Data Processing Agreement

pursuant to Article 28 (3) p. 1 GDPR

– hereinafter referred to as **DP Agreement** –

between

Name / company: _____

Street, No.: _____

Post code, place, country: _____

Commercial register, No.: _____

Director: _____

– hereinafter referred to as **principal** –

and

sms77 e.K.
Köhlerkoppel 19
24109 Melsdorf
Germany
Register court: Amtsgericht Kiel, Register number: HRA 9532 KI

– hereinafter referred to as **contractor** –

– Contractor and principal are hereinafter also referred to as **contracting parties.** –

Annex

- annex 1 “security concept”

1. Subject of the contract, data categories, affected persons, kind, scope and purspose of the processing (Article 28 (3), 30 (2) GDPR)

1.1. The object of the DP Agreement, the personal data processed in the context of the order (Article 4 No. 1 GDPR; hereinafter referred to as „**data**“), the persons affected by the processing (hereinafter referred to as „**persons affected**“) as well as the kind, scope and purpose of the processing will be determined by the following legal relationship(s) between the contracting parties (hereinafter referred to as **„main contract“**):

- Service contract with the contractor based on the registration of the principal on the contractors' website and thereby acceptance of the terms and conditions

The provisions of this DP Agreement have priority over the main contract.

1.2. Kind of data:

- inventory data (e.g. names, adresses).

- contact data (e.g. email, phone numbers).

- content data (e.g. text input, photographs, videos).

- contracz data (e.g. contractual object, term).

- payment data (e.g. bank details, payment historie).

- usage data (e.g. interests, websites visited, buying behavior, access times, log data).

- meta / cummunication data (e.g. device IDs, IP addresses, location data).

- phone numbers (sender / recipient), contact information in the address book , telecommunication services such as SMS notifications (journal).

1.3. Processing of special categories of data (Article 9 (1) GDPR):

- In principle, no special categories of data are processed unless they are transferred by the principal, his customers, users or employees etc. to the processing.

1.4. Categories of persons affected:

- Customers / prospects / users of the principal.

- employees of the principal.

- suppliers of the principal.

1.5. Purpose of processing:

- Transit of telecommunication services (short messages, voice, emails).

- Analysis of subscriber information

- Storage of subscriber information (contacts)

- Storage of telecommunication services such as SMS notifications (journal)

2. Accountability and right of instruction

2.1. The principal as the **responsible person** is responsible pursuant to Article 4 No. 7 GDPR for the compliance with data protection regulations, in particular for the selection of the contractor, the data transmitted to him as well as issued instructions (Article 28 (3) lit. a, 29 and 32 (4) GDPR).

2.2. The contractor may process data only in the context of the main contract and the instructions of the principal (which also applies in particular to their rectification, deletion or limitation of processing) and only to the extent that the processing is required, unless the contractor is obligated to the processing by the law of the Union or the Member States to which the contractor is subject; in such a case, the contractor shall inform the principal of these legal requirements prior to processing, unless the relevant law prohibit such a notification because of an important public interest (Article 28 (3) p. 2 lit. a GDPR).

2.3. The principal has the right to issue additional instructions at any time with regard to the processing of the data and the security measures.

2.4. If the contractor is of the opinion that an instruction of the principal violates applicable data protection law, he will inform the principal immediately. In this case, the contractor is entitled to suspend the execution of the instruction until the confirmation of the instruction by the principal and to refuse them in case of obvious illegal instructions.

2.5. If additional instructions of the principal exceed the contractor's service obligation after the main contract and are not based on a misconduct by the contractor, then the principal must indemnify the contractor separately for the resulting additional expenses.

2.6. The contracting parties may determine entitled persons to issue and receive instructions (especially if these do not already arise from the main contract) and are obliged to notify changes of this information without delay.

3. Security concept and related obligations

3.1. The Contractor will design the internal organization within his area of responsibility in accordance with legal requirements and will in particular take technical and organizational measures (hereinafter referred to as "**TOMs**") for adequately security, in particular the confidentiality, integrity and availability of principals' data, considering the state of the art, the implementation costs and the kind, scope, circumstances and purposes of the processing as well as the different likelihood and severity of the risks to the rights and freedoms of persons affected, as well as their maintenance (Article 28 (3) and (32 - 39) in the sense of Article 5 GDPR). In particular, the TOMs include access control, disclosure control, input control, order control, availability control, separation control and the securing of the rights of persons affected.

3.2. The TOMs on which this DP Agreement is based arise out of the **Annex 1 "Security concept"**. They may be further developed in accordance with technical progress and replaced by adequate protective measures provided that they do not fall below the level of security of the specified measures and significant changes are communicated to the principal.

