Auftragsverarbeitungsvertrag gemäß Art. 28 DSGVO

Stand: April 2024

zwischen

_____

_____

_____

– Verantwortlicher – nachstehend „Auftraggeber“ –

und

weclapp GmbH

Friedrich-Ebert-Straße 28
97318 Kitzingen

– Auftragsverarbeiter – nachstehend „Auftragnehmer“ –

Auftraggeber und Auftragnehmer werden nachstehend als „Vertragsparteien“ und einzeln als „Vertragspartei“ bezeichnet.

Data Processing Agreement in accordance with Art. 28 GDPR

Version: April 2024

between

– Controller – Hereinafter referred to as “Client" –

and

– Processor – Hereinafter referred to as “Contractor” –

Client and Contractor hereinafter referred to as “Parties” and individually as a “Party”.

PRÄAMBEL

(1) Der Auftragnehmer ist ein Entwickler und Anbieter von Unternehmenssoftwarelösungen für kleinere und größere Unternehmen.
(2) Der Auftragnehmer stellt seinen Kunden eine Unternehmenssoftware zur Verfügung, die ein breites Spektrum von Branchen bedient und zahlreiche Geschäftsprozesse unterstützt (nachstehend „**Dienstleistungen**“).
(3) Die Vertragsparteien haben einen Vertrag über die Nutzung der vom Auftragnehmer entwickelten Software geschlossen, auf den die Nutzungsbedingungen Anwendung finden (nachstehend „**Dienstleistungsvertrag**“).
(4) Im Rahmen der Erbringung der Dienstleistungen und des Dienstleistungsvertrags verarbeitet der Auftragnehmer im Auftrag des Auftraggebers bei der Erfüllung des Dienstleistungsvertrags mit dem Auftraggeber personenbezogene Daten (nachstehend „**personenbezogene Daten**“).
(5) In Anbetracht der vorstehenden Rahmenbedingungen haben die Vertragsparteien vereinbart, diesen Auftragsverarbeitungsvertrag (nachstehend „**Auftragsverarbeitungsvertrag**“) zu schließen.

1. Allgemeines

(1) Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers i. S. d. Art. 28 der Verordnung (EU) 2016/679 (Datenschutz-Grundverordnung, DSGVO). Dieser Auftragsverarbeitungsvertrag regelt die Rechte und Pflichten der Vertragsparteien im Zusammenhang mit der Verarbeitung von personenbezogenen Daten.
(2) Dieser Auftragsverarbeitungsvertrag enthält nach dem Willen der Vertragsparteien den Vertrag im Sinne des Art. 28 DSGVO.
(3) Begriffe wie „Verarbeitung“, „personenbezogene Daten“, „Verantwortlicher“ und „Auftragsverarbeiter“ haben die ihnen in der Datenschutz-Grundverordnung (2016/679/EU; nachstehend „DSGVO“) zugewiesene Bedeutung.

2. Gegenstand und Laufzeit des Auftragsverarbeitungsvertrags sowie Vertragsinhalt

(1) Dieser Auftragsverarbeitungsvertrag gilt ausschließlich für die Verarbeitung personenbezogener Daten im Auftrag des Auftraggebers im Rahmen des Dienstleistungsvertrags zwischen den Vertragsparteien für die Erbringung der Dienstleistungen. Dieser Auftragsverarbeitungsvertrag ist wesentlicher Bestandteil des Dienstleistungsvertrags und alle Bestimmungen des Dienstleistungsvertrags gelten auch für diesen Auftragsverarbeitungsvertrag.
(2) Der Auftragnehmer wird die personenbezogenen Daten nur in der Weise und in dem Umfang verarbeiten, wie dies für die Erbringung der Dienstleistungen im Rahmen des Dienstleistungsvertrags notwendig ist, es sei denn, dies ist erforderlich, um eine gesetzliche Verpflichtung zu erfüllen, der der Auftragnehmer unterliegt, oder um Weisungen des Auftraggebers zu befolgen. Der Auftragnehmer darf die personenbezogenen Daten keinesfalls für andere Zwecke verarbeiten.
(3) Die Laufzeit dieses Auftragsverarbeitungsvertrags entspricht der Laufzeit des Dienstleistungsvertrags.
(4) Der Umfang, die Art und der Zweck der Verarbeitung sowie die Art der personenbezogenen Daten und die Kategorien der betroffenen Personen sind in Anlage 1 dieses Auftragsverarbeitungsvertrags aufgeführt.
(5) Für den Fall, dass der Auftraggeber als Auftragsverarbeiter i. S. d. Art. 4 Nr. 8 DSGVO betrachtet wird, gilt der Auftragnehmer als Unterauftragsverarbeiter und die Bedingungen dieses Auftragsverarbeitungsvertrags bleiben in vollem Umfang gültig.

