RELATION CITY
OMNI CHANNEL

DATA PROCESSING AGREEMENT

Data Processing Agreement incl. Standard Contractual Clauses

For the purposes of Article 28(3) of Regulation 2016/679 (the GDPR)

between

ONLINECITY.IO
Buchwaldsgade 50
5000 Odense C, Denmark
VAT nr.: DK-27364276

(the data processor)

and

COMPANY NAME
STREET, NR
POSTAL CODE, CITY
VAT nr.:
Att.:

(the data controller)

each a ‘party’; together ‘the parties’

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to meet the requirements of the GDPR and to ensure the protection of the rights of the data subject.

TABLE OF CONTENTS

2. Preamble

1. These terms and conditions (hereinafter referred to as “Terms” of www.relationcity.com (hereinafter referred to as “RelationCity”)) apply to any use of RelationCity.

2. The Clauses have been designed to ensure the parties’ compliance with Article 28(3) of Regulation 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).

3. RelationCity is an advanced communication platform that allows the Customer to send SMS and other formats of communication (the Services). “Communication” means all formats of communication (SMS, email, RCS, RBM, etc.). In the context of the provision of the Services, the data processor will process personal data on behalf of the data controller in accordance with the clauses.

4. The Clauses shall take priority over any similar provisions contained in other agreements between the parties.

5. Four appendices are attached to the Clauses and form an integral part of the Clauses.

6. **Appendix A** contains details about the processing of personal data, including the purpose and nature of the processing, type of personal data, categories of data subject and duration of the processing.

6. **Appendix B** contains the data controller’s conditions for the data processor’s use of sub-processors and a list of sub-processors authorized by the data controller.

6. **Appendix C** contains details about the processing of personal data, including the purpose and nature of the processing, type of personal data, categories of data subject and duration of the processing.

6. **Appendix D** contains provisions for other activities which are not covered by the Clauses.

3. The rights and obligations of the data controller

1. The data controller is responsible for ensuring that the processing of personal data takes place in compliance with the GDPR (see Article 24 GDPR), the applicable EU or Member State data protection provisions and the Clauses.

2. The data controller has the right and obligation to make decisions about the purposes and means of the processing of personal data.

3. The data controller shall be responsible, among other, for ensuring that the processing of personal data, which the data processor is instructed to perform, has a legal basis.

4. The data processor acts according to instructions

1. The data processor shall process personal data only on documented instructions from the data controller, unless required to do so by Union or Member State law to which the processor is subject. Such instructions shall be specified in appendices A and C. Subsequent instructions can also be given by the data controller throughout the duration of the processing of personal data, but such instructions shall always be documented and kept in writing, including electronically, in connection with the Clauses.

2. The data processor shall immediately inform the data controller if instructions given by the data controller, in the opinion of the data processor, contravene the GDPR or the applicable EU or Member State data protection provisions.

5. Confidentiality

1. The data processor shall only grant access to the personal data being processed on behalf of the data controller to persons under the data processor's authority who have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality and only on a need to know basis. The list of persons to whom access has been granted shall be kept under periodic review. On the basis of this review, such access to personal data can be withdrawn, if access is no longer necessary, and personal data shall consequently not be accessible anymore to those persons.

2. The data processor shall at the request of the data controller demonstrate that the concerned persons under the data processor's authority are subject to the abovementioned confidentiality.

6. Security of processing

1. Article 32 GDPR stipulates that, 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, the data controller and data processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk.

   The data controller shall evaluate the risks to the rights and freedoms of natural persons inherent in the processing and implement measures to mitigate those risks. Depending on their relevance, the measures may include the following:

   a. Pseudonymisation and encryption of personal data,

   b. the ability to ensure ongoing confidentiality, integrity, availability and resilience of processing systems and services,

   c. the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident,

   d. a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.

Continued on next page

2. According to Article 32 GDPR, the data processor shall also – independently from the data controller – evaluate the risks to the rights and freedoms of natural persons inherent in the processing and implement measures to mitigate those risks. To this effect, the data controller shall provide the data processor with all information necessary to identify and evaluate such risks.