3.3. The contractor shall ensure that the persons authorized to process the data of the principal are bound to confidentiality and secrecy (Article 28 (3) p.2 lit. b and 29, 32 (4) GDPR) and have been instructed in the protective provisions of the GDPR or are subject to an appropriate statutory confidentiality obligation.

3.4. The data as well as data media transmitted in the context of the DP Agreement and all copies made thereof remain the property of the principal, must be carefully kept by the contractor, protected against access by unauthorized third parties and may only be destroyed with the consent of the principal and only according to data protection. Copies of data may only be made if they are necessary to fulfill the main and secondary service duties of the contractor to the principal (for example, backups).

3.5. Insofar as specified by the GDPR or supplementary, in particular national, regulations, the contractor entitle a data protection officer according to the legal requirements and inform the principal accordingly (Articles 37 to 39 GDPR).

4. Information and cooperation obligations

4.1. The rights of persons affected are to be performed vis-à-vis the principal, whereby the contractor supports the principal pursuant to Article 28 (3) p. 2 lit. e GDPR and informs him in particular about the inquiries he receive from persons affected.

4.2. The principal shall inform the contractor immediately and in full if, with regard to the processing of the data, he identifies errors or irregularities relating to provisions of this DP Agreement or relevant data protection regulations.

4.3. In the event that the contractor determines facts that justify the assumption that the protection of the data processed for the principal has been violated, the contractor must inform the principal immediately and in full, take immediately necessary protective measures, and support the principal in the fulfillment of his duties pursuant to Articles 33 and 34 GDPR.

4.4. Should the security of the data of the principal be endangered (e.g. seizure, confiscation, insolvency proceedings, etc.) by measures of third parties (e.g. creditors, authorities, courts, etc.), the contractor will immediately inform the third party that the sovereignty and the ownership of the data belongs exclusively to the principal and after consultation with the principal, if necessary, take appropriate protective measures (e.g. submit objection, applications, etc.).

4.5. The contractor will inform the principal without delay if a supervisory authority acts against the contractor and this activity may affect to the data processed for the contractor. The contractor assists the principal in the fulfillment of his duties (in particular to provide information and tolerating of controls) vis-à-vis supervisory authorities (Article 31 GDPR).

4.6. The contractor shall provide the principal with information concerning the processing of data under this DP Agreement, which are necessary for its fulfillment of statutory obligations (in particular this includes requests from persons affected or authorities and the compliance with his accountability obligations pursuant to Article 5 (2) GDPR, as well as the conducting of a privacy impact assessment pursuant to Article 35 GDPR), provided that the principal can not obtain this information himself. The information must be available to the contractor and does not have to be procured from third parties, whereby employees, agents and subcontractors of the principal are not considered as third parties.

4.7. If the provision of the necessary information and the participation exceeds of contractor's service obligations after the main contract and are not based on a misconduct by the contractor, then the principal must indemnify the contractor separately for the resulting additional expenses.

5. Control powers

5.1. The principal has the right to control compliance with the legal requirements and the provisions of this DP Agreement, in particular the TOMs, at the contractor at any time to the required extent (Article 28 (3) lit. h GDPR).

5.2. On-the-spot controls are made during normal business hours, must be notified by the principal within a reasonable time (at least 14 days, except in emergencies) and must be supported by the contractor (for example, by providing personnel).

5.3. The controls are limited to the necessary scope and must take into account the business and trade secrets of the contractor as well as the protection of personal data of third parties (such as other customers or

employees of the contractor). Only competent persons, who can legitimize themselves and are obliged to maintain secrecy with regard to the business and trade secrets as well as the processes of the contractor and personal data of third parties, are authorized to carry out the control.

5.4. Instead of inspections and on-the-spot controls, the contractor may refer the principal to an equivalent control by independent third parties (e.g. neutral privacy auditors), compliance with approved codes of conduct (Article 40 GDPR) or appropriate data protection or IT security certification pursuant to Article 42 GDPR. This applies in particular if business and trade secrets of the contractor or personal data of third parties would be jeopardized by the controls.

5.5. If the tolerance and participation in the inspections or adequate alternative measures of the principal exceed the contractor's service obligation after the main contract and and are not based on a misconduct by the contractor, then the principal must indemnify the contractor separately for the resulting additional expenses.