3. Rechte und Pflichten des Auftraggebers

(1) Der Auftraggeber ist der Verantwortliche i. S. d. Art. 4 Nr. 7 DSGVO für die Verarbeitung von Daten durch den Auftragnehmer im Auftrag des Auftraggebers. Der Auftraggeber hat das Recht, ergänzende Weisungen über Art, Umfang und Verfahren der Datenverarbeitung zu erteilen. Die Weisungen müssen schriftlich (mind. Textform) erfolgen.
(2) Erteilt der Auftraggeber ergänzende Weisungen, die über die vertraglich vereinbarten Leistungen hinausgehen, und erklärt sich der Auftragnehmer zur Leistungserbringung bereit, ist der Auftragnehmer berechtigt, eine Vergütung für den Mehraufwand zu verlangen.
(3) Der Auftraggeber kann weisungsberechtigte Personen benennen. Sofern weisungsberechtigte Personen benannt werden, muss dies mindestens in Textform erfolgen. Für den Fall, dass sich

WHEREAS

(1) The Contractor is a developer and supplier of business software solutions for smaller and larger sized companies.

(2) The Contractor provides business software serving a wide range of branches and supporting multiple business processes to its customers (hereinafter to be referred to as: the “**Services**”).

(3) The Parties have concluded an agreement for the use of the software developed by Contractor under which the Terms of Use are applicable (hereinafter to be referred to as: the “**Service Agreement**”).
(4) Pursuant to the provision of the Services and the Service Agreement, the Contractor will be processing personal data (hereinafter to be referred to as: the “**Personal Data**”) on behalf of the Client in the course of the performance of the Service Agreement with the Client.
(5) In consideration of the foregoing premises, Parties have agreed to enter into this data processing agreement (hereinafter to be referred to as: the “**Data Processing Agreement**”).

1. General

(1) The Contractor processes Personal Data on behalf of the Client within the meaning of art. 28 of Regulation (EU) 2016/679 – General Data Protection Regulation (GDPR). This Data Processing Agreement governs the rights and obligations of the Parties in relation to the processing of Personal Data.

(2) This Data Processing Agreement expresses the will of the Parties within the meaning of Art. 28 GDPR.
(3) Terms such as “processing”, “personal data”, “controller” and “processor” shall have the meaning ascribed to them in the General Data Protection Regulation (2016/679/EU) (hereinafter to be referred to as: “GDPR”).

2. Subject-matter and duration of the Data Processing Agreement and contractual content

(1) This Data Processing Agreement applies exclusively to the processing of Personal Data on behalf of the Client in the scope of the Service Agreement between the Parties for the provision of the Services. This Data Processing Agreement forms an integral part of the Service Agreement, and all the provisions of the Service Agreement are applicable on this Data Processing Agreement.

(2) The Contractor will only process the Personal Data in such manner and to the extent necessary for the provision of the Services under the Service Agreement, except as required to comply with a legal obligation to which the Contractor is subject, or to follow instructions of the Client. The Contractor shall never process the Personal Data for any other purposes.

(3) The duration of this Data Processing Agreement is equivalent to the duration of the Service Agreement.
(4) The extent, nature and purpose of the processing, the type of Personal Data and the categories of data subjects are specified in Annex 1 to this Data Processing Agreement.

(5) In the event the Client is considered to be a processor within the meaning of article 4(8) GDPR, the Contractor is considered to be a sub-processor and the terms and conditions of this Data Processing Agreement will remain in full force and effect.

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

die weisungsberechtigten Personen beim Auftraggeber ändern, wird der Auftraggeber dies dem Auftragnehmer unverzüglich mindestens in Textform mitteilen.
(4) Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten im Zusammenhang mit der Verarbeitung personenbezogener Daten durch den Auftragnehmer feststellt.
(5) Für den Fall, dass eine Informationspflicht gegenüber Dritten nach Art. 33, 34 DSGVO oder einer sonstigen, für den Auftraggeber geltenden gesetzlichen Meldepflicht besteht, ist der Auftraggeber für deren Einhaltung verantwortlich.

