS

The capitalized terms used in this Data Processing Agreement have the following meanings:

1. *Data Subject:* the individual who is the subject of Personal Data.
2. *Data Processing Agreement:* the present Data Processing Agreement.
3. *Personal Data:* any information relating to an identified or identifiable natural person the Processor processes for the purposes of the execution of the Agreement with the Controller.
4. *Agreement:* the agreement between the Controller and the Processor regarding the use of the CMNTY platform.

2. PROCESSING OF PERSONAL DATA

1. The categories of Data Subjects and types of Personal Data processed by the Processor are the accounts created within the CMNTY Platform including, but not limited to the given profile information and created content.
2. The Processor shall process the Personal Data it has received only on the basis of the Controller's written instructions and only for the purposes of the execution of the Agreement, unless any provision of EU law or Member State law requires it to carry out this processing. In that case, the Processor shall notify the Controller of this legal requirement prior to the processing operation unless this legislation prohibits this notification for important reasons of public interest.
3. The Processor does not have any control over the purposes and means of the processing of Personal Data. Nothing in this Data Processing Agreement is intended to transfer control over Personal Data to the Processor in any way.
4. The Processor is not permitted:
    a. to process Personal Data for its own purposes;
    b. to process Personal Data for other or more extensive purposes than those that are reasonably required for the execution of the Agreement;
    c. to disclose Personal Data to third parties to the extent this is not permitted under the Agreement and/or the Data Processing Agreement and/or under any mandatory statutory provision requiring the Processor to disclose Personal Data to supervisory or investigation authorities.

3. COMPLIANCE WITH STATUTORY AND OTHER RULES

1. The parties shall act in accordance with the provisions of the GDPR and any future national or European statutory and other rules on the processing of Personal Data that may be in force from time to time. If future statutory and other rules reveal a need to adjust the Data Processing Agreement, the parties will consult with each other for the purpose of making new arrangements that reflect the tenor of this Data Processing Agreement as much as possible.
2. The Processor agrees to cooperate with the Controller in the execution of a Privacy Impact Assessment to the extent it may do so given the information available to it and the nature of the processing. The reasonable costs this duty to cooperate entails must be borne by the Controller.
3. To the extent that the Controller is required under statutory or other rules to give information about the processing of Personal Data to a supervisory authority, the Processor shall, when first requested to do so by the Controller, render all cooperation with the Controller that is reasonably requested, so as to ensure that this information is made available and the supervisory authority can be adequately informed.
4. The Processor shall not be liable for any administrative fine imposed by a supervisory authority or for any loss or damage suffered by Data Subject(s) or the Controller unless in cases of gross negligence or deliberate recklessness on the part of the Processor or its managers.

4. CONFIDENTIALITY

1. The Processor agrees to maintain confidentiality of the Personal Data and to ensure that the persons authorized to process the Personal Data undertake to maintain confidentiality.
2. This duty of confidentiality will continue to exist even after the termination of this Data Processing Agreement, unless it concerns information that is already available to the public other than as a result of any violation of the aforementioned duty of confidentiality.

5. SECURITY MEASURES TO BE TAKEN BY THE PROCESSOR

1. The Processor will take the appropriate technical and organizational measures which are set out in the **Data Security Statement.**
2. When taking technical and organizational security measures, the Processor shall take account of the state of the art and the implementation costs of the security measures as well as of the nature, scope and context of the processing operations, the purposes and the intended use of its products and services, the

processing risks and the expected various risks, in terms of probability and severity, for the rights and freedoms of Data Subjects, considering the intended use of products and services.

3. In assessing the appropriate security level, the Processor shall take particular account of the processing risks, mainly those relating to the destruction, loss, change or the unauthorized disclosure of or unauthorized access to transmitted, stored or in any other way processed data, either accidentally or unlawfully.

4. Unless explicitly stated otherwise, the Processor's CMNTY platform is not intended for the processing of special categories of Personal Data, social security numbers or data concerning convictions and offenses.

6. SUPERVISION BY CONTROLLER

1. The Processor agrees to provide the Controller with the necessary information at the latter's request, to ensure that the Controller is able to assess the Processor's compliance with the provisions of this Data Processing Agreement.

2. The Controller is entitled to engage an independent expert to ascertain whether the Processor fulfills the obligations of the Processor in this Data Processing Agreement, which independent expert will be under an obligation to main confidentiality in respect of the foregoing. The Processor shall cooperate in the audit and make all information that is reasonably relevant to the audit available as soon as possible. The costs of the audits carried out on the instructions of the Controller must be borne by the Controller, unless it turns out that the Processor has failed to fulfill its obligations to a sufficient extent, in which case the Processor must bear the costs.

3. If the audit report of the independent expert shows that the measures taken by the Processor do not sufficiently comply with the GDPR and/or other statutory or other rules that are in force, the Processor shall immediately take the proposed improvement measures as the Processor considers appropriate, taking into account the processing risks related to its product or service, the state of art, the implementation costs, the market in which it operates and the intended use of its product or service.

7. NOTIFICATION OBLIGATION WITH RESPECT TO DATA BREACHES

1. The Processor shall inform the Controller immediately, but in any case within 48 hours, as soon as it finds that there has been any breach with respect to the Personal Data. This information provided must enable the Controller to fulfill its obligations under Articles 33 and 34 of the General Data Protection Regulation.

2. The Processor shall always keep the Controller fully informed about the progress of any actions to remedy the breach and all relevant developments in respect of the breach as referred to in Article 7.1 and the consequences thereof. The Processor shall take all measures that can be reasonably expected from it to remedy or mitigate the adverse consequences of any unauthorized access as referred to in Article 7.1 as much as possible, where appropriate.

