Contract on Order Processing

pursuant to Article 28 EU GDPR

between

Company

Street, ZIP, City, Country

- Controller - hereinafter referred to as Principal -

and

SmartWeWorld SE
CAS-Weg 1-5, 76131 Karlsruhe, Germany
- Processor - hereinafter referred to as Contractor -

1. Subject and duration of the order

The subject matter of the order is derived from the Service Agreement of the respective application on the SmartWe platform that has been concluded on (YYYY/MM/DD).

The duration of this order (term) corresponds to the duration of the Service Agreement.

2. Specification of the order content

2.1 Type and purpose of the planned processing of data

Type and purpose of the processing of personal data by the Contractor on behalf of the Principal are specifically described in the Service Agreement.

The performance of the contractually agreed data processing shall take place exclusively in a Member State of the European Union or in another contracting state which is a party to the Agreement on the European Economic Area.

2.2 Data types

The subject of the processing of personal data are the following data types/categories (enumeration/description of the data categories)

- ☐ Address data / personal master data (including position and title)
- ☐ Communication and contact data (e.g. telephone, e-mail)
- ☐ Contract master data (order data, contractual relationship, product or contract interest)
- ☐ Customer history

- ☐ Sales information (e.g. leads, project information)
- ☐ Contract billing and payment data
- ☐ Bank data
- ☐ Health data
- ☐ Social insurance data
- ☐ Planning and control data
- ☐ Information (from third parties, e.g. credit agencies, or from public directories)
- ☐ _____
- ☐ _____

Categories of data subjects

The categories of data subjects affected by processing include:

- ☐ Customers
- ☐ Prospects
- ☐ Subscribers
- ☐ Employees / Workers
- ☐ Applicants
- ☐ Suppliers
- ☐ Service providers / distributors and integration partners
- ☐ Commercial agents
- ☐ Contact persons
- ☐ _____
- ☐ _____

3. Technical and organizational measures

(1) The Contractor shall document the implementation of the technical and organizational measures set out prior to the award of the order before processing, in particular with regard to the specific execution of the order, and provide them over to the Principal for review. If accepted by the Principal, the documented measures become the basis of the order. If the review/ audit undertaken by the Principal results in a need for adjustment, this must be implemented by mutual agreement.

(2) The Contractor shall create the security pursuant to Article 28 (3) (c), 32 GDPR, in particular in conjunction with Article 5 (1), (2) GDPR. Overall, the actions to be taken are data security measures and to ensure a level of protection appropriate to the level of risk with regard to the confidentiality, integrity, availability and resilience of the systems. The state of the art, the implementation costs and the nature, scope and purpose of the processing as well as the different probability and severity of the risk for the rights and freedoms of natural persons within the meaning of Article 32 (1) GDPR must be taken into account. The technical and organizational measures taken by the Contractor are to be documented by the latter in writing. The documentation is attached to this Agreement as Appendix 1.

(3) The technical and organizational measures are subject to technical progress and further development. In that regard, the Contractor is permitted to implement alternative adequate measures. In doing so, the security level of the specified measures must not be reduced. Material changes are to be documented.

4. Rectification, blocking and deletion of data

(1) The Contractor may not rectify or delete the data subject to contracted processing or restrict its processing without authorization, but only in accordance with the Principal's documented instructions. Insofar as a data subject directly addresses the Contractor in this regard, the Contractor shall immediately forward this request to the Principal within the statutory deadline.

(2) Insofar as included in the scope of services, the deletion concept, right to be forgotten, rectification, data portability and information are to be ensured by the Contractor within the statutory deadline.