4. Rechte und Pflichten des Auftragnehmers

(1) Der Auftragnehmer führt die Datenverarbeitung im Rahmen dieses Auftragsverarbeitungsvertrags grundsätzlich in den Mitgliedstaaten der Europäischen Union (EU) bzw. des Europäischen Wirtschaftsraums (EWR) durch. Der Auftragnehmer darf personenbezogene Daten auch außerhalb der EU bzw. des EWR verarbeiten, wenn in dem Drittland entsprechende Unterauftragnehmer unter Einhaltung der Anforderungen in Ziffer 5 eingesetzt werden und die Anforderungen von Art. 44 bis 48 DSGVO erfüllt sind oder eine Ausnahme i. S. v. Art. 49 DSGVO vorliegt.
(2) Der Auftragnehmer ist verpflichtet, sein Unternehmen und seine Betriebsabläufe so zu gestalten, dass die Daten, die er im Auftrag des Auftraggebers verarbeitet, im jeweils erforderlichen Maß gesichert und vor einem unbefugten Abfangen durch Dritte geschützt sind.
(3) Der Auftragnehmer verarbeitet personenbezogene Daten im Rahmen des Dienstleistungsvertrags und ggf. in Übereinstimmung mit dokumentierten ergänzenden Weisungen des Auftraggebers. Hiervon ausgenommen sind gesetzliche Regelungen, durch die der Auftragnehmer möglicherweise verpflichtet ist, die Daten in anderer Weise zu verarbeiten.
(4) Der Auftragnehmer wird den Auftraggeber unverzüglich benachrichtigen, wenn eine vom Auftraggeber oder in dessen Namen erteilte Weisung nach seiner Auffassung gegen datenschutzrechtliche Bestimmungen verstößt. Der Auftragnehmer ist berechtigt, die Ausführung der betreffenden Weisung solange auszusetzen, bis diese vom Auftraggeber bestätigt oder geändert wird. Sofern der Auftragnehmer darlegen kann, dass die Verarbeitung nach Weisung des Auftraggebers zu einer Haftung seitens des Auftragnehmers nach Art. 82 DSGVO führen könnte, steht es dem Auftragnehmer frei, die weitere Verarbeitung insoweit bis zu einer Klärung der Haftung zwischen den Vertragsparteien auszusetzen.
(5) Der Auftragnehmer ist verpflichtet, dem Auftraggeber jede ihm bekannt gewordene Verletzung des Schutzes personenbezogener Daten unverzüglich mitzuteilen, die im Zuge der Verarbeitung von Daten des Auftraggebers auftritt. Der Auftragnehmer wird den Auftraggeber informieren, wenn eine Aufsichtsbehörde gegen den Auftragnehmer gemäß Art. 58 DSGVO tätig wird und dies die Kontrolle der Verarbeitung betrifft, die der Auftragnehmer im Auftrag des Auftraggebers durchführt.
(6) Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in Art. 32 bis 36 DSGVO genannten Pflichten hinsichtlich der Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, der Datenschutz-Folgenabschätzung und der vorherigen Konsultation. Dem Auftragnehmer ist bekannt, dass für den Auftraggeber eine Meldepflicht nach Art. 33, 34 DSGVO bestehen kann, die eine Meldung an die Aufsichtsbehörde binnen 72 Stunden nach Bekanntwerden vorsieht. Der Auftragnehmer wird den Auftraggeber bei der Umsetzung dieser Meldepflichten unterstützen. Insbesondere wird der Auftragnehmer dem Auftraggeber jeden unbefugten Zugriff auf personenbezogene Daten, die im Auftrag des Auftraggebers verarbeitet werden, unverzüglich ab Kenntnis des Zugriffs mitteilen.
(7) Für die Unterstützungsleistungen, die nicht auf ein Fehlverhalten des Auftragnehmers zurückzuführen sind, kann der Auftragnehmer eine Vergütung verlangen.

5. Unterauftragsverhältnisse

(1) Der Auftragnehmer ist berechtigt, Unterauftragsverarbeiter i. S. d. Art. 28 DSGVO zu beauftragen. Der Auftraggeber stimmt der derzeitigen Beauftragung von Unterauftragsverarbeitern zu, die unter https://www.weclapp.com/de/datenschutz/unterauftragsverarbeiter aufgeführt sind.
(2) Dem Auftragnehmer wird die allgemeine Genehmigung eingeräumt, weitere Unterauftragsverarbeiter mit der Verarbeitung der Daten des Auftraggebers zu beauftragen oder den bestehenden Unterauftragsverarbeiter zu wechseln, vorausgesetzt, der Auftragnehmer informiert den Auftraggeber über jede beabsichtigte

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 immediately 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 shall generally carry out data processing under this Data Processing Agreement in Member States of the European Union (EU), the European Economic Area (EEA). The Contractor is also permitted to process Personal Data outside the EU or EEA if corresponding subcontractors are used in the third country in compliance with the requirements of Section 5 and the requirements of Art. 44-48 of the GDPR are met or an exception as defined in Art. 49 of the GDPR exists.

(2) 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.

(3) The Contractor shall process Personal Data within the scope of the Service Agreement and/or in compliance with any supplementary, documented instructions issued by the Client. Excluded from this are legal regulations which may oblige the Contractor to process the data in a different manner.