3. Furthermore, the data processor shall assist the data controller in ensuring compliance with the data controller's obligations pursuant to Articles 32 GDPR, by inter alia providing the data controller with information concerning the technical and organizational measures already implemented by the data processor pursuant to Article 32 GDPR along with all other information necessary for the data controller to comply with the data controller's obligation under Article 32 GDPR.

   If subsequently – in the assessment of the data controller – mitigation of the identified risks require further measures to be implemented by the data processor, than those already implemented by the data processor pursuant to Article 32 GDPR, the data controller shall specify these additional measures to be implemented in Appendix C.

7. Use of Sub-processors

1. The data processor shall meet the requirements specified in article 28(2) and (4) GDPR in order to engage another processor (a sub-processor).

2. The data processor shall therefore not engage another processor (sub-processor) for the fulfillment of the clause without the prior general written authorisation of the data controller.

3. The data processor has the data controller's general authorisation for the engagement of sub-processors. The data processor shall inform in writing the data controller of any intended changes concerning the addition or replacement of sub-processors at least 30 days in advance, thereby giving the data controller the opportunity to object to such changes prior to the engagement of the concerned sub-processor(s). Longer time periods of prior notice for specific sub-processing services can be provided in Appendix B. The list of sub-processors already authorized by the data controller can be found in Appendix B.

Continued on next page

4. Where the data processor engages a sub-processor for carrying out specific processing activities on behalf of the data controller, the same data protection obligations as set out in the Clauses shall be imposed on that sub-processor by way of a contract or other legal act under EU or Member State law, in particular providing sufficient guarantees to implement appropriate technical and organizational measures in such a manner that the processing will meet the requirements of the Clauses and the GDPR. The data processor shall therefore be responsible for requiring that the sub-processor at least complies with the obligations to which the data processor is subject pursuant to the Clauses and the GDPR.

5. A copy of such a sub-processor agreement and subsequent amendments shall – at the data controller's request – be submitted to the data controller, thereby giving the data controller the opportunity to ensure that the same data protection obligations as set out in the Clauses are imposed on the sub-processor. Clauses on business related issues that do not affect the legal data protection content of the sub-processor agreement, shall not require submission to the data controller.

6. The data processor shall agree a third-party beneficiary clause with the sub-processor where – in the event of bankruptcy of the data processor – the data controller shall be a third-party beneficiary to the sub-processor agreement and shall have the right to enforce the agreement against the sub-processor engaged by the data processor, e.g. enabling the data controller to instruct the sub-processor to delete or return the personal data.

8. Transfer of data to third countries or international organizations

1. Any transfer of personal data to third countries or international organizations by the data processor shall only occur on the basis of documented instructions from the data controller and shall always take place in compliance with Chapter V GDPR.

2. In case transfers to third countries or international organizations, which the data processor has not been instructed to perform by the data controller, is required under EU or Member State law to which the data processor is subject, the data processor shall inform the data controller of that legal requirement prior to processing unless that law prohibits such information on important grounds of public interest.

Continued on next page

3. Without documented instructions from the data controller, the data processor therefore cannot within the framework of the Clauses:

   a. transfer personal data to a data controller or a data processor in a third country or in an international organization,

   b. transfer the processing of personal data to a sub-processor in a third country,

   c. have the personal data processed in by the data processor in a third country.

4. The data controller's instructions regarding the transfer of personal data to a third country including, if applicable, the transfer tool under Chapter V GDPR on which they are based, shall be set out in Appendix C.6.

5. The Clauses shall not be confused with standard data protection clauses within the meaning of Article 46(2)(c) and (d) GDPR, and the Clauses cannot be relied upon by the parties as a transfer tool under Chapter V GDPR.

9. Assistance to the data controller

1. Taking into account the nature of the processing, the data processor shall assist the data controller by appropriate technical and organizational measures, insofar as this is possible, in the fulfillment of the data controller's obligations to respond to requests for exercising the data subject's rights laid down in Chapter III GDPR.