5. Quality assurance and other obligations of the Contractor

In addition to compliance with the provisions of this order, the Contractor has statutory obligations pursuant to Articles 28 to 33 GDPR; to such extent it shall ensure compliance with the following requirements:

a) Written appointment of a Data Protection Officer who carries out his activity in accordance with Article 38 and 39 GDPR.
b) The current contact data of the Data Protection Officer can be easily accessed on the Contractor's homepage.
c) The preservation of confidentiality pursuant to Article 28 (3) (b), 29, 32 in conjunction with (4) GDPR. The Contractor shall deploy only employees who are committed to confidentiality and who have been previously familiarized with the data protection regulations that are relevant to them. The Contractor and any person subordinated to the Contractor who has access to order-relevant personal data may process such data only in accordance with the instructions of the Principal, including the powers granted herein, unless they are legally obliged to process.
d) The implementation of and compliance with all technical and organizational measures required for this order pursuant to Article 28 (3) Sentence 2 (c), 32 GDPR [details in Appendix 1].
e) On request, the Principal and the Contractor shall cooperate with the supervisory authority in performing their tasks.
f) Immediate notification to the Principal about control procedures and measures adopted by the supervisory authority, insofar as they relate to this order. This also applies insofar as a competent authority investigates the Contractor within the framework of administrative or criminal proceedings with respect to the processing of personal data in order processing.
g) Insofar as the Principal is subject to a review by the supervisory authority, an administrative offense or criminal proceedings, the liability claim of a data subject or a third party or any other claim in connection with order processing by the Contractor, the Contractor shall support the Principal to the best of its ability.
h) The Contractor shall regularly review internal processes and technical and organizational measures to ensure that the processing within his area of responsibility complies with the requirements of applicable data protection law and ensure the protection of the data subject's rights.
i) Verifiability of the technical and organizational measures taken vis-a-vis the Principal within the scope of its supervisory powers under section 7 of this Agreement.

6. Subcontracts

(1) For the purposes of this provision, subcontracts are defined as those services that directly relate to the provision of the main service. This does not include ancillary services which the Contractor avails of, for example, telecommunication services, postal/transport services, maintenance and user services or the disposal of data storage media as well as other measures to ensure the confidentiality, availability, integrity and resilience of the hardware and software of data processing systems. However, the Contractor is obliged to take appropriate and legally compliant contractual agreements and control measures in order to ensure data protection and data security of the Principal's data, even in the case of outsourced ancillary services.

(2) The Contractor may only mandate subcontractors (other processors) after prior express written or documented consent of the Principal. The Principal agrees to the engagement of the subcontractors listed in Appendix 2 under the condition of a contractual agreement in accordance with Article 28 (2)-(4) GDPR.
The further engagement of a new subcontractor or changing the existing subcontractor is permissible insofar as:

- the Contractor notifies such outsourcing to a subcontractor to the Principal within a reasonable time in advance in writing or in text form and
- the Principal does not object to the planned outsourcing in writing or in text form by the time the data is handed over to the Contractor and

a contractual agreement in accordance with Article 28 (2)-(4) GDPR is used.

(3) The transfer of personal data of the Principal to the subcontractor and its initial taking of action are only permitted if all prerequisites for subcontracting have been met.

(4) If the subcontractor provides the agreed service outside the EU/EEA, the Contractor shall ensure admissibility under data protection law by taking appropriate measures. The same applies if service providers within the meaning of para. 1 sentence 2 are to be engaged.

All contractual arrangements in the chain of contract must also be imposed on the additional subcontractor.

7. Principal's rights of control

(1) The Principal has the right to carry out checks in consultation with the Contractor or have them carried out by reviewers to be named in individual cases. The Principal has the right to verify compliance with this agreement by the Contractor in his business through spot checks, which must typically be notified in good time.

(2) The Contractor shall ensure that the Principal can verify compliance with the obligations of the Contractor in accordance with Article 28 GDPR. The Contractor undertakes to provide the Principal, on request, with the necessary information and, in particular, to provide documentary evidence of the implementation of the technical and organizational measures.

(3) Documentary evidence of such measures not merely relating to the specific order can be furnished by way of current certificates, reports, or report abstracts of independent authorities (e.g. public auditor, internal audit department, Data Protection Officer, IT security department, data protection auditors, quality auditors).