(4) The Contractor will immediately inform the Client if the Contractor believes that an instruction issued by or on behalf of 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 without undue delay 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 Art. 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 without undue delay 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. Subcontractual relationships

(1) The Contractor is permitted to engage Sub-Processors within the meaning of Art. 28 GDPR. The Client consents to the currently engagement of the Sub-Processors listed at https://www.weclapp.com/en/privacy/sub-processors.

(2) The Contractor is granted general authorization to engage additional Sub-Processors 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

Änderung in Bezug auf die Hinzuziehung oder Ersetzung eines Unterauftragnehmers und der Auftraggeber erhebt gegenüber dem Auftragnehmer keinen Einspruch (mind. Textform) innerhalb von 4 Wochen nach Erhalt der Information.
(3) Ein Einspruch gegen die beabsichtigte Änderung kann nur aus einem wichtigen datenschutzrelevanten Grund erfolgen. Erhebt der Auftraggeber gegen die Hinzuziehung oder Ersetzung einen zulässigen Einspruch, ist der Auftragnehmer berechtigt, die Leistung ohne die beabsichtigte Änderung zu erbringen oder – wenn die Erbringung der Leistung ohne die beabsichtigte Änderung für den Auftragnehmer nicht zumutbar ist – die von der Änderung betroffene Leistung innerhalb von 2 Wochen nach Zugang des Einspruchs mit einer Frist von 4 Wochen zu kündigen.
(4) Der Auftragnehmer hat dem Unterauftragsverarbeiter dieselben Verpflichtungen aufzuerlegen, die in diesem Auftragsverarbeitungsvertrag gemäß Art. 28 Abs. 3 DSGVO festgelegt sind.
(5) Nicht als Unterauftragsverarbeiterverhältnisse gelten Dienstleistungen, für die der Auftragnehmer Dritte als Nebendienstleistung zur Erfüllung der geschäftlichen Tätigkeit beauftragt. Dazu zählen insbesondere Reinigungsleistungen, Postdienste, Telekommunikationsleistungen und Bewachungsdienste. Der Auftragnehmer ist jedoch verpflichtet, auch bei diesen Dienstleistungen geeignete Vorkehrungen zum Schutz personenbezogener Daten zu treffen.

to the Contractor (at least in text form) within 4 weeks after obtaining the information.

(3) The objection to the intended change can only be made for an important data protection reason. If the Client submits a justified objection to the engagement or replacement, the Contractor shall be entitled to provide the service without the intended change or – if the provision of the service without the intended change is not reasonable for the Contractor – to terminate the service affected by the change within 2 weeks after receipt of the objection with a notice period of 4 weeks.

(4) The Contractor must impose the same obligations on the Sub-Processor that are stipulated in this Data Processing Agreement pursuant to Art. 28 (3) GDPR.

(5) Services for which the Contractor engages third parties as a secondary service to the business activities are not considered as Sub-Processor relationships. This includes in particular 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.

6. Kontrollrechte des Auftraggebers

(1) Der Auftragnehmer ermöglicht dem Auftraggeber, sich insbesondere von der Einhaltung der technischen und organisatorischen Maßnahmen durch den Auftragnehmer zu überzeugen. Dazu kann der Auftraggeber Auskünfte einholen oder eine Vor-Ort-Kontrolle durchführen. Der Nachweis der Einhaltung der technischen und organisatorischen Maßnahmen kann durch den Auftragnehmer auch durch Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DSGVO, aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z. B. Wirtschaftsprüfer, IT-Sicherheitsabteilung oder Datenschutzbeauftragter), Zertifizierung nach einem geeigneten Zertifizierungsverfahren gemäß Art. 42 DSGVO oder geeignete Zertifizierung durch ein IT-Sicherheits- oder Datenschutzaudit erbracht werden. Auftragnehmer und Auftraggeber sind sich darüber einig, dass der Nachweis zudem durch sonstige Nachweise erbracht werden kann, die wahrscheinlich machen, dass der Auftragnehmer seine Tätigkeiten unter Einhaltung der Vorgaben der DSGVO sorgfältig und gewissenhaft erbringt.
(2) Der Auftraggeber kann nach Vereinbarung eines Termins (einschließlich Uhrzeit) eine Kontrolle am Sitz des Auftragnehmers zu den Geschäftszeiten des Auftragnehmers vornehmen. Der Auftraggeber sorgt dafür, dass die Kontrollen nur im erforderlichen Umfang durchgeführt werden, um den Betrieb des Auftragnehmers durch die Kontrollen nicht unverhältnismäßig zu stören. Die Vertragsparteien gehen davon aus, dass eine Kontrolle nicht häufiger als einmal pro Jahr erforderlich ist. Weitere Kontrollen sind vom Auftraggeber konkret zu begründen. Der Auftragnehmer wird den Auftraggeber bei der Durchführung der Kontrolle unterstützen und an der vollständigen und zügigen Durchführung der Kontrolle mitwirken. Der Auftragnehmer wird dem Auftraggeber hierzu erforderliche Auskünfte erteilen und die Umsetzung der technischen und organisatorischen Maßnahmen nachweisen, soweit dies für die Durchführung der Kontrolle erforderlich ist.
(3) Der Auftragnehmer ist berechtigt, für die Ermöglichung der Kontrolle eine Vergütung zu verlangen. Die Grundlage für die Kostenberechnung wird dem Auftraggeber vom Auftragnehmer vor der Durchführung der Kontrolle mitgeteilt.

