Processing Agreement in accordance with Art. 28 GDPR

[Use of software over the internet, Version: August 2019]

between

_____

_____

_____

– Controller – Hereinafter referred to as Client –

and

weclapp SE

Neue Mainzer Straße 66-68

60311 Frankfurt am Main

– Processor – Hereinafter referred to as Contractor –

1. General

(1) The Contractor processes personal data on behalf of the Client within the meaning of Art. 4 (8) and Art. 28 of Regulation (EU) 2016/679 – General Data Protection Regulation (GDPR). This contract governs the rights and obligations of the parties in relation to the processing of personal data.

(2) This contract expresses the will of the parties within the meaning of Art. 28 GDPR.

(3) Insofar as the terms "data processing" or "processing" (of data) are used in this contract, the underlying definition of "processing" is based on Art. 4 (2) GDPR. Processing of personal data particularly includes collecting, storing, use, disclosure through transfer, distribution or other form of provision, blocking, erasure or other use of data.

2. Object and duration of the processing agreement and contractual content

(1) The Contractor performs various services on behalf of the Client (use of software on the internet and associated services such as support services) within the framework of a "cloud service agreement" that is referenced in this document. This contract specifies the obligations and rights of the Client and Contractor concerning data protection in connection with the processing of the Client's personal data by the Contractor.

(2) The duration of this contract is equivalent to the duration of the cloud service agreement.

(3) The nature and purpose of data processing are based on the agreements reached and based on the Client's instructions. The Contractor is prohibited from processing data in any deviating manner unless the Client has granted consent (at least in text form).

(4) The nature of the personal data includes all types of personal data that the Contractor processes on behalf of the Client. The types of data affected by data processing particularly include:

(Client must adjust if necessary)

☐ Communication data (e.g. phone, email)

☐ Payment data (e.g. IBAN)

☐ Customer data, user data (e.g. name)

☐ Bank data

☐ Employee data

☐

☐

☐

☐

(5) The categories of data subjects affected by data processing particularly include:
(Client must adjust if necessary)
☐ Employees
☐ Interested parties
☐ Suppliers
☐ Applicants
☐ Contacts
☐ Third parties
☐
☐
☐
☐

3. Rights and obligations of the Client

(1) The Client is the controller within the meaning of Art. 4 (7) GDPR for the processing of data by the Contractor on the Client's behalf. The Client has the right to issue supplementary instructions concerning the nature, scope and methods of data processing. The instructions must be issued in writing (at least text form).
(2) If the Client issues supplementary instructions that exceed the contractually agreed services and the Contractor declares its willingness to provide the services, the Contractor is entitled to demand remuneration for the extra efforts.
(3) The Client may appoint individuals who are authorized to issue instructions. If individuals are given authorization to issue instructions, this must occur at least in text form. If there is a change in the individuals who are authorized to issue instructions on behalf of the Client, the Client must promptly inform the Contractor at least in text form.
(4) The Client will promptly inform the Contractor if any errors or discrepancies are detected in the processing of personal data by the Contractor.
(5) If there is an obligation to inform third parties pursuant to Art. 33, 34 GDPR or another statutory information obligation applies for the Client, the Client is responsible for compliance.

4. Rights and obligations of the Contractor

(1) The Contractor is entitled to carry out data processing under this agreement in Member States of the European Union, the European Economic Area, or in a third country while observing mandatory applicable regulations.
(2) For core functions of the software (e.g. offer management, customer and contact management), the Contractor carries out data processing under

this agreement only in Member States of the European Union or the European Economic Area – unless otherwise agreed.

(3) The Contractor is obliged to organize its company and operational processes such that the data processed on behalf of the Client is secured to the necessary extent and protected against unauthorized interception by third parties.

(4) The Contractor will promptly inform the Client if the Contractor believes that an instruction issued by the Client violates data protection regulations. The Contractor is entitled to suspend the performance of the instruction in question until this is confirmed or modified by the Client. If the Contractor can prove that processing according to the Client's instructions may cause the Contractor to be liable pursuant to Art. 82 GDPR, the Contractor is free to suspend further processing until the parties have resolved the question of liability.

(5) The Contractor is obliged to inform the Client upon gaining knowledge of any breaches in the protection of personal data that occur while processing the Client's data. The Contractor will inform the Client if a supervisory authority takes action against the Contractor pursuant to Art. 58 GDPR and this concerns monitoring of the processing which the Contractor carries out on behalf of the Client.