   This entails that the data processor shall, insofar as this is possible, assist the data controller in the data controller's compliance with:

   a. the right to be informed when collecting personal data from the data subject

   b. the right to be informed when personal data have not been obtained from the data subject,

   c. the right of access by the data subject,

   d. the right to rectification,

   e. the right to erasure ('the right to be forgotten'),

   f. the right to restriction of processing,

Continued on next page

g. notification obligation regarding rectification or erasure of personal data or restriction of processing,

h. the right to data portability,

i. the right to object,

j. the right not to be subject to a decision based solely on automated processing, including profiling.

2. In addition to the data processor's obligation to assist the data controller pursuant to Clause 6.3., the data processor shall furthermore, taking into account the nature of the processing and the information available to the data processor, assist the data controller in ensuring compliance with:

a. The data controller's obligation to without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the competent supervisory authority, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons;

b. the data controller's obligation to without undue delay communicate the personal data breach to the data subject, when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons;

c. the data controller's obligation to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data (a data protection impact assessment);

d. the data controller's obligation to consult the competent supervisory authority, Datatilsynet, prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the data controller to mitigate the risk.

3. The parties shall define in Appendix C the appropriate technical and organizational measures by which the data processor is required to assist the data controller as well as the scope and the extent of the assistance required.
This applies to the obligations foreseen in Clause 9.1. and 9.2.

10. Notification of personal data breach

1. In case of any personal data breach, the data processor shall, without undue delay after having become aware of it, notify the data controller of the personal data breach.

2. The data processor's notification to the data controller shall, if possible, take place without undue delay or within 24 hours after the data processor has become aware of the personal data breach to enable the data controller to comply with the data controller's obligation to notify the personal data breach to the competent supervisory authority, cf. Article 33 GDPR.

3. In accordance with Clause 9(2)(a), the data processor shall assist the data controller in notifying the personal data breach to the competent supervisory authority, meaning that the data processor is required to assist in obtaining the information listed below which, pursuant to Article 33(3)GDPR, shall be stated in the data controller's notification to the competent supervisory authority:

    a. The nature of personal data including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned,

    b. the likely consequences of the personal data breach,

    c. 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.

4. The parties shall define in Appendix C all the elements to be provided by the data processor when assisting the data controller in the notification of a personal data breach to the competent supervisory authority.

11. Erasure and return of data

1. On termination of the provision of personal data processing services, the data processor shall be under obligation to delete all personal data processed on behalf of the data controller and certify to the data controller that it has done so unless Union or Member State law requires storage of the personal data.

12. Audit and inspection

1. The data processor shall make available to the data controller all information necessary to demonstrate compliance with the obligations laid down in Article 28 and the Clauses and allow for and contribute to audits, including inspections, conducted by the data controller or another auditor mandated by the data controller.

2. Procedures applicable to the data controller's audits, including inspections, of the data processor and sub-processors are specified in appendices C.7. and C.8.

3. The data processor shall be required to provide the supervisory authorities, which pursuant to applicable legislation have access to the data controller's and data processor's facilities, or representatives acting on behalf of such supervisory authorities, with access to the data processor's physical facilities on presentation of appropriate identification.

13. The Parties' agreement on other terms

1. The parties may agree to other clauses concerning the provision of the personal data processing service specifying e.g. liability, as long as they do not contradict directly or indirectly the Clauses or prejudice the fundamental rights or freedoms of the data subject and the protection afforded by the GDPR.

14. Commencement and termination

1. The Clauses shall become effective on the date of both parties' signature.

2. Both parties shall be entitled to require the Clauses renegotiated if changes to the law or inexpediency of the CLauses should give rise to such renegotiation.

3. The Clauses shall apply for the duration of the provision of personal data processing services. For the duration of the provision of personal data processing services, the Clauses cannot be terminated unless other Clauses governing the provision of personal data processing services have been agreed between the parties.