6. 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 Client shall ensure that the inspections are only carried out to the extent necessary in order not to disproportionately disrupt the Contractor's operations as a result of the inspections. The Parties assume that an inspection is required no more than once a year. Further inspections shall be justified by the Client stating the reason. 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. The basis of the cost calculation shall be communicated to the Client by the Contractor prior to the performance of the inspection.

7. Geheimhaltungspflicht

(1) Der Auftragnehmer wird alle personenbezogenen Daten streng vertraulich behandeln.
(2) Der Auftragnehmer gewährleistet, dass alle zur Verarbeitung personenbezogener Daten berechtigten Personen zur Vertraulichkeit verpflichtet worden sind.
(3) Diese Verpflichtungen hindern eine Vertragspartei nicht an der Weitergabe von Informationen an Dritte, wenn eine derartige Weitergabe nach geltendem Recht vorgeschrieben ist.

7. Confidentiality obligation

(1) The Contractor will treat all Personal Data as strictly confidential.
(2) The Contractor shall ensure that all persons authorized to process the Personal Data are bound to confidentiality.

(3) These obligations will not prevent a Party from sharing information with a third party to the extent such disclosure is mandatory under applicable law.

8. Wahrung von Betroffenenrechten

(1) Der Auftraggeber ist für die Wahrung der Betroffenenrechte allein verantwortlich. Der Auftragnehmer ist im Rahmen seiner Möglichkeiten verpflichtet, den Auftraggeber bei seiner Pflicht zur Bearbeitung von Anträgen von betroffenen Personen nach Art. 12 bis 22 DSGVO zu unterstützen. Der Auftragnehmer wird den

8. Preserving the rights of data subjects

(1) The Client bears sole responsibility for preserving the rights of data subjects. The Contractor is obliged to the extent possible 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

Auftraggeber informieren, wenn Betroffene ihre Betroffenenrechte an den Auftragnehmer richten.
(2) Benötigt der Auftraggeber die Mitwirkung des Auftragnehmers zur Wahrung der Betroffenenrechte (insbesondere auf Auskunft, Berichtigung, Sperrung oder Löschung), wird der Auftragnehmer den Auftraggeber auf Anforderung (mind. in Textform) im Rahmen seiner Möglichkeiten unterstützen.

(3) Der Auftragnehmer wird den Auftraggeber dabei unterstützen, Informationen so schnell wie möglich bereitzustellen. Voraussetzung hierfür ist, dass der Auftraggeber den Auftragnehmer hierzu auffordert (mind. in Textform).
(4) Für Unterstützungsmaßnahmen, die im Zusammenhang mit der Wahrnehmung der Betroffenenrechte ergriffen werden, kann der Auftragnehmer vom Auftraggeber eine Vergütung verlangen.

9. Technische und organisatorische Maßnahmen zur Datensicherheit

(1) Der Auftragnehmer verpflichtet sich gegenüber dem Auftraggeber zur Einhaltung der technischen und organisatorischen Maßnahmen, die zur Erfüllung der einschlägigen Datenschutzvorschriften erforderlich sind. Dazu gehören insbesondere die Vorgaben aus Art. 32 DSGVO.
(2) Der aktuelle Stand der getroffenen technischen und organisatorischen Maßnahmen ist in Anlage 2 dokumentiert und wird dem Auftraggeber zur Prüfung zur Verfügung gestellt.
(3) Die Vertragsparteien sind sich darüber einig, dass zur Anpassung an technische und rechtliche Gegebenheiten Änderungen der technischen und organisatorischen Maßnahmen erforderlich werden können. Der Auftragnehmer ist daher bei entsprechender Änderung berechtigt, die technischen und organisatorischen Maßnahmen anzupassen. Wesentliche Änderungen werden dokumentiert.
(4) Der Auftraggeber hat das Recht, den Auftragnehmer aufzufordern, angemessene zusätzliche Sicherheitsmaßnahmen zu ergreifen, die zum Schutz der Interessen seiner Kunden und der personenbezogenen Daten erforderlich sind. Der Auftragnehmer entscheidet nach alleinigem Ermessen, ob die zusätzlichen Sicherheitsmaßnahmen wirtschaftlich zumutbar sind.
(5) Der Auftraggeber ist berechtigt, jederzeit eine aktualisierte Fassung der technischen und organisatorischen Maßnahmen anzufordern.