6. **Subcontracting conditions**

6.1. If the contractor uses the services of a subcontractor to carry out certain processing activities in the name of the principal, he must give the subcontractor in form of a contract or other legal instrument permitted by the GDPR the same data protection obligations to which the contractor has committed in this DP Agreement (in particular with regard to the compliance with instructions, observance of TOMs, providing information and toleration of controls). In addition, the contractor must carefully select the subcontractor, examine his reliability and monitor his compliance with the contractual and legal requirements (Article 28 (2) and (4) GDPR).

Without prejudice to any limitations imposed by the main contract, the principal expressly agrees that the contractor may use subcontractors as part of order processing.

6.2. The subcontracting conditions already existing at the conclusion of this DP Agreement are specified by the contractor on the website at https://www.sms77.io/en/annex-subcontractors/ and are deemed approved by the contractor.

6.3. The contractor will inform the principal regarding to any changes with the subcontractors on the website at https://www.sms77.io/en/annex-subcontractors/ , which are relevant to order processing. Here, the principal has the opportunity to subscribe to updates via email. The principal shall exercise his right to object regarding to the changes or new subcontractors only in accordance with the principles of good faith as well as the appropriateness and equity.

6.4. Contractual relationships in which the contractor uses the services of third parties as a mere ancillary service to carry out his business activities (e.g. cleaning, guarding or transport services) do not constitute subcontracting processing within the meaning of the above provisions of this DP Agreement. Nevertheless, the processor has to ensure, e.g. by contractual agreements or notes and instructions that the security of the data is not jeopardized and the provisions of this DP Agreement and the data protection regulations are observed.

7. Processing in third countries

7.1. The provision of the contractually agreed data processing takes place exclusively in a member state of the European Union or in another contracting state to the Agreement on the European Economic Area (EEA).

7.2. The processing of orders in a third country, also by subcontractors, requires the prior consent of the proncipal and may only take place if the special conditions of Article 44 et seq. GDPR are met, unless the contractor is bound by the law of the Union or the member states to which the contractor is subject, for processing in a third country; in such a case, the contractor shall inform the principal of these legal requirements prior to processing, unless the relevant law prohibits such notification because of an important public interest (Article 28 (3) p. 2 lit. a GDPR).

7.3. The consent of the principal for processing in a third country shall be deemed to have been granted in regard of the processing operations referred to in **Annex 2 "Subcontracting conditions"**.

8. Duration of the contract, contract termination and data deletion

8.1. This DP Agreement becomes valid upon its conclusion, is concluded for an indefinite period and ends no later than the term of the main contract.

8.2. The right to extraordinary termination remains reserved to the contracting parties, in particular in the case of a serious infringement of the provisions of this DP Agreement and applicable data protection law. The extraordinary termination must in principle be preceded by a warning in good time, but it is not required if it is unlikely that the offending infringements are remedied or they weigh so heavily that adherence to the DP Agreement of the terminating party is unreasonable.

8.3. Upon conclusion of the provision of the processing services under this DP Agreement, the contractor will either delete or give back all personal data collected as well as their copies (and also all documents, process and usage results and data inventory created in connection with the contract relationship), at the choice of the principal, unless under EU law or the law of the Member States there is an obligation to store personal data (Article 28 (1) p. 2 lit. g GDPR). The objection of a right of retention is excluded with regard to the processed data and the associated data carriers. With regard to the deletion or return, the information, verification and control rights of the principal apply in accordance with this DP Agreement.

8.4. For the rest, the obligations arising from this DP Agreement with regard to the data processed in the order remain valid even after the termination of the DP Agreement.

8.5. If the deletion or the return of the data exceed the contractor's service obligation after the main contract and are not based on a misconduct by the contractor, then the principal must indemnify the contractor separately for the resulting additional expenses.

9. Payment

9.1. The payment agreed under this DP Agreement also includes an expense allowance for the working time of the personnel required by the contractor as well as any necessary expenses (such as travel or material costs). If possible, foreseeable and reasonable, the contractor will inform the principal of the amount of the payment by means of an appropriate estimate.

9.2. If the contractor is entitled to payment in accordance with this DP Agreement, this will be charged at an hourly rate of 59.00 EUR net. For the rest, the payment regulations of the main contract apply.

10. Liability

10.1. In the internal relationship to the contractor, alone the principal is responsible to the person affected for compensation for damages suffered by this person affected due to data processing or use in the context of order processing which is inadmissible or incorrect pursuant to data protection laws.

10.2. The contractual parties shall each release themselves from liability if one of the contractual parties proves that it is in no way responsible for the circumstances in which the damage occurred to the person affected.

11. Final provisions, ranking, changes, form of communication, choice of law, place of jurisdiction

11.1. Changes, additional agreements and additions to this DP Agreement and its annexes require a written agreement and the explicit reference to the fact that this is an amendment or supplement to this DP Agreement. This also applies to the waiver of this form requirement.