Continued on next page

4. If the provision of personal data processing services is terminated, and the personal data is deleted or returned to the data controller pursuant to Clause 11.1. and Appendix C.4. The Clauses may be terminated by written notice by either party.

5. Signature

ON BEHALF OF THE DATA CONTROLLER

Name: _____

Position: _____

Telephone: _____

E-mail:_____

_____

Signature and date

ON BEHALF OF THE DATA PROCESSOR

Name: _____

Position: _____

Telephone: _____

E-mail:_____

_____

Signature and date

15. Data controller and data processor contact details

1. The parties may contact each other using the following contact details:

ON BEHALF OF THE DATA CONTROLLER

Name: _____

Position: _____

Telephone: _____

E-mail:_____

ON BEHALF OF THE DATA PROCESSOR

Name: _____

Position: _____

Telephone: _____

E-mail:_____

The parties shall be under obligation continuously to inform each other of changes to contact details.

Appendix A - Information about the processing

A.1. The purpose of the data processor's processing of personal data on behalf of the data controller is:

- To provide the Services for sending and receiving Communication.

A.2. The data processor's processing of personal data on behalf of the data controller shall mainly pertain to (the nature of the processing):

- To keep end-user lists/campaigns and display logs of both sent and possibly received Communication and delivery status for Communication sent through the Services.

A.3. Duration of the data processor's processing of personal data on behalf of the data controller

- Storage of data for the period specified by the Data Controller on its account in the self-service platform. The period is set to 12 months by default, but may be modified by the Data Controller on their account.

A.4. The processing includes the following types of personal data about data subjects:

- Telephone number, message/communication content (and depending on this possible information such as member numbers, subscription number, subscription types, appointment times, etc.), sender name/number, e-mail address, names, customer categories and other information that the Data Controller uses for communication campaigns.

- The Data Controller may not provide sensitive personal data, as per GDPR article 9, for processing

A.5. Processing includes the following categories of data subject:

- Customers, partners, employees, members.

A.6. The data processor's processing of personal data on behalf of the data controller may be performed when the Clauses commence. Processing has the following duration:

- Until termination of the cooperation in the event of termination of this agreement or user account, in case of violation of the general terms of use or in the event of prolonged inactivity of the user account (see "Terms & Conditions" for details).

Appendix B - Authorized sub-processors

B.1. Approved sub-processors

- On commencement of the Clauses, the data controller authorizes the engagement of the following sub-processors:

NAME	VAT-NR	ADDRESS	DESCRIPTION OF PROCESSING
Hetzner Online GmbH	**DE** 812871812 **FI** 2720758-9	**Co-locations in Germany:** Am Datacenter-Park 1, 08223 Falkenstein / Vogtland Sigmundstraße 135, 90431 Nürnberg Industriestr. 25, 91710 Gunzenhausen **Co-location in Finland:** Huurrekuja 10 04360 Tuusula	Communication database hosting (storage)

The data controller shall on the commencement of the Clauses authorize the use of the abovementioned sub-processors for the processing described for that party. The data processor shall not be entitled – without the data controller's explicit written authorisation – to engage a sub-processor for a 'different' processing than the one which has been agreed upon or have another sub-processor perform the described processing.

Continued on next page

B.2. Prior notice for the authorisation of sub-processors

ONLINECITY.IO sends a notification when changing sub-processors to the Data Controller 30 days before the change, and considers the lack of feedback of the notification as approval of the sub-processor.

Appendix C - Instruction pertaining to the use of personal data

C.1. The subject of/instruction for the processing

The data proccesor's processing of personal data on behalf of the data controller shall be carried out by the data processor performing the following:

- Sending and receiving Communication and other communication formats via the Services and partners' Communication gateways.
- Storage of end user lists/campaigns containing names, telephone numbers, e-mail addresses and own defined data fields.

C.2. Security of processing

The processing includes no personal data covered by GDPR article 9 on "Special categories of personal data '', for which a "low level security" must be established.