(6) The Contractor will support the Client with compliance with the obligations named in Article 32 to 36 of the GDPR concerning the security of personal data, reporting obligations in case of data breaches, data protection impact assessment and prior consultation. The Contractor is aware that the Client may have a reporting obligation pursuant to Art. 33, 34 GDPR that involves a report to the supervisory authorities within 72 hours upon obtaining knowledge. The Contractor will assist the Client with implementing these reporting obligations. In particular, the Contractor will inform the Client of any unauthorized access to personal data processed on behalf of the Client immediately after obtaining knowledge of such access.

(7) The Contractor may demand remuneration for support services that are not caused by misconduct on the part of the Contractor.

5. Data protection officer of the Contractor

(1) The Contractor confirms that a company data protection officer has been appointed pursuant to Art. 37 GDPR.

(2) The Contractor ensures that the data protection officer has the necessary qualifications and the required specialist knowledge.

(3) The contact data for the data protection officer has been placed in an easily accessible location on the Contractor's homepage. On request, the Contractor can provide the Client with the name and contact details of the data protection officer.

6. Subcontractual relationships

(1) The Contractor is only permitted to engage subcontractors to process the Client's data with the consent of the Client. The Client consents to the engagement of the subcontractors listed in Annex 2. The Contractor is granted general authorization to engage additional subcontractors to process the Client's data or to change the existing subcontractor as long as the Contractor informs the Client concerning every intended change with respect to bringing in or replacing a subcontractor and the Client does not make an objection to the Contractor (at least in text form) within 2 weeks after obtaining the information.

(2) Objection is only permitted if bringing in or replacing a subcontractor would result in processing that does not comply with data protection regulations.

(3) If the Client submits a justified objection to the engagement or replacement, the Contractor is entitled to terminate the cloud services agreement along with the accompanying services within a 4 week notice period.

(4) The contract with the subcontractor must be drawn up in writing, which also includes electronic formats. The Contractor must oblige the subcontractor to observe the same obligations that are stipulated in this contract pursuant to Art. 28 (3) GDPR.

(5) Services for which the Contractor engages third parties as a secondary service to fulfill business activities are not considered subcontractual relationships. This includes cleaning services, mailing services, telecommunications services and guarding services. However, the Contractor is obligated to adopt suitable preventive measures to protect personal data during these services as well. The maintenance and upkeep of IT systems or applications is a subcontractual relationship requiring authorization and is considered contract processing within the meaning of Art. 28 GDPR if it involves the maintenance and inspection of such IT systems that are also used in connection with the provision of services for the Client and if personal data that is processed on behalf of the Client can be accessed during maintenance.

7. Control rights of the Client

(1) The Contractor will allow the Client to review, in particular, compliance with the Contractor's technical and organizational measures. To this end, the Client may request information or conduct an on-site inspection. The Contractor may also demonstrate compliance with technical and organizational measures by observing approved codes of conduct pursuant to Art. 40 GDPR, updated certificates, reports or excerpts from reports of independent entities (e.g. auditor, IT security department or data protection officer), certification under a suitable certification process pursuant to Art. 42 GDPR or suitable certification through an IT security audit or data protection audit. The Contractor and Client agree that verification can also

be provided in the form of other evidence plausibly demonstrating that the Contractor carries out its activities carefully and conscientiously in compliance with the requirements of the GDPR.

(2) After agreeing on a date and time, the Client may conduct an on-site inspection at the Contractor's premises during the Contractor's business hours. The Contractor will assist the Client in carrying out the inspection and cooperate with the complete and rapid performance of the inspection. To this end, the Contractor will provide the Client with the necessary information and verify that the technical and organizational measures have been implemented if this is necessary in order to conduct the inspection.

(3) The Contractor is entitled to demand remuneration for facilitating the inspection.

8. Confidentiality obligation

(1) The Contractor declares that he is aware of the relevant applicable regulations of data protection law and that he is familiar with their application.

(2) The Contractor ensures that the employees engaged with the processing of personal data have committed to data secrecy and/or confidentiality and are familiar with the data protection provisions that are relevant for them.

9. Preserving the rights of data subjects

(1) The Client bears sole responsibility for preserving the rights of data subjects. The Contractor is obliged to assist the Client with the Client's duty to handle requests from data subjects pursuant to Art. 12-22 GDPR. The Contractor will inform the Client if data subjects address requests concerning their rights to the Contractor.

(2) If the Client requires the cooperation of the Contractor to preserve the rights of data subjects (in particular the rights to access information, rectification, blocking or erasure), the Contractor will assist the Client if requested to do so (at least in text form).

(3) (3) The Contractor will assist the Client in providing information. The precondition is that the Client must request the Contractor to do so (at least in text form).

(4) The Contractor may demand remuneration from the Client for support measures carried out in connection with pursuing the rights of data subjects.