10. Beendigung des Vertrags

(1) Nach Beendigung des Dienstleistungsvertrags hat der Auftragnehmer dem Auftraggeber alle ihm überlassenen Unterlagen (einschließlich etwaig vorhandener Kopien) mit personenbezogenen Daten zurückzugeben oder auf Wunsch des Auftraggebers zu löschen, sofern nicht nach Unionsrecht oder nach dem Recht der Bundesrepublik Deutschland eine Pflicht zur Aufbewahrung der Daten besteht.
(2) Der Auftraggeber kann sein Wahlrecht (Rückgabe bzw. Löschung personenbezogener Daten) bis spätestens zum Zeitpunkt der Beendigung des Dienstleistungsvertrags ausüben (mind. in Textform). Macht der Auftraggeber von seinem Wahlrecht keinen Gebrauch, wird der Auftragnehmer alle personenbezogenen Daten des Auftraggebers 14 Tage nach Beendigung des Dienstleistungsvertrags löschen.
(3) Die Löschung ist in geeigneter Weise zu dokumentieren und dem Auftraggeber auf Verlangen zu bestätigen (mind. in Textform).

11. Haftung

(1) Die zwischen den Vertragsparteien im Dienstleistungsvertrag vereinbarten Haftungsklauseln gelten auch für den vorliegenden Auftragsverarbeitungsvertrag.
(2) Soweit Dritte Ansprüche gegen den Auftragnehmer geltend machen, die darauf zurückzuführen sind, dass der Auftraggeber diesen Auftragsverarbeitungsvertrag oder seine Pflichten als Verantwortlicher schuldhaft verletzt hat, stellt der Auftraggeber den Auftragnehmer von diesen Ansprüchen frei.

12. Schlussbestimmungen

(1) Sollten einzelne Teile dieses Auftragsverarbeitungsvertrags unwirksam sein, bleibt die Wirksamkeit der übrigen Bestimmungen des Auftragsverarbeitungsvertrags hiervon unberührt.
(2) Jede Änderung dieses Auftragsverarbeitungsvertrags bedarf der Schriftform, die auch in elektronischer Form erfolgen kann.
(3) Für sämtliche Rechtsbeziehungen zwischen den Vertragsparteien gilt das für die Rechtsbeziehungen inländischer

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 to the extent possible the Client if requested to do so (at least in text form).
(3) The Contractor will assist the Client in providing information as soon as reasonably possible. 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.

9. 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 obligations in Art. 32 GDPR.

(2) The latest status of the technical and organizational measures that have been implemented is documented in Annex 2 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.

(4) The Client has the right to request the Contractor to take reasonable additional security measures, necessary to protect the interest of its customers and the Personal Data. The Contractor will decide in its sole discretion if the additional security measures are reasonably commercially possible.

(5) The Client is entitled to request an updated version of the technical and organizational measures at any time.

10. Termination

(1) After the termination of the 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 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 Service Agreement.

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

11. Liability

(1) The liability clauses as agreed between the Parties in the Service Agreement are also applicable for this Data Processing Agreement.
(2) Insofar as third parties assert claims against the Contractor which have their cause in a culpable breach by the Client of this Data Processing Agreement or of one of its obligations as a controller, the Client shall indemnify the Contractor against such claims.

12. Final provisions

(1) If individual parts of this Data Processing Agreement should be ineffective, this will not affect the validity of the remaining provisions of the Data Processing Agreement.
(2) Any amendment to this Data Processing Agreement must be made in written form, which may also be in an electronic format.
(3) For all legal relationships between the Parties, the laws of the Federal Republic of Germany that are authoritative for legal

Parteien maßgebliche Recht der Bundesrepublik Deutschland. Die Bestimmungen des UN-Kaufrechts finden keine Anwendung.

(4) Gerichtsstand ist Marburg/Lahn. Ein etwaiger ausschließlicher Gerichtsstand bleibt hiervon unberührt.

relationships between domestic parties apply. The provisions of the UN Convention on Contracts for the International Sale of Goods shall not apply.

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

_____,_____

Ort/*Place* Datum/*Date*

Kitzingen,_____

Ort/*Place* Datum/*Date*

– Auftraggeber/*Client* –

– weclapp GmbH –

Anlage 1: Umfang, Art und Zweck der vorgesehenen Datenverarbeitung; Arten von Daten und Kategorien der betroffenen Personen

Umfang der Datenverarbeitung: Die vom Auftraggeber oder unter seiner Verantwortung eingegebenen Daten werden gespeichert und verarbeitet, wenn und soweit der Auftraggeber dies wünscht.

