TeamViewer
Data Processing Agreement (DPA)

1 Applicability

For the data processing activities described in **Annex 1** of this agreement, where Customer acts as data controller and TeamViewer acts as the Customer's processor, the parties agree to the following provisions on the commissioned processing of personal data, which shall supplement the TeamViewer End User License Agreement (**EULA**) (Data Processing Agreement, (**DPA)**) until further notice.

The DPA does not apply if the Customer is a natural person using the Software or the Services in the course of a purely personal or family activity (cf. Art. 2(2)(c) EU General Data Protection Regulation (EU 2016/679), (**GDPR)**).

The provisions of this DPA and the EULA concluded at the same time complement each other and exist side by side. In the event of any contradictions in the area of data protection, the DPA shall take precedence over the provisions of the EULA.

For Customer's convenience, TeamViewer provides an overview of how it collects and processes personal data in connection with the use of TeamViewer Software and Services in its Data Protection Information Sheet for TeamViewer Customers, as amended from time to time.

2 Rights and obligations of TeamViewer

2.1 Applicable laws

The obligations of TeamViewer shall arise from this DPA and the applicable data protection laws. The applicable laws shall in particular include the German Federal Data Protection Act (*Bundesdatenschutzgesetz* (**BDSG**)) and the GDPR.

2.2 Processing on instructions only

To the extent this DPA is applicable, TeamViewer shall only process personal data within the scope of this DPA and on documented instructions of the Customer, which are mutually agreed upon by the parties in the EULA and especially defined by the Product functionality, unless TeamViewer is required to do so by European Union or member state law to which TeamViewer is subject; in such a case TeamViewer shall inform the Customer of that legal requirement before processing, unless the respective law prohibits such information on important grounds of public interest. The Customer can give additional written instructions as far as this is necessary to comply with the applicable data protection law. The documentation on issued instructions shall be kept by the Customer for the term of the DPA.

2.3 Obligation of confidentiality

TeamViewer shall ensure that the persons authorized to process the personal data are committed to confidentiality or under an appropriate statutory obligation of confidentiality.

2.4 Technical and Organizational Measures

TeamViewer has implemented and maintains reasonable and appropriate technical and organization measures regarding the protection of personal data in accordance with Art. 32 GDPR (**TOMs**). The TOMs are described in detail in the documentation of the TOMs, which is attached to this DPA as **Annex 2**. Further information on TeamViewer's security can be found in TeamViewer's Trust Center.

The TOMs take into account the state of art, the implementation costs, and the nature, scope, context and purposes of processing personal data to ensure a level of security appropriate to the risk to the rights and freedoms of the natural persons affected by the processing. To this end, the protection objectives of Art. 32 (1) GDPR, such as confidentiality, integrity and availability of systems and services and their resilience in terms of the nature, scope, as well as context of the processing shall be addressed in such a way that the risks are mitigated continuously by appropriate TOMs.

The procedures for the regular review, assessment, and evaluation of the effectiveness of the then-current TOMs is further described in **Annex 2**. The TOMs are subject to technical progress and further development. TeamViewer may review and update the TOMs from time to time without notification of the Customer, provided that any such update will not degrade the security of the personal data and of the Software and Services of TeamViewer.

2.5 Assistance with requests

TeamViewer shall, taking into account the nature of the processing, assist the Customer as far as this is possible by appropriate technical and organizational measures in the fulfillment of requests to exercise the rights of affected data subjects as referred in Chapter III of the GDPR. Should a data subject contact TeamViewer directly to exercise the data subject's rights regarding the data processed on behalf of the Customer (as far as identifiable), TeamViewer shall immediately forward such request to the Customer. Upon request, the Customer shall remunerate TeamViewer with an appropriate compensation for the effort resulting from such assistance, if and as far as permitted by applicable data protection laws.

2.6 Assistance with compliance with Art. 32 - 36 GDPR

Taking into account the type of processing and the information available to TeamViewer, TeamViewer shall support the Customer with appropriate technical and organizational measures to comply with the obligations mentioned in Art. 32-36 GDPR, especially with regard to the security of the processing, the notification of personal data breach, the data protection impact assessment as well as the consultation with supervisory authorities. Upon request, the Customer shall remunerate TeamViewer an appropriate compensation for the effort resulting from such assistance, if and as far as permitted by applicable data protection laws.