3. The Processor is not permitted to communicate a breach in the scope of Article 7.1. with the relevant Data Subject(s) and/or supervisory authorities other than on the instructions of the Controller or with its express and explicit permission.

8. SUBPROCESSING

1. The Processor shall hereby obtain permission to subcontract part of the processing of Personal Data to other processors for the duration of the contract.

2. In the case of general written permission, the Processor shall inform the Controller in advance about intended changes regarding the addition or replacement of other processors, the Controller being entitled to object to these changes in advance.

3. The Processor shall ensure that all processors engaged by it who are instrumental in the implementation of the Agreement are committing to an equivalent level of protection of the Personal Data as the Processor is bound to under this Data Processing Agreement.

9. REQUESTS FROM THE DATA SUBJECT

1. Under the GDPR, the Controller has obligations vis-à-vis the Data Subject, such as in respect of the provision of information, giving access to, rectifying and deleting Personal Data. The Processor shall – where possible – cooperate with the Controller in fulfilling the latter's obligations in this regard. The Processor maintains the right to charge the Controller a reasonable fee for its cooperation.

2. If a Data Subject directly contacts the Processor in relation to the execution of the former's rights under the GDPR, the Processor may not react to the content thereof but shall immediately inform the Controller thereof and request further instructions.

10. INTERNATIONAL FLOW OF PERSONAL DATA

1. The Processor shall ensure that every processing operation of Personal Data that is performed by or on behalf of the Processor, including third parties engaged by it for the purposes of the execution of the Agreement, is carried out within the European Economic Area (EEA) or to or from countries that offer an adequate level of protection in accordance with the GDPR.
2. Consequently, without the Controller's prior written permission, the Processor may not transmit Personal Data to or store them in a country outside the EEA or make Personal Data accessible from a non-EEA country, unless this country ensures an adequate level of protection or if an applicable provision of Union law or Member State law requires it to process the relevant data. In that case the Processor shall notify the Controller, prior to the processing operation, about that legal requirement, unless this legislation prohibits this notification for important reasons of public interest.

11. WARRANTY AND INDEMNITY

1. The Controller warrants that the data processing will be carried out in accordance with the law, including the GDPR. This means in any case that the Controller warrants that it is entitled to collect data or have data collected and that it is entitled to process these data and have these collected.
2. The Controller shall indemnify the Processor for any loss or damage and costs resulting from any claims by third parties, expressly including the Data Subjects and supervisory authorities, relating to or arising from any unlawful processing operation and/or any other violation of the GDPR or the Data Processing Agreement that can be attributed to the Controller.

12. LIABILITY

1. The Processor shall ensure correct compliance with the obligations under this Data Processing Agreement. This Data Processing Agreement fully takes part of the Agreement between the Controller and the Processor and the (total) liability of the Processor is (therefore) restricted in accordance with the provisions of Article 16 of the General Conditions/Agreement.

13. DURATION OF THE DATA PROCESSING AGREEMENT

1. This Data Processing Agreement enters into force at the time of entry into force of the Agreement and is entered into for the duration of the Agreement.
2. As soon as the Agreement terminates or is terminated for whatever reason, the present Data Processing Agreement will remain in force as long as Personal Data are processed by the Processor, after which this Data Processing Agreement ends by operation of law.
3. Upon the termination of this Data Processing Agreement, the Processor shall delete all Personal Data in its possession and received from the Controller within a year, in such a way that they can no longer be used or be accessible or, if agreed,
4. The Processor can charge possible costs in the scope of Article 13.3 to the Controller.
5. The Processor may retain a copy of the Personal Data only if it is obliged to do so in accordance with a mandatory statutory provision.

14. FINAL PROVISION

1. Amendments and additions to the present Data Processing Agreement are valid only if the Parties have agreed upon them in writing.

    For clients based in North or South America:

2. This Data Processing Agreement is exclusively governed by New York law.
3. This Agreement shall be governed by, and construed in accordance with, the laws of the State of New York. Any disputes or claims arising out of or in relation to this Agreement or the breach hereof shall be finally settled under the Rules of Conciliation and Arbitration of the International Chamber of Commerce by one or more arbitrators appointed in accordance with those Rules. The arbitration proceedings shall be conducted in New York City, New York, U.S.A.

    For clients based in the European Union (EU) and the rest of the world:

4. This Data Processing Agreement is exclusively governed by Dutch law.
5. Any disputes arising under or in connection with this Data Processing Agreement must be exclusively submitted to the District Court of Oost-Brabant, 's Hertogenbosch, The Netherlands unless mandatory law designates another court as the court of competent jurisdiction.

APPENDIX A: Platform Subprocessors

Infrastructure Subprocessors

Entity Name	Purpose	Entity Country	Note
AWS	Platform hosting & Infrastructure	United States	AWS is a USA based company. However, we store data in one of their regions (Canada, Europe, US or Australia) depending on your contract with us.
InQdo Cloud B.V.	Platform hosting & Infrastructure Management	The Netherlands	

Optional Platform Subprocessors

Entity Name	Purpose	Entity Country	Note
Twilio, Inc	2FA SMS Services	United States	Only when 2FA with SMS is enabled.
Stripe, Inc	Payment Services	United States	Only when payment is performed within the platform.
Google Inc	Analytics service	United States	Only when Google Analytics is activated.
AWS	Video Conferencing	United States	Only when using Focus.
AWS	Sentiment, Image, Video and Text Analysis	United States	