The level of security shall take into account:

- Ensure that login and password procedures, firewall, antivirus software, and strong encryption of personal data is maintained
- Ensure that only employees with work-related purposes have access to personal data
- Store data storage media properly so that they are not accessible to third Parties
- Ensure that buildings and systems used for data processing are secure, and that only high-quality hardware and software is used, which is constantly updated

Continued on next page

- Ensure that employees receive adequate instructions and guidelines for the processing of personal data. The data processor is required to ensure that the employees involved in the processing of personal data are familiar with the security requirements

- Ensure that employees who are authorized to process personal data have entered into confidentiality agreements or are subject to the necessary statutory confidentiality obligation

- Ensure that data is used solely on behalf of the Data Controller and that the Data Processor cannot dispose of the information for his own purposes, including commercial use

The data processor shall hereafter be entitled and under obligation to make decisions about the technical and organizational security measures that are to be applied to create the necessary (and agreed) level of data security.

The data processor shall however – in any event and at a minimum – implement the following measures that have been agreed with the data controller:

The Data Processor deletes the recipient number, e-mail address, name and/or campaign information, message content, sender ID of communications 12 months after the message is sent, as per default. The Data Controller can modify this period on their account.

Establishment, maintenance and annual testing of the contingency plan as well as regular backup of personal information, as well as 24/7 monitoring of the operating systems.

Annual review of the procedures included in the procedures included as a control area in ISAE 3000 company audit, which is carried out annually.

Access to personal information via the Internet only via authorized users and through encrypted and / or secure connection, ie. HTTPS, TLS 1.3, X25519, and AES_128_GCM, as well as logical access control as well as authorization and rights management through Ed25519 encrypted key.

Confidentiality statements with employees and partners.

Continued on next page

Training and raising awareness about employee safety as well as sharing guidelines, procedure descriptions and policies.

Protection of personal information during transmission using highly encrypted Internet connections and e-mails.

Firewall and antivirus software to protect against unauthorized access to personal information.

Alarm preparedness, alarm security on doors, windows and entrances, and locking of printed personal information in safes, monitoring of common areas.

Access to work-related systems for employees on external communication connections, e.g. at home or in public places, only via encrypted and secure Internet connections, TLS 1.2 as a minimum.

Logging of systems, databases and networks, i.e. of logins and transmissions via API as well as access to databases with personal information.

C.3. Assistance to the data controller

The data processor shall insofar as this is possible – within the scope and the extent of the assistance specified below – assist the data controller in accordance with Clause 9.1. and 9.2. by implementing the following technical and organizational measures:

The Data Controller has put in place policies and procedures to ensure that ONLINECITY.IO can assist the data controller in fulfilling its obligation to respond to requests for the exercise of data subjects' rights.

The Data Processor has put in place policies and procedures to ensure that ONLINECITY.IO can assist the data controller in ensuring compliance with the obligations set out in Article 32 on processing security, Article 33 on notification and notification of breaches of personal data security, and Articles 34 - 36 on impact assessments.

Data Processor introduced policies and procedures that ensure that ONLINECITY.IO can make all information necessary to demonstrate compliance with data processor requirements available to the data controller.

The data processor also provides for and contributes to audits, including inspections carried out by the data controller or others authorized by the data controller.

C.4. Storage period/erasure procedures

Personal information is stored for 12 months after sending or receiving Communication, after which they are deleted by the data processor, as per default. The Data Controller may modify this period on their account.

Upon termination of the provision of personal data processing services, the data processor shall either delete or return the personal data in accordance with Clause 11.1., unless the data controller – after the signature of the contract – has modified the data controller's original choice. Such modification shall be documented and kept in writing, including electronically, in connection with the Clauses.

C.5. Processing location

Processing of the personal data under the Clauses cannot be performed at other locations than the following without the data controller's prior written authorisation:

In the Data Processor's premises or at the Data Processor's sub-data processors. The head office for the data processor, ONLINECITY.IO ApS, is Buchwaldsgade 50, 5000 Odense C, with other offices in Copenhagen Kronprinsensgade 6A, 2, 1114 København K, and C. A. Olesens Gade 4, 9000 Aalborg. Sub-data processors have an address, cf. Appendix B, section 1.