(4) The Contractor can assert a claim for remuneration in order to enable the checks to be carried out by the Principal.

8. Notification in case of violations by the Contractor

(1) The Contractor shall assist the Principal in complying with the obligations on security of personal data, reporting of data breaches, data protection impact assessments and prior consultations, as set out in Articles 32 to 36 GDPR. These include:

a) ensuring an adequate level of protection through technical and organizational measures that take into account the circumstances and purposes of the processing and the predicted likelihood and severity of a possible breach of rights by security vulnerabilities, and enable the immediate detection of relevant violations
b) the obligation to report violations of personal data immediately to the Principal
c) the obligation to support the Principal in providing information to the data subject and to provide him with all relevant information without delay in this connection within the statutory deadline
d) the Principal's support for their privacy impact assessment
e) the support of the Principal in the context of prior consultations with the supervisory authority

(2) For support services that are not included in the service specification or are not the result of misconduct by the Contractor, the Contractor may claim compensation.

9. Authority of the Principal to issue instructions

(1) Verbal instructions are confirmed by the Principal immediately (at least in text form).

(2) The Contractor shall inform the Principal without delay if it believes an instruction is contrary to data protection regulations. The Contractor shall be entitled to suspend the implementation of the corresponding instruction until it is confirmed or modified by the Principal.

10. Deletion and return of personal data

(1) Copies and duplicates shall not be created without the Principal's knowledge. This does not include backup copies, to the extent necessary to ensure proper data processing, and data required to comply with statutory retention requirements.

(2) Upon termination of the contractual relationship or prior request by the Principal, the Contractor shall, if requested, electronically transfer the data relating to the contractual relationship to the Principal and subsequently delete it from its data processing systems. If a legal requirement requires storage beyond the end of the contract, the Principal is responsible for complying with the relevant statutory retention periods.

(3) Documentation which is documentary evidence of proper data processing shall be retained by the Contractor above and beyond the agreement end date in accordance with the respective retention periods. It may, to avoid liability, transfer such documentation to the Principal at contract end.

11. Liability and penalties

(1) For damages of the Principal due to culpable breaches of the Contractor of this contract as well as of the legal data protection regulations, the legal liability regulations apply. Insofar as third parties assert claims against the Principal due to the demonstrable breach of data protection regulations caused by the Contractor, which are caused by the collection or use of Principal data contrary to the contract, the Contractor shall indemnify the Principal from these claims upon request.

(2) The Contractor shall bear the burden of proof that any damages are not based on a circumstance for which it is responsible, insofar as the cause of the damage is the collection or use of Principal data under this contract.

12. Final provisions

(1) Amendments of and supplements to and the rescission of this contract shall be made in writing. This shall also apply to the amendment or waiver of the written form requirement.

(2) If a provision in this contract is or becomes ineffective or contains a loophole, this shall have no effect on the validity of the remaining provisions. The parties undertake to replace the ineffective provision with a legally permissible provision that comes closest to the purpose of the invalid provision and that best meets the requirements of Article 28 EU GDPR.

(3) In case of contradictions between this contract and other agreements between the parties, in particular the main contract, the provisions of this contract and other agreements between the parties shall prevail.

_____	Karlsruhe, _____
(Place, Date)	(Place, Date)
_____	_____
(Signature Principal)	(Signature Contractor)

Appendix 1: Technical and organizational measures

1. Confidentiality

1.1. Physical access control

No unauthorized access to data processing systems:

- Security service with connection to the police
- Installed and active motion detectors
- Building access predominantly only with chip key
- Central locking system with security locks
- Access to the server room only for authorized persons
- Central EDP predominantly outsourced in data center (DIN ISO / IEC 27001: 2005) (Housing):
    1. Building secured with fence, barbed wire, grid, roller door and lock system
    2. Access only with chip cards, PIN and keys
    3. Electronic locking system
    4. Alarm systems
    5. Video installations
    6. Locked server racks