Art und Zweck der Erhebung, Verarbeitung und Nutzung personenbezogener Daten	Art und Zweck der Datenverarbeitung richten sich nach dem Dienstleistungsvertrag und den Weisungen des Auftraggebers. Der Zweck besteht insbesondere darin, für Auftraggeber Dienstleistungen zu erbringen.
Art der Daten	Alle vom Auftraggeber eingegebenen personenbezogenen Daten, zu denen auch E-Mail-Adressen, Namen und Adressen von Personen und andere Arten von Daten gehören können.
Kategorien von betroffenen Personen	Regelmäßig Mitarbeiter des Auftraggebers, Ansprechpartner des Auftraggebers in externen Unternehmen wie seine Kunden oder Interessenten und deren jeweilige Mitarbeiter.

Annex 1: the extent, nature and purpose of the intended processing of data; the type of data and categories of data subjects

The extent of the processing data: data entered by or under the responsibility of the Client is stored and processed if and to the extent requested by the Client.

Nature and purpose of the collection, processing or use of data	The nature and purpose of data processing are based on the Service Agreement and on the Client's instructions. The purpose is in particular to provide clients with services.
The type of data	All personal data entered by the Client, which may include e-mail addresses, names and addresses of persons, and other types of data.
Categories of data subjects	Regularly employees of the Client, contacts of the Client from external companies such as its customers or prospective customers and their respective employees.

Anlage 2: Technische und organisatorische Maßnahmen zur Datensicherheit gemäß Art. 32 Abs. 1 DSGVO

1. Zutrittskontrolle zu Räumlichkeiten und Einrichtungen
Der unbefugte Zugang (im physischen Sinne) muss verhindert werden.
Technische und organisatorische Maßnahmen zur Kontrolle des Zugangs zu Räumen und Einrichtungen, insbesondere zur Überprüfung der Berechtigung:

- Zutrittskontrollsystem
- Ausweisleser, Chipkarte
- Türverriegelung
- Sicherheitspersonal
- Überwachungseinrichtungen
- Alarmanlage, Videoüberwachung

2. Zugangskontrolle zu den Systemen
Der unberechtigte Zugriff auf IT-Systeme muss verhindert werden.
Technische (ID-/Passwortsicherheit) und organisatorische (Benutzerstammdaten) Maßnahmen zur Benutzeridentifikation und -authentifizierung:

- Passwortverfahren (inkl. Sonderzeichen, Mindestlänge, Passwortwechsel)
- Automatische Sperrung (z.B. Passwort oder Timeout)
- Anlegen eines Stammsatzes pro Benutzer
- Zwei-Faktor-Authentifizierung

3. Zugriffskontrolle auf Daten
Aktivitäten in IT-Systemen, die nicht durch die zugewiesenen Zugriffsrechte abgedeckt sind, müssen verhindert werden.
Anforderungsgerechte Definition des Berechtigungsschemas und der Zugriffsrechte sowie Überwachung und Protokollierung der Zugriffe:

- Differenzierte Zugriffsrechte (Profile, Rollen, Transaktionen und Objekte)
- Berichte
- Protokollierter Zugriff
- Protokollierte Änderung
- Protokollierte Löschung

Annex 2: Technical and organizational measures of Contractor for data security according to Art. 32 (1) GDPR

1. Access control to premises and facilities
Unauthorized access (in the physical sense) must be prevented.

Technical and organizational measures to control access to premises and facilities, particularly to check authorization:

- Access control system
- ID reader, chip card
- Door locking
- Security staff
- Surveillance facilities
- Alarm system, video monitoring

2. Access control to systems
Unauthorized access to IT systems must be prevented.
Technical (ID/password security) and organizational (user master data) measures for user identification and authentication:

- Password procedures (incl. special characters, minimum length, change of password)
- Automatic blocking (e.g. password or timeout)
- Creation of one master record (one-identity) per user
- Two factor authentication

3. Access control to data
Activities in IT systems not covered by the allocated access rights must be prevented.
Requirements-driven definition of the authorization scheme and access rights, and monitoring and logging of accesses:

- Differentiated access rights (profiles, roles, transactions and objects)
- Reports
- Logged Access
- Logged Change
- Logged Deletion

4. Weitergabekontrolle
Die Weitergabe personenbezogener Daten muss kontrolliert werden: elektronische Übermittlung, Datentransport, Übermittlungskontrolle, etc.
Maßnahmen zum Transport, zur Übermittlung und Kommunikation oder zur Speicherung von Daten auf Datenträgern (manuell oder elektronisch) und zur späteren Kontrolle:

