Data Privacy Statement for the Teamplace app (iOS)

The Teamplace app is a client component of the cloud service Teamplace (hereinafter referred to as "Teamplace"), which can also be accessed via the Internet browser via the web address https://web.teamplace.net/. Teamplace is offered by Cortado Mobile Solutions GmbH (see below) (hereinafter referred to as "CMS"). The Teamplace app complies with the data protection requirements of the EU General Data Protection Regulation (GDPR), the German Federal Data Protection Act (German: Bundesdatenschutzgesetz, BDSG) as well as other German and European laws relevant to data protection.

Permissions of the Teamplace app

If you use the Teamplace app, at the time of the first access you will be asked if you want to allow the app access to:

1. **Get Accounts, Authenticate Account and Manage Accounts**
   (your account data and your profile on the iOS device)
2. **Read Contacts**
   (your address book on the iOS device)
3. **Microphone and Camera Usage**
   (text files, pictures, videos, audio files stored on the iOS device or on the device's external storage)
4. **Photo Library**
   (device identification number, telephone number of the SIM card, call number of the other party when calling)

The Teamplace app uses these permissions for the following purposes:

1. **Get Accounts, Authenticate Account and Manage Accounts**
   If you log in or register with Google or Facebook, these account data can be used to authenticate your user account at the Teamplace service.

2. **Read Contacts**
   The contacts of the device's address book can be used to invite participants into a *Teamplace*-named team project.

3. **Microphone and Camera Usage**
   You can use the Teamplace app to take photos or movies and use them directly in a *Teamplace*-named team project.

4. **Photo Library**
   Access to the user's file space is used to upload local data (such as photos or videos) and to download data from Teamplace to the device.

In general, the Teamplace app only accesses your data if you decide this yourself – for example, it will access your address book when you invite someone to a *Teamplace*-named team project, or to the file system of your iOS device, if you want to upload a file to a *Teamplace*. If necessary, you can **revoke** the permission for access from the app in *Settings→ Teamplace* as well as in *Settings→ Privacy*.

Data used by the Teamplace app

Data you entered (user data)

When you **register** with the app as a user at Teamplace to purchase, download, or book services through Teamplace's web portal, you must provide **personal information**, namely an e-mail address, a display name, and a password for the user's Teamplace account. If you purchase Teamplace services that are subject to a fee, you must also provide payment information. In general, any and all information that allows us to individually

identify people are considered personal information. We always receive and transmit any and all personal data by way of encryption, and passwords must be sufficiently complex. Instead of storing your access data locally on your iOS device, we place an authentication token in a protected app area. In addition to tokens, only a user ID, the e-mail address, and the display name are stored locally on the iOS device. If you purchased Teamplace services that are subject to a fee, the payment is handled by the German company PayOne GmbH (Fraunhoferstraße 2–4, 24118 Kiel, Germany, the Sparkassen Financial Group is the majority shareholder) or the Stripe Inc. (185 Berry Street, Suite 550, San Francisco, CA 94107, USA). Both companies – PayOne GmbH and Stripe Inc. – have entered into a Data Processing Agreement in accordance with Article 28 of GDPR. We do not forward any data to any other third company.

Optionally you can use existing credentials from Facebook (Facebook, Inc., 1601 Willow Road, Menlo Park, California 94025, USA) or Google (Google LLC, 1600 Amphitheatre Pkwy, Mountain View, California 94043, USA) accounts to register with Teamplace or log-in to your Teamplace account. In this case Teamplace retrieves the following information from Facebook or Google: public profile (including name and avatar), e-mail address (for setting up the Teamplace account) and user ID (for matching the Teamplace account with the Facebook or Google user). Facebook and/or Google will log your use of the Teamplace account. Beyond that, we do not send any other data to Facebook or Google here.

Upon registration with Teamplace you must choose a **display name**, this is the name other users of Teamplace will see. It is NOT required that you provide your real name, it is explicitly permitted to choose names like “Pippi Longstocking” or “Ronia the Robber’s Daughter” as a display name. Your e-mail address will not be displayed to other members of a *Teamplace*-named team project. The freely selectable display name allows a data protection-compliant (pseudonymized) assignment of the Teamplace account. However, the business feature Organization allows members of such Organizations to see each other’s e-mail addresses.

Deletion of user data

If you register with the app at Teamplace but do not complete the registration - that is because you did not click the Activate button in the activation e-mail - then your data will be deleted automatically on the Teamplace server after 31 days (except with the business features Organization where your account can be activated automatically within a company). The deletion deadline also applies to your data when you cancel your Teamplace account, with the exception of such data you have uploaded to other *Teamplace*-named team projects (for example, your comments will remain existent).

Data collected by Teamplace (usage data)

On your first visit to a **Teamplace website**, we send a **cookie**, e.g. a small electronic file consisting of a certain character string allowing us to identify your browser. Other cookies are used to cache logon data and usage preferences. All Teamplace cookies are recognizable at the string **teamplace.net** in the name of the cookie.

You may adjust your browser to reject cookies or to ask for permission each time a cookie is sent. A rejection of only third-party cookies prevents login with credentials from Facebook or Google. A rejection of *all* cookies (or of cookies Teamplace sends) would however prevent the registration at Teamplace itself.

In addition, Teamplace evaluates the usage behavior of all app users statistically. In this case, however, **no personal data** is collected or processed, but only anonymized and pseudonymized information – namely the number of users performing an operation (event tracking) such as installation and first use of the app, registration, purchase of a paid service, clicking on an advertising banner or possibly a crash report of the app. These usage data are sent to the Teamplace servers and, if necessary, to external service providers such as Fabric Answers (for event tracking), Fabric Crashlytics (for crash reports) and Firebase Cloud Messaging (for transmitting push messages; all from Google) and Appfabric (for service optimization; Microsoft Corporation, 1 Microsoft Way, Redmond, Washington, 98052, USA).

Teamplace logged data (log files)

The Teamplace app can log your IP address and your e-mail address for each event. This serves to prevent misuse of our e-mail service, the error diagnostics as well as the purposes of evidence. You can enable or disable logging with *Settings→ Teamplace→ Write to log file*. All log data are automatically deleted after 30 days.

Your approval for the collection of personal data/revocation

If you register for a specific service on the Teamplace websites, we ask for your personal data (see above). If such data shall be used for a different purpose than originally indicated, we request your consent for us doing so by checking an applicable box. However, you may refuse to give your consent. Without your express prior consent, CMS will not use your personal information for other purposes than indicated and in connection with the respective services or products.

You are at all times entitled to refuse to provide personal information or to revoke provided personal data. Please be aware, though, that in such case CMS might not be able to offer you all available services for Teamplace. If you revoke personal data which is still required for processing valid contractual relations between you and CMS, we will delete any personal data promptly after termination of the contractual relations.

Transfer of personal data to third parties

CMS will transfer your personal data (user data) only upon your express prior consent to any third party. Without your express prior consent, CMS will only transfer or disclose your personal data upon presentation of a search warrant, judicial order, judicial decree or another form of lawful cases regulated by law.

Data security

CMS uses adequate security measures to prevent unauthorized access or change, transfer or deletion of personal information. Such measures include, but are not limited to, internal review of our data collection practices, filings and processing by the duly appointed Data Protection Officer as well as physical and technical measures to prevent access to the systems we use to store such sensitive data. Any data collected via Teamplace is filed at Frankfurt/Main, Germany, at the facilities of AWS "*EU (Frankfurt)*". Hence, the strict Data Protection Laws and Regulation of Germany, especially GDPR and BDSG, apply. AWS is the cloud provider Amazon Web Services Inc. (410 Terry Avenue North, Seattle WA 98109, USA) which only provides the server platform. The management of the data including their encryption is the responsibility of CMS and its parent company Cortado Holding AG (Alt-Moabit 91 b, 10559 Berlin, Deutschland). AWS has been certified according to German Principles of Basic IT Security of the TÜV Austria Group (https://www.tuv.at/en/tuev-austria-group/about-us/). For further information on data security at AWS, please visit https://aws.amazon.com/compliance/data-privacy-faq/ & https://aws.amazon.com/compliance/resources/. Both companies – Amazon Web Services Inc. and Cortado Holding AG – have entered into a Data Processing Agreement in accordance with article 28 of GDPR or section 11 of BDSG.

Access to and updating or deletion of personal data

CMS enables you to access your personal data through the various websites and offers you the possibility to correct, modify, or delete such data if necessary and if they are not required for legal means of processing of contractual relations. In the interest of data security, you have to identify yourself with your log-in credentials before you can modify or delete any personal data. For deletion, you can also contact our Data Protection Officer (see below).

Further privacy information

For additional information, as well as the Data Privacy Statement of the Teamplace website, and thus Teamplace's server-side cloud components, please visit: https://www.teamplace.net/en/policy/

Enforcement

CMS regularly checks compliance with this Data Privacy Statement. If you have any questions, comments, requests for information, rectification, processing restrictions, portability or erasure of data, please feel free to contact our duly appointed Data Protection Officer at dataprotection@teamplace.net. **You have the right to**

object at any time to the processing of your personal data or to revoke your consent. In addition, you have the right to complain to the relevant recourse authority.

Alterations and amendments

Please note that this Data Privacy Statement may be altered and/or amended from time to time. Without your express consent, though, we will not restrain your rights under the current Data Privacy Statement. Amendments and/or alterations concerning the Data Privacy Statement will be announced by CMS on the Teamplace websites. Earlier versions of the Data Privacy Statement will be filed and will be available for reference upon your request.

Berlin, May 2018

Legal Notes

Cortado Mobile Solutions GmbH

Alt-Moabit 91a
10559 Berlin, Germany

Phone: +49-30-408 198 500
Fax: +49-30-408 198 501
E-mail: info@cortado.com
Internet: www.cortado.com

Managing Directors: Sven Huschke, Benjamin Schüler
Commercial Register No.: *HRB 163439 B*
State regulator: Amtsgericht Berlin-Charlottenburg
Value Added Tax (VAT): DE297882285