10. Technical and organizational measures for data security

(1) The Contractor ensures the Client that the Contractor will observe the technical and organizational measures that are necessary for compliance with the applicable data protection regulations. In particular, this includes the regulations in Art. 32 GDPR.

(2) The latest status of the technical and organizational measures that have been implemented is documented in Annex 1 and will be provided to the Client for review.

(3) The parties agree that it may be necessary to modify the technical and organizational measures in order to adapt to the technical and legal circumstances. The Contractor is therefore entitled to adjust the technical and organizational measures if corresponding changes occur. Significant changes will be documented. The Client is entitled to request an updated version of the technical and organizational measures at any time.

11. Termination

(1) After the termination of the cloud service agreement, the Contractor must return to the Client all documents that were handed over (including any existing copies) with personal data or to delete this data at the request of the Client unless there is an obligation to store the data according to Union law or the laws of the Federal Republic of Germany.

(2) The Client may exercise its choice (return or erasure of personal data) up until the termination date of the cloud service agreement at the latest (at least in text form). If the Client does not exercise its choice, the Contractor will erase all the Client's personal data 14 days after the termination of the agreement.

(3) This erasure must be appropriately documented and confirmed to the Client on request (at least in text form).

(4) If the Client desires a return transfer of the data processed in the weclapp cloud, this requires a separate agreement.

12. Right of retention

The parties agree that the contractor is not entitled to invoke the right of retention within the meaning of Section 273 BGB concerning the processed data.

13. Release from liability in the event of Art. 82 (4) GDPR

If the Contractor or Client are subject to liability/claims asserted by a data subject pursuant to Art. 82 (4) GDPR, they agree to mutually release one another, at first request, from all claims corresponding to the other party's share in responsibility for the damages under the conditions stipulated in Art. 82 (2) GDPR.

14. Cancellation of the "Processing Agreement" pursuant to Section 11 BDSG

If the Client and Contractor established a processing agreement pursuant to Section 11 BDSG for the cloud service agreement, this is canceled by mutual agreement upon entering into this processing agreement pursuant to Art. 28 GDPR.

15. Final provisions

(1) If individual parts of this contract should be ineffective, this will not affect the validity of the remaining provisions of the contract.

(2) For all legal relationships between the contracting parties, the laws of the Federal Republic of Germany that are authoritative for legal relationships between domestic parties apply, to the exclusion of private international law.

(3) The place of jurisdiction is Marburg/Lahn. Any exclusive place of jurisdiction remains unaffected by this.

_____, _____ Frankfurt am Main, _____

Place Date Place Date

_____ _____

– Client – – weclapp SE –

Annex 1 Technical and organizational measures for data security pursuant to Art. 32 (1) GDPR

I. Encryption (Art. 32 (1)(a) GDPR)

The Contractor uses encryption methods for the electronic transfer of data.

II. Confidentiality (Art. 32 (1)(b) GDPR)

1. Access control and entry control

Entry control

Marburg location

The business premises at the Marburg location are subdivided into several security areas. Visitors must identify themselves at the reception and are only guided to the relevant security areas in the company of their contacts. Access to the security areas is protected through an automatic access control system. Issuing keys for the security areas is managed and monitored centrally and access authorizations are distributed according to the role concept and user privileges established on this basis. Authorized personnel are verified in the access control system using a chip card/transponder lock system. Only restricted personnel are allowed to access particularly critical systems like the server room. Access areas are secured by alarm systems. In case of unauthorized access to the server rooms, alarm signals are transmitted at several different security levels; the most critical level is transmitted to the nearest police station. Motion sensors are used within the areas. Security staff and cleaning staff are chosen carefully.

Kitzingen location

Entry to the Kitzingen location is protected by an electronic access system. Access is only permitted for employees with an electronic key. Entry to the premises is recorded by the electronic access system. The role concepts and user rights are centrally regulated for all employees at all locations. Accordingly, the measures described above for the Marburg location also apply for the Kitzingen location.

Access control

The data processing systems are protected particularly by antivirus software, firewall systems (hardware/software) and proxy servers. Management of the security software is regularly secured and is only carried out by authorized personnel. Authorization of personnel is ensured through assigned user rights and user profiles. Through these profiles, verification may be carried out on the respective IT systems using a user name and password. Access to the data processing systems occurs via secure connections (including VPN technology).

2. Access control

Rights are granted according to the authorization concept and management is the responsibility of the system administrators. As a rule, the number of administrators is limited to what is "strictly necessary". To ensure that only authorized personnel have access to data, storage media and data are encrypted and access is regulated using user rights. A password guideline obligates employees to select passwords that are technically and organizationally appropriate and to change them regularly. Access to systems and applications is password-protected and depends on user rights: each employee can only access the necessary functions to perform his or her work within the scope of his or her responsibility. The Contractor observes the principle of generating as little printed matter as possible. Document shredders are used for disposal. Data storage media are stored and locked in secure areas with restricted access. A service provider is engaged for proper destruction of storage media. This destruction will be recorded and monitored. Unlawful access to systems or to data integrity via security gaps in programs is prevented by regular scans of the network infrastructure and prompt rectification of problems that are identified. In this way, both external and internal accesses are detected and their impact is minimized.

3. Separation control

The Contractor complies with the requirements of the GDPR to process data separately that is collected for different purposes. This requirement is clarified by organizational separation of roles and administration of security areas; this principle is largely fulfilled within the departments as well. Data collected for different clients is managed separately and processed separately. A comprehensive authorization concept was developed to guarantee this separation which also provides the basis for database rights. Logical client separation is provided and guaranteed in the software. Test environments are managed independently of the production system: customer data will not be carried over into this test system and such transfers are technically prevented.

III. Integrity (Art. 32 (1)(b) GDPR)

1. Transfer control

The electronic exchange of data is monitored by security systems. Unauthorized removal of data storage media in the company is restricted through security areas. Guidelines are issued for the respective areas that prevent the unauthorized removal of data storage media. Data storage media are also encrypted. Discarded storage media are retained in sealed containers and destroyed according to the requirements. Implementation relies on a dual-review principle. There is also an assignment of rights to enter, modify and erase data based on an authorization concept. Secure transport containers are used during physical transport of data storage media.

2. Input control

Restricted assignment of rights limits the input, modification or removal of personal data in data processing systems. The input, modification and removal of data by the respective user is recorded and is traceable. A list has been created defining which applications may be used to input, modify and erase data. The assignment of rights to enter, modify and erase data is based on an authorization concept.

IV. Availability and resilience (Art. 32 (1)(b) GDPR) and recoverability in a timely manner (Art. 32 (1)(c) GDPR

To limit accidental destruction or loss during contract-based data processing, a backup and recovery concept has been created and implemented and recovery is regularly tested. Data backups are stored in a secure off-site location. To ensure the regular and secure operation of systems even in case of disruptions to the power grid, an uninterruptible power supply (UPS) is used in combination with an emergency generating system. The server room is secured through various surveillance and alarm systems, particularly including devices to monitor temperature and humidity as well as fire alarms and smoke alarms. Measures for risk mitigation such as organized distribution of fire extinguishers and installation of fire dampers are a matter of course. Regular maintenance of alarm systems and control systems takes place at defined intervals. Spaces are designed based on their purpose and fulfill the typical security requirements. In this regard, care is taken to position areas requiring special protection in isolated zones and to safeguard them against breakdowns. An emergency concept has been developed to this end and the necessary relevant measures have been implemented.

V. Process for regular review, assessment and evaluation (Art. 32 (1)(d) GDPR)

1. Order control

The Contractor processes the data submitted according to the established contract and observes the statutory regulations and contractually defined requirements according to the Client's instructions. In this way, the transfer of data to unauthorized third parties is excluded by contract and the scope of instructions is defined. For subcontracts, the mandatory content of Art. 28 GDPR is primarily considered when defining this scope. The Contractor will enable the Client to review the documentation of "technical/organizational measures", or where necessary, an on-site visit to the data processing systems. In this way, the Contractor enables and assists with the option of inspecting the Contractor and the Contractor's data processing activities.

2. Data protection management

The Contractor's employees are regularly informed about the requirements of data protection. All of the Contractor's employees commit to data secrecy and agree to maintain confidentiality. This is documented in a docket. A data protection officer has been appointed who is involved with all questions concerning the protection of personal data. The data protection officer monitors compliance with the requirements of data protection and is supported by data protection coordinators.

3. Data protection through technological design and configurations that facilitate data protection

The principle of data protection through technological design and configurations that facilitate data protection is observed through a variety of measures. For instance, two-factor authentication prevents unauthorized individuals from gaining unauthorized access to the Client's account. The Contractor is allowed to assign authorizations to data and software applications in a flexible manner, for instance by issuing read and write permissions. The option of erasing data depends on the assigned authorization. Mandatory fields are restricted to a minimum.

Annex 2 Subcontractors pursuant to Art. 28 (2) GDPR

Subcontractor	Service
1&1 IONOS Cloud GmbH (formerly known as ProfitBricks GmbH) Greifswalder Straße 207 10405 Berlin	Provision of data center services in the form of IaaS cloud computing.