C.6. Instruction on the transfer of personal data to third countries

Personal data may only be transferred to secure third countries or international organizations or third countries resp. international organizations with a valid legal basis and only for necessary purposes. However, personal data must in any case be sought to remain within the EU.

In addition, personal data may be transferred to insecure third countries, but only on the basis of the entered-into EU standard contractual clauses (SCC) and additional measures, as mentioned in the judgment of the European Court of Justice in the Schrems II case, in order to preserve and support giving the data subjects the same level of protection as under the GDPR as well as the same rights under the European essential guarantees, ie The EU Charter of Human Rights and the EU Charter of Fundamental Rights.

For any third country transfers within the sense of Chapter V of the GDPR, the EU standard contractual provisions will be used as a transfer mechanism.

If the data controller does not in the Clauses or subsequently provide documented instructions pertaining to the transfer of personal data to a third country, the data processor shall not be entitled within the framework of the Clauses to perform such transfer.

By entering into this Data Processing Agreement, the data controller is aware that they are specifically instructing the data processor to use the sub-processor(s) defined in appendix B and that this sub-processor(s) has been instructed to use the mentioned data centers.

C.7. Procedures for the data controller's audits, including inspections, of the processing of personal data being performed by the data processor

The data processor shall yearly at the Data Processor's expense obtain an audit report from an independent third party concerning the data processor's compliance with the GDPR, the applicable EU or Member State data protection provisions and the Clauses.

The parties have agreed that the following types of audit report may be used in compliance with the Clauses:

- ISAE 3000

The audit report shall without undue delay be submitted to the data controller for information. The data controller may contest the scope and/or methodology of the report and may in such cases request a new audit under a revised scope and/or different methodology.

Based on the results of such an audit/inspection, the data controller may request further measures to be taken to ensure compliance with the GDPR, the applicable EU or Member State data protection provisions and the Clauses.

The data controller or the data controller's representative shall in addition have access to inspect, including physically inspect, the places where the processing of personal data is carried out by the data processor, including physical facilities as well as systems used for and related to the processing. Such an inspection shall be performed, when the data controller deems it required.

The data controller's costs, if applicable, relating to physical inspection shall be defrayed by the data controller. The data processor shall, however, be under obligation to set aside the resources (mainly time) required for the data controller to be able to perform the inspection.

C.8. Procedures for audits, including inspections, of the processing of personal data being performed by sub-processors

The data processor shall yearly at the data processor's expense obtain an auditor's report from an independent third party concerning the sub-processor's compliance with the GDPR, the applicable EU or Member State data protection provisions and the Clauses.

Continued on next page

The parties have agreed that the following types of auditor's report may be used in compliance with the Clauses:

- SSAE18 SOC 2 rapport / ISAE 3000 or similar reports

The auditor's report shall without undue delay be submitted to the data controller for information, if requested. The data controller may contest the scope and/or methodology of the report and may in such cases request a new audit/inspection under a revised scope and/or different methodology at their own expense.

Based on the results of such an audit/inspection, the data controller may request further measures to be taken to ensure compliance with the GDPR, the applicable EU or Member State data protection provisions and the Clauses.

The data processor or the data processor's representative shall not have access to inspect, including physically inspect, the places where the processing of personal data is carried out by the sub-processor, including physical facilities as well as systems used for and related to the processing. Such inspections are carried out in a company audit and the results thereof are maintained in the above auditor's statements and certificates.

Documentation for such inspections shall without delay be submitted to the data controller for information. The data controller may contest the scope and/or methodology of the report and may in such cases request a new inspection under a revised scope and/or different methodology at their own expense.

RELATION CITY
OMNI CHANNEL

DATA PROCESSING AGREEMENT

APRIL 2024