11.2. This DP Agreement only obliges the contractor to the extent that this is necessary to fulfill the legal obligations, in particular pursuant to Article 28 et seq. GDPR, and does not impose any further obligations on the contractor.

11.3. Subject to an obligation to the written form in this DP Agreement and in the main contract, the communication between the contractor and principal is done within the context of this DP Agreement (in particular with regard to instructions and information) at least in text form (e.g. email). A lesser form (e.g. verbal) may be permitted in the circumstances instead of the text form (e.g. in an emergency situation), but must be immediately confirmed at least in text form. If the written form is required, the written form in the sense of the GDPR is meant.

11.4. It applies the law of the Federal Republic of Germany. The exclusive place of jurisdiction for all disputes arising from or in connection with this DP Agreement is the registered office of the contractor, provided that the principal is a merchant, legal entity under public law or public law special fund or if the principal has no place of jurisdiction in the Federal Republic of Germany. The contractor reserves the right to assert his claims at the legal place of jurisdiction.

sms77
Köhlerkoppel 19 · 24109 Melsdorf
www.sms77.io · support@sms77.io
Tel: +49 4340 4047477 · Fax: +49 4340 4997118
Inhaber: Christian Leo · USt-ID: DE241588166

Melsdorf, 16.5.2018

Place, date, signature of the principal

Place, date, signature of the contractor

Annex 1 – Security concept

Technical and organizational measures pursuant to Article 32 GDPR

Basic measures to safeguard the rights of persons affected, for immediate response in emergencies, requirements of technology development and employee-level data protection:

- There is an internal data protection management, whose compliance is constantly monitored, as well as evaluated on an event-related basis and at least every six months.
- There is a concept which guarantees the safeguarding of the rights of persons affected (information, correction, deletion or limitation of the processing, data transfer, revocation and objections) within the legal deadlines. It includes forms, guidance and established implementation procedures, as well as the names of the persons responsible for implementation.
- There is a concept which guarantees an immediate and legally binding response to breaches of personal data protection (control, documentation, reporting). It includes forms, guidance and established implementation procedures, as well as the names of the persons responsible for implementation.
- The protection of personal data is taking into account the state of the art, the implementation costs and the kind, scope, circumstances and purposes of the processing as well as the different likelihood and severity of the process-related risks to the rights and freedoms of natural persons already during the development or selection of hardware, software and procedures, according to the principle of data protection by technology development and privacy-friendly default settings (Article 25 GDPR).
- The software used is always kept up to date, as are virus scanners and firewalls.
- With regard to data protection, employees are obliged to maintain secrecy, will be informed and instructed, as well as advised of possible liability consequences. If employees work outside company-intern offices or use private devices for operational activities, special regulations exist for the protection of data in these constellations and the securing of the rights of principals of an order processing.
- The keys issued to employees, access cards or codes, as well as authorizations granted with regard to the processing of personal data, are withdrawn after they have left the company or their responsibilities have changed.
- Cleaning personnel, security personnel and other service providers used to fullfil ancillary business tasks are carefully selected, and it will be ensured that they take account into the protection of personal data.

Spatial access control	- Security locks - Access regulations for external persons - Chip cards / transponder locking systems - Window securing - Supervision of auxiliary staff - All data processing servers are located in particularly secured data centers of the current hosts Hetzner Online AG and domainfactory GmbH
Digital access control	- Firewalls (hardware / software). - Constantly up-to-date virus protection - Constantly up-to-date software versions - Authorization / authentication concepts with access regulations restricted to the absolute minimum - Minimum password lenghts and password manager - Locks of external interfaces (USB etc.) - Use of intrusion detecton systems - Encryption of mobile data carriers and devices - Logging of access to data - Proper destruction of data carriers
Transfer control	- Definition and documentation of the recipients - Pseudonymization - Encryption of data carriers and connections (SSH, SSL, VPN). - Dedicated transfer entitlements
Input control	- Logging of data input, changes and deletions - Retention of forms from which data has been transferred to automated processes - Assignment of rights to input, change and delete data based on an authorization concept
Order control	- Selection of contractors under due diligence - Written determination of the instructions - Control of compliance with order
Availability control / integrity	- Emergency conzept - Constantly controlled backup and recovery concept - Additional backup copies with storage in specially protected locations - Regular performance of stress tests
Warranty of the earmarking and separation obligation	- Logical client separation (software side) - Separation of productive and test system - For pseudonymized data: separation of the assignement file and retention on a separate, secured system