1.2. System access control

No unauthorized system usage by:

- Secure, complex passwords and password policy
- Automatic blocking (e.g. password or timeout)
- Setup of a user master record per user
- Encryption of data storage media
- User ID query with password
- Password convention: at least 12 characters with special characters, numbers, upper and lower case
- Activity logs

1.3. Data access control

No unauthorized reading, copying, modification or removal within the system:

- Authorization and administration concept existing
- Access logs by log with logging of policy violations
- Password protected screen lock, timed activation

1.4. Separation control

Separate processing of data collected for different purposes:

- Separate databases for companies and customers
- Processing the project data separately on virtual servers
- Creation of an authorization concept
- Specification of database rights
- Separation of productive and test system

2. Integrity

2.1. Data transfer control

No unauthorized reading, copying, modification or removal during electronic transmission or transport:

- E-mail transmission with encryption can be implemented if required (S/MIME, PDF encryption 256bit)
- Disk encryption
- Encryption of data paths for remote maintenance (VPN, HTTPS)
- Attachments in the e-mails can be encrypted with the current encryption programs if required
- Encryption of data carriers for a possible data carrier transport/ dispatch

2.2. Input control

Determining whether and by whom personal data has been entered, changed or removed in data processing systems:

- All entries/changes in the central CRM genesisWorld are logged
- Logging deletions
- Granting of rights to enter, modify and delete data based on an authorization concept

3. Availability and resilience

3.1. Availability control

Protection against accidental or willful destruction or loss:

- Central EDP outsourced to data center (DIN ISO / IEC 27001: 2005) (Housing)
- Backup concept with full backups and incremental backups, virtualization
- Storage of backups in separate fire protection zone
- Additional backups and tested restorations
- RAID hard disk space
- Virus scanners and multilevel firewalls
- Server room climate control, UPS, nitrogen extinguishing system, fire detector (DC)
- Protection of the entire data center/server with UPS and emergency diesel
- Mirroring the data into a 2nd fire area
- Backup-to-disk with emergency commissioning of virtual machines directly from the backup
- Outsourcing of backup (localization)
- Signature-based IPS (Intrusion Prevention System) for web access to CAS services
- Defined message paths and contingency plans for restart
- Central monitoring of availability, utilization, temperature of the systems incl. escalation management (e-mail, SMS)

3.2. Quick recoverability

- Rapid recovery of “snapshots” created from data multiple times a day

4. Procedures for periodic review, assessment and evaluation

4.1. Data protection management

- Software solution for data protection management used
- External Data Protection Officer

  DATENSCHUTZ perfect GbR, Karlsruhe

  Thomas Heimhalt; contact: cas-datenschutz@SmartWeWorld.de
- Internal working group of data protection officers of the different company divisions
- Clear responsibilities in training/informing employees and developing the necessary measures
- Employees committed to confidentiality / data secrecy
- Annual review of technical protective measures

4.2. Incident response management

- Use of firewall and regular updating
- Use of spam filters and regular updating
- Use of virus scanners and regular updating
- Task and checklists for the technical management of security breaches
- Involvement of the external data protection officer in case of security breaches
- Use of IPS (Intrusion Prevention System) and regular update

4.3. Privacy-friendly default settings

- No more personal data is collected than is necessary for the specific purpose

4.4. Order control

No order processing within the meaning of Article 28 GDPR without corresponding instructions of the Principal:

- Use of the measures taken depending on the order
- Written external data protection officer with deputy
- Compliance with and implementation of the provisions of EU GDPR
- Unambiguous form of contract
- Strict selection of the service provider
- Preliminary conviction duty

Appendix 2: Sub-contractors

Sub-contractors	Activities	Purpose	Data categories	Data subjects
CAS Software AG, Karlsruhe, DE	Hosting, Sales, Service, Support, Accounting	Hosting, Sales, Service, Support, Accounting	Customer an identi-fication data	Customer, Prospective customer