- Verschlüsselung/VPN = Virtual Private Network
- Protokollierung
- Transportsicherung

4. Disclosure control
Disclosure of personal data must be controlled: electronic transfer, data transport, transmission control, etc.
Measures to transport, transmit and communicate or store data on data media (manual or electronic) and for subsequent checking:

- Encryption/VPN = Virtual Private Network
- Logging
- Transport security

5. Eingabekontrolle
Es muss eine vollständige Dokumentation der Datenverwaltung und -pflege geführt werden.
Maßnahmen zur nachträglichen Kontrolle, ob und von wem Daten eingegeben, geändert oder entfernt (gelöscht) wurden:

- Protokollierungs- und Berichtssysteme
- Protokollierung der Eingabe, Veränderung und Löschung von Daten
- Änderung und Löschung von Daten durch Benutzernamen

5. Input control
Full documentation of data management and maintenance must be maintained.
Measures for subsequent checking whether data have been entered, changed or removed (deleted), and by whom:

- Logging and reporting systems
- Logging the entry, change and deletion of data
- Change and deletion of data using User names

6. Auftragskontrolle
Die Auftragsdatenverarbeitung muss weisungsgemäß durchgeführt werden.
Maßnahmen (technisch/organisatorisch) zur Trennung der Verantwortlichkeiten zwischen dem für die Verarbeitung Verantwortlichen und dem Auftragsverarbeiter:

- Eindeutige Formulierung des Vertrages
- Formalisierte Beauftragung
- Kriterien für die Auswahl des Auftragnehmers
- Überwachung der Vertragserfüllung

6. Task control
Commissioned data processing must be carried out according to instructions.
Measures (technical/organizational) to segregate the responsibilities between the Controller and the Processor:

- Unambiguous wording of the contract
- Formal commissioning
- Criteria for selecting the Agent
- Monitoring of contract performance

7. Verfügbarkeitskontrolle
Die Daten müssen gegen zufällige Zerstörung oder Verlust geschützt werden.
Maßnahmen zur Gewährleistung der Datensicherheit (physisch/logisch):

- Backup-Verfahren
- Spiegelung von Festplatten, z.B. RAID-Technologie
- Unterbrechungsfreie Stromversorgung (USV)
- Remote-Storage
- Antiviren-/Firewall-Systeme
- Plan zur Wiederherstellung im Katastrophenfall

7. Availability control
The data must be protected against accidental destruction or loss.
Measures to assure data security (physical/logical):

- Backup procedures
- Mirroring of hard disks, e.g. RAID technology
- Uninterruptible power supply (UPS)
- Remote storage
- Anti-virus/firewall systems
- Disaster recovery plan

8. Trennungskontrolle
Daten, die für unterschiedliche Zwecke erhoben werden, müssen auch getrennt verarbeitet werden.
Maßnahmen, die eine getrennte Verarbeitung (Speicherung, Änderung, Löschung, Übermittlung) von Daten für unterschiedliche Zwecke gewährleisten:

- Mandantentrennung
- Trennung von Funktionen (Produktivsystem/Testsystem)

8. Segregation control
Data collected for different purposes must also be processed separately.
Measures to provide for separate processing (storage, amendment, deletion, transmission) of data for different purposes:

- Mandates separation
- Segregation of functions (production/testing)

9. Organisationskontrolle
Es müssen auf organisatorischer Ebene Verfahren zur Gewährleistung der Sicherheit der Datenverarbeitung bestehen.
Maßnahmen zur Organisationskontrolle der Sicherheit der Datenverarbeitung:

- Datenschutz-Management
- Bestellung eines Datenschutzbeauftragten
- Datenschutzteam
- Verpflichtung der Mitarbeiter zur Wahrung der Vertraulichkeit und zur Beachtung der datenschutzrechtlichen Anforderungen nach der DSGVO sowie zur Verschwiegenheit nach § 203 Abs. 4 StGB
- Schulungen zum Datenschutz

9. Organizational control
Procedures must be in place at the organizational level to ensure the security of data processing.
Measures to organizational control of the security of data processing:

- Data protection management
- Appointment of a data protection officer
- Data protection team
- Obligation of employees to maintain confidentiality and to comply with data protection requirements in accordance with the GDPR and to maintain confidentiality in accordance with Section 203 (4) of the German Criminal Code (StGB)
- Training on data protection
- Policy for employees on dealing with data breaches

- Richtlinie für Mitarbeiter zum Umgang mit Datenpannen
- Datenschutzrichtlinie für Mitarbeiter
- Verpflichtung der Mitarbeiter zur Verschwiegenheit

- Data protection policy for employees
- Obligation of employees to confidentiality