Data Processing Addendum
for services of Cortado Mobile Solutions GmbH

in accordance with Article 28 (3) of the EU General Data Protection Regulation (GDPR)

Preamble

To better protect individuals' personal data, we are providing this Data Processing Addendum (DPA) to govern our and your handling of these data (hereinafter referred to as "Addendum"). This Addendum supplements the General Terms and Conditions of Cortado Mobile Solutions (hereinafter referred to as "Agreement") – with this Addendum being an annex thereto – and requires no further action on your part.

The Addendum details the obligations of the parties to the Agreement with regard to data protection. The contracting parties are you as the **Company (Controller)** and **Cortado Mobile Solutions GmbH, Alt-Moabit 91a, 10559 Berlin, Germany** (hereinafter referred to as "CMS") as the **Supplier (Processor)**. The Addendum applies to all activities that are related to the provisions of the Agreement and in which employees of the Supplier or of a subprocessor process personal data (hereinafter referred to as "Data") of the Customer.

§ 1 Scope, duration and specification of data processing

The scope and duration and the detailed stipulations on the type and purpose of processing shall be governed by the Agreement. Specifically, processing shall include, but not be limited to, the following Data:

Type of Data	Type and purpose (subject matter) of processing	Categories of Data subjects affected
• user accounts in the client's Active Directory • general information required at meetings or on-site assignments or information that is learned by chance • if necessary, form data on the websites of the contractor • if applicable, data processed by the CMS software, such as log data	• contact data of contact persons will be stored in the contractor's customer database and will be used exclusively for the purpose of fulfilling the business purposes between Company and Supplier. In particular this concerns: name, first name, position, if necessary branch office of the client, company telephone number, company e-mail address • support, sales, billing and consulting services	Company's employees, customers or business partners

Except where this Addendum stipulates obligations beyond the term of the Agreement, the term of the Agreement shall be the term of this Addendum.

§ 2 Scope of application and responsibilities

(1) Supplier shall process Data on behalf of and at the instruction of Company. This includes activities that are specified in the Agreement and in service descriptions such as Service Level Agreements. Within the scope of this Addendum, Company shall be solely responsible for compliance with the applicable statutory requirements on data protection, including, but not limited to, the lawfulness of disclosing Data to Supplier and the lawfulness of having Data processed on behalf of Company. Company shall be the »Controller« in accordance with Article 4 (7) of the GDPR.

(2) Company's individual instructions on processing shall, initially, be as detailed in this Addendum. Company shall, subsequently, be entitled to, in writing or in a machine-readable format (in text form), modifying, amending or replacing such individual instructions by issuing such instructions to the point of contact designated by Supplier. Instructions not foreseen in or covered by the Addendum shall be treated as requests for changes to the statement of work. Company shall, without undue delay, confirm in writing or in text form any instruction issued orally.

(3) Supplier processes Company's Data exclusively for the purpose described in § 1. The described purpose will be passed on to all Subprocessors as defined in § 7. Exception: In the event of an error, it may become necessary to evaluate log data of computers for error analysis.

§ 3 Supplier's obligations

(1) Except where expressly permitted by Article 28 (3)(a) GDPR, Supplier shall process data subjects' Data only within the scope of the statement of work and the instructions issued by Company – including with regard to transfers of personal data to a third country or an international organisation. In such an exceptional case, Supplier shall inform Company of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest. Where Supplier believes that an instruction would be in breach of applicable law, Supplier shall notify Company of such belief without undue delay. Supplier shall be entitled to suspending performance on such instruction until Company confirms or modifies such instruction.

(2) Supplier shall, within Supplier's scope of responsibility, organize Supplier's internal organization so it satisfies the specific requirements of data protection. Supplier shall implement technical and organizational measures to ensure the adequate protection of Company's Data, which measures shall fulfil the requirements of the GDPR and specifically its Article 32. Supplier shall implement technical and organizational measures and safeguards that ensure ongoing confidentiality, integrity, availability and resilience of processing systems and services. Company is familiar with these technical and organizational measures (see Exhibit 1).

Supplier reserves the right to modify the measures and safeguards implemented, provided, however, that the level of security shall not be less protective than initially agreed upon.

(3) Supplier shall support Company and where possible for Supplier, in fulfilling data subjects' requests and claims, as detailed in chapter III of the GDPR and in fulfilling the obligations enumerated in Articles 33 to 36 of the GDPR.

(4) Supplier warrants that all employees involved in processing of Company's Data and other such persons as may be involved in processing within Supplier's scope of responsibility shall be prohibited from processing Data outside the scope of the instructions. Furthermore, Supplier warrants that any person entitled to process Data on behalf of Controller has undertaken a commitment to secrecy or is subject to an appropriate statutory obligation to secrecy. All such secrecy obligations shall survive the termination or expiration of such processing.

(5) Supplier shall notify Company, without undue delay, if Supplier becomes aware of breaches of the protection of personal data within Supplier's scope of responsibility.

Supplier shall implement the measures necessary for securing Data and for mitigating potential negative consequences for the data subject; the Supplier shall coordinate such efforts with Company without undue delay.

(6) Supplier shall notify to Company the contact person for any issues related to data protection arising out of or in connection with the Agreement. At the time of contract conclusion, this is the Data Protection Officer of Cortado Mobile Solutions GmbH:

Mr *Herbert Hemke* (dataprotection@cortado.com)

(7) Supplier warrants that Supplier fulfills its obligations under Article 32 (1)(d) GDPR to implement a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures and to dynamically adapt it in this context for ensuring the security of the processing.

(8) Supplier shall correct or erase Data if so instructed by Company and where covered by the scope of the instructions permissible. Where an erasure, consistent with data protection requirements, or a corresponding restriction of processing is impossible, Supplier shall, based on Company's instructions, and unless agreed upon differently in the Agreement, destroy, in compliance with data protection requirements, all carrier media and other material or return the same to Company.

In specific cases, to be determined by Company, storage or handover shall take place, unless already agreed in the Agreement.

(9) Supplier shall, upon conclusion of the contractual work or request by Company – but latest upon termination of contract processing – return all Data, carrier media and other materials to Company or delete the same unless Union or Member State law requires storage of the personal data. The same applies to testing and discarded material. The log of deletion/destruction shall be submitted upon Company's request.

Supplier must retain documentations that prove the orderly and proper processing of data according to the respective retention periods beyond the conclusion of the contractual work. Supplier is allowed to hand over such documentations to Company for discharge upon conclusion of the contractual work.

(10) Where a data subject asserts any claims against Company in accordance with Article 82 of the GDPR, Supplier shall support Company in defending against such claims, where possible.

§ 4 Company's obligations

(1) Company shall notify Supplier, without undue delay, and comprehensively, of any defect or irregularity with regard to provisions on data protection detected by Company in the results of Supplier's work.

(2) Company shall notify to Supplier the contact person for any issues related to data protection arising out of or in connection with the Agreement.

§ 5 Enquiries by data subjects

Where a data subject asserts claims for rectification, erasure or access against Supplier, and where Supplier is able to correlate the data subject to Company, based on the information provided by the data subject, Supplier shall refer such data subject to Company. Supplier shall forward the data subject's claim to Company without undue delay. In view of the nature of the processing, the Supplier shall support Company as far as possible with appropriate technical and organizational measures in complying with its obligation to respond to requests to exercise the rights of the data subject referred to in Chapter III GDPR. Supplier shall not be liable in cases where Company fails to respond to the data subject's request in total, correctly, or in a timely manner.

§ 6 Options for documentation

(1) Supplier shall document and prove to Company Supplier's compliance with the obligations agreed upon in this Addendum by appropriate measures.

(2) Where, in individual cases, audits and inspections by Company or an auditor appointed by Company are necessary, such audits and inspections will be conducted during regular business hours, and without interfering with Supplier's operations, upon prior notice, and observing an appropriate notice period. Supplier may also determine that such audits and inspections are subject to prior notice, the observation of an appropriate notice period, and the execution of a confidentiality undertaking protecting the Data of other customers and the confidentiality of the technical and organisational measures and safeguards implemented. Supplier shall be entitled to rejecting auditors which are competitors of Supplier.

Supplier shall be entitled to requesting a remuneration for Supplier's support in conducting inspections. This corresponds to the remuneration for consulting services by the Supplier. Supplier's time and effort for such inspections shall be limited to one day per calendar year, unless agreed upon otherwise.

(3) Where a data protection supervisory authority or another supervisory authority with statutory competence for Company conducts an inspection in connection with the specific commissioned processing of Supplier for Company described under § 1, para. 2 above shall apply mutatis mutandis – with the exception of the regulation on remuneration. The execution of a confidentiality undertaking shall not be required if such supervisory authority is subject to professional or statutory confidentiality obligations whose breach is sanctionable under the applicable criminal code.

§ 7 Subprocessors (further processors on behalf of Company)

(1) Company hereby consents in principle to Supplier's use of subprocessors or subcontractors. Supplier shall, prior to the use or replacement of subprocessors, inform Company thereof. Company shall be entitled to contradict any change notified by Supplier within four weeks' time and only for materially important reasons. Where Company fails to contradict such change within such period of time, Company shall be deemed to have consented to such change. If a subcontractor is not accepted by Company, and failing an amicable resolution of this matter by the parties, Company shall be entitled to terminating the Agreement.

(2) Where Supplier commissions subprocessors, Supplier shall be responsible for ensuring that Supplier's obligations on data protection resulting from this Addendum as well as sufficient guarantees for the technical and organizational measures are valid and binding upon subprocessor.

(3) Supplier will conduct the performance agreed upon, or the parts of the performance identified below, using the subprocessors enumerated below:

Name and address of the subprocessr	Description of the affected parts of performance	Legal basis for data export
Cortado Holding AG, Alt-Moabit 91 a/b, 10559 Berlin, Germany (parent company)	business activities of the group such as: • administration of websites, social media, web and cloud services such as Amazon Web Services, Microsoft Azure, Teamplace and Cortado MDM • services such as marketing, sales, customer support, recruiting, team management, payment processing, bookkeeping and accounting • representation of the Supplier at authorities and companies in legal and tax matters, in audits, in questions of personnel management, pension provision and profit sharing • security organization such as IT administration, IT security, alarm system and security	
Freshworks Inc., 1250 Bayhill Drive, Suite 315, San Bruno, California 94066, USA	Supplier's use of the following cloud platforms: • Freshdesk as helpdesk for support and consulting • Fresworks CRM (formerly Freshsales) as customer database • Freshchat as a chat platform	SCC-2021 including TIA

SCC-2021 = Standard Contractual Clauses of the European Commission dated June 4, 2021, Decision (EU) 2021/914
TIA = Transfer Impact Assessment according to Clauses 14 + 15 of the SCC-2021

§ 8 Obligations to inform, mandatory written form, choice of law

(1) Where the Data becomes subject to search and seizure, an attachment order, confiscation during bankruptcy or insolvency proceedings, or similar events or measures by third parties while in Supplier's control, Supplier shall notify Company of such action without undue delay. Supplier shall, without undue delay, notify to all pertinent parties in such action, that any data affected thereby is in Company's sole property and area of responsibility, that data is at Company's sole disposition, and that Company is the Controller in the sense of the EU General Data Protection Regulation (GDPR).

(2) No modification of this Addendum and/or any of its components – including, but not limited to, Supplier's representations and warranties, if any – shall be valid and binding unless made in writing or

in a machine-readable format (in text form), and furthermore only if such modification expressly states that such modification applies to the regulations of this Addendum; the foregoing shall also apply to any waiver or modification of this mandatory written form. Company shall be entitled to contradict any change notified by Supplier within four weeks. Where Company fails to contradict such change within such period of time, Company shall be deemed to have consented to such change.

(3) In case of any conflict, the data protection regulations of this Addendum shall take precedence over the regulations of the Agreement. Where individual regulations of this Addendum are invalid or unenforceable, the validity and enforceability of the other regulations of this Addendum shall not be affected.

(4) This Addendum is subject to the laws of Germany.

§ 9 Liability and damages

Company and Supplier shall be liable to data subject in accordance with Article 82 of the GDPR.

Exhibit 1: Technical and organisational measures of CMS in accordance with Article 32 of the GDPR

General

- regular training for all CMS employees, especially on IT security and data protection
- data protection information in the internal CMS wiki information system
- information and measures to sensitize CMS employees to attacks on the IT infrastructure
- annual security and data protection audits, checking, among other things, the content and effectiveness of the following documents:
  - Data Privacy Statement of the Cortado Mobile Solutions GmbH
  - Data Privacy Statements of the CMS apps

and the following documents of the parent company Cortado Holding AG:

- Information Security Policy
- Logical Access Control Policy + Password Policy
- Audit and Assessment Policy
- Data Protection Training
- Mobile Device Policy
- Contract Policy + Non-Disclosure Policy
- Workforce Policy + Workspace and Premises Policy
- Business Continuity & Incident Response Plan
- Information Security Management Framework (ISMF)

IT environment

CMS IT infrastructure:

- access protocols for server rooms
- antivirus software on all PCs
- information security program and intrusion prevention system (IPS)
- incident response concept
- remote access to servers via VPN and remote desktop connections (RDP)
- web platforms on own servers, e. g.:, Confluence (knowledge base), Cortado Enterprise Portal (external self-service portal for partners and customers), -project management, e-mails
- use of cloud services, e. g.: payment services, online shops, customer databases, teamwork and online storage (Teamplace), mobile device management (Cortado MDM), Microsoft Office 365, chat, meeting and webinar platforms

Entry control

Measures to prevent unauthorized persons from gaining access to data processing systems with which personal data are processed or used

CMS IT infrastructure:

- separate server rooms for company data and alarm system
- electronic locking system with token and PIN
- as well as security locks with key control (manual locking system)
- locked doors in absentia
- server rooms without windows
- access authorization rule
- access rules for non-admins and non-employees

- security personnel for the times when the company is not occupied:
  Sicherheit Nord GmbH & Co. KG, Berlin branch office, Ringstraße 44/45, 12105 Berlin, Germany, phone: +49-30-70 79 20-0, www.sicherheit-nord.de
- employee and visitor badges, identity check at the reception

Access control

Measures to prevent data processing systems from being used without authorization

CMS IT infrastructure:

- identification and authentication
- limitation of failed attempts
- time-controlled dark switching of screens with password protection
- assignment of user permissions
- password assignment
- authentication with user name and password
- use of anti-virus software
- use of a hardware firewall
- use of VPN technology
- encryption of print data
- pull printing (ThinPrint Personal Printing)
- mobile device management: Cortado Server (e. g. for external data deletion, device locking and localization)

Permission control

Measures to ensure that persons entitled to use a data processing system have access only to the data to which they have a right of access, and that personal data cannot be read, copied, modified or removed without authorization in the course of processing or use and after storage

CMS IT infrastructure:

- authorization concept
- identification and authentication
- storage of data carriers in data safes
- off-site storage of backups
- number of administrators reduced to the “bare” essentials
- special admins are usually defined for each application
- use of shredders
- administration of permissions by system administrator
- password policy including password length, password change
- secure storage of data carriers

Transmission control

Measures to ensure that personal data cannot be read, copied, modified or removed without authorization during electronic transmission or transport, and that it is possible to check and establish to which bodies the transfer of personal data by means of data transmission facilities is envisaged

CMS IT infrastructure:

- off-site storage of backups exclusively by IT admins
- installation of leased lines or VPN tunnels
- e-mail encryption, if required, e. g. for mail traffic with auditors and tax advisors (default: S/MIME)

- sharing data via a secure cloud platform (Teamplace)
- transmission of data in anonymized or pseudonymized form

Job control

Measures to ensure that, in the case of commissioned processing of personal data, the data are processed strictly in accordance with the instructions of the principal or “Controller” as defined in article 4 (7) and article 28 (10) GDPR.

See the relevant data processing agreement or addendum in accordance with Art. 28 para. 3 GDPR.

Availability control

Measures to ensure that personal data are protected from accidental destruction or loss

CMS IT infrastructure:

- alarm message in the event of unauthorized access to company premises
- uninterruptible power supply (UPS)
- fire and smoke detection systems
- fire extinguishers in the immediate vicinity of the server rooms
- devices for monitoring temperature and humidity in server rooms
- air conditioning in server rooms
- server rooms are not under sanitary facilities
- protective socket strips in server rooms
- backup & recovery concept
- performing data backups
- off-site storage of backups
- data recovery testing

Separation requirement

Measures to ensure that data collected for different purposes are processed separately

CMS IT infrastructure:

- physically separate storage on separate systems or data carriers
- authorization concept
- definition of database permissions
- logical client separation (software-side)
- separation of production and test system
- separate databases (per application)