2.7 Records of processing activities

TeamViewer will provide the Customer with the information necessary to maintain the records of processing activities.

2.8 Data Deletion

At the choice of the Customer, TeamViewer shall delete or return the personal data that is processed on behalf of the Customer, if and to the extent that the law of the European Union or a member state to which TeamViewer is subject does not provide for an obligation to store the personal data.

2.9 Assistance with demonstration of DPA compliance

TeamViewer shall provide the Customer with all information necessary to demonstrate compliance with the obligations resulting from Sections 2 and 3 of this DPA. TeamViewer will also provide certificates of regular audits by recognized auditors or other qualified third parties, if required.

If and insofar there are objectively justified indications of a violation of this DPA or of data protection regulations by TeamViewer, TeamViewer will enable and contribute to additional audits, including inspections, which are carried out by the Customer or by a qualified auditor appointed by the Customer. When conducting the inspection, the Customer will not disrupt TeamViewer's operations in a disproportionate manner.

2.10 Notification of doubts regarding the instructions

TeamViewer shall inform the Customer immediately if TeamViewer is of the opinion that the execution of an instruction could lead to a violation of the applicable data protection law. TeamViewer is entitled to suspend the execution of the relevant instruction until it is confirmed in writing or changed by the Customer after the review.

2.11 Notification of breaches

If TeamViewer detects violations of the applicable data protection law, this DPA, or instructions of the Customer regarding the commissioned processing of personal data, TeamViewer shall inform the Customer immediately.

2.12 Data protection officer

TeamViewer has appointed an external data protection officer, who can be reached at privacy@teamviewer.com, or at TeamViewer Germany GmbH, for the attention of the Data Protection Officer, Bahnhofsplatz 2, 73033 Göppingen, Germany.

2.13 Data transfers to a third country

TeamViewer will generally only transfer personal data processed within the scope of this DPA to a country outside the EU or the European Economic Area (**EEA**) for which no adequacy decision of the EU Commission in the sense of Art. 45(3) GDPR exists (**unsafe third country**), provided that:

a. the Customer or the Customer's user gives TeamViewer instructions for such a transfer, e.g., by requesting TeamViewer to establish a connection to an endpoint located in an unsafe third country (in such cases the Customer is responsible for ensuring that the data transfer is carried out in accordance with Art. 44 et seq. GDPR), or

b. TeamViewer is obliged to do so according to the law of the European Union or a member state to which TeamViewer is subject; in such a case TeamViewer will inform the Customer about these legal requirements prior to processing, unless the respective law prohibits such a communication on important grounds of public interest.

Furthermore, TeamViewer shall be entitled to utilize Subprocessors in a third country to process personal data, insofar as the requirements of Art. 44 GDPR are met.

3 Subprocessors

3.1 Authorised Subprocessors

TeamViewer utilizes the services of a number of another processors (hereinafter, "**Subprocessors**"). The list of Subprocessors used by TeamViewer for each of the TeamViewer products can be found under the following link as Annex 3. By concluding the DPA, the Customer agrees to the engagement of the Subprocessors that are included in Annex 3 at the time of concluding the DPA for the relevant TeamViewer Product.

3.2 Appointment of new Subprocessors

If TeamViewer wishes to commission further or other Subprocessors to provide the contractually agreed services (e.g., hosting), such Subprocessors have to be selected with the required care and due diligence. TeamViewer shall notify the Customer at least fifteen (15) days in advance about the appointment of any new Subprocessors. The Customer has the right to object to the engagement of the Subprocessor by stating objectively comprehensible reasons. If no objection is raised within this period, the new Subprocessor notified accordingly shall be deemed approved. If, in the event of an objection within the deadline, no solution can be reached, either party is entitled to terminate the DPA with a notice period of two (2) weeks. When the termination of the DPA becomes effective, the EULA shall also be considered terminated. Reference is made to section B.5.5 (Consequences of termination) of the EULA.

3.3 Subprocessors in third countries

Subprocessors in third countries may only be engaged if the special requirements of Art. 44 et seq. GDPR are fulfilled.

3.4 Obligations of Subprocessors

TeamViewer shall structure the contracts with Subprocessors in a way that they comply with the requirements of the applicable data protection laws and this DPA and shall oblige the Subprocessors to commission additional or different Subprocessors with the processing of personal data when observing the provisions of section 3.2 towards TeamViewer. TeamViewer shall contractually impose obligations on the Subprocessors providing sufficient warranties that the appropriate technical and organizational measures will be implemented in such a way that the processing is carried out in accordance with the requirements of the GDPR and this DPA.

4 Changes to this DPA

TeamViewer is generally entitled to amend the provisions of this DPA. TeamViewer will inform the Customer about the planned change and the content of the new DPA at least twenty-eight (28) days before such changes become effective. The change is considered approved if the Customer does not object to TeamViewer within fifteen (15) days after receipt of this information. If the Customer objects to the change, the DPA continues under the existing conditions.

5 Liability

Reference is made to Art. 82 of the GDPR.

For the rest, it is agreed that the regulations on limitation of liability from the corresponding license agreement shall apply.

Annex 1 to the Data Processing Agreement

Details of Data Processing – TeamViewer products

Version as of 17 March 2025

Content

1 Subject

The general subject of data processing is described in the EULA as well as in the relevant Product Specification.

2 Duration

The duration of the data processing corresponds to the duration of the EULA.

3 Nature and purpose of the processing

TeamViewer will process personal data as the Customer's Processor in order to enable the use of the Software and Services as defined under the EULA according to documented instructions (in accordance with the product functionality) of the Customer and/or its users. This essentially covers the processing of the transmitted content as well as the organization of the contents of the user account.

When using the respective TeamViewer products, TeamViewer will carry out the processing activities on behalf of the Customer as set out below.

The further specification of the Software and Services is provided under the Product Specification Page. Processing outside the scope of this DPA is described in the Product Privacy Notice.

Product	Nature and Purpose of the Processing
All TeamViewer products (except Frontline, Assist AR, Engage/Co-Browsing function module and Classroom, see separate section below)	- Processing of the data that the user enters into the user account, in particular storage and making it accessible to other users in the context of the connection e.g., name, contacts, email address, profile picture, as well as content data of the connections (e.g., chat). - Processing of contacts stored in the user's account, e.g., contact lists. - Transmission of the content data from the respective user to other users within a remote connection (e.g., desktop image, transmitted data and files as well as any other information exchanged). - Processing of data in the context of company profile management, such as licensed devices, rules, administration of the company profile, distribution of company policies, user access management, connection reports, Wake on LAN feature, etc. - Transmission of the obfuscated client account data through the new security feature (if applicable). - Processing of data in the context of meeting session planning e.g., start time, meeting topic, participants, meeting ID. - Processing data in the scope of the provision of an integration service. - Providing Customer and/or technical support. - Provisioning of the Connection Report feature. - Allowing iOS in-app purchases and linking them to an account. - Procession of data in connection with your use of specific features or functions (available in the respective product depending on your license), e.g.: • **Remote Monitoring**, encompassing the monitoring of critical aspects of Customer’s devices. • **Network Device Monitoring**, encompassing the monitoring of the availability and issues of network devices, such as routers, printers, etc. • **Asset Management, Asset Management and Discovery**, encompassing visibility of all Customers IT assets. • **Patch Management**, encompassing monitoring of vulnerabilities and patching of Customer’s software and OS, as well as 3rd party applications. • **Endpoint Protection**, encompassing the protection of Customer’s devices against viruses, trojans, spyware, ransomware etc. • **Endpoint Protection/Endpoint Detection & Response**, processing of personal data for the purpose of providing security and data protection services, enhancing threat defenses, and providing licenses to TeamViewer and endpoint protection/ endpoint detection and response products and services. • **Device Management**, processing of data for the purpose of providing mobile device management services. • **Remote Scripting**, which includes the creation, storage, deployment, and execution of scripts on remote devices. • **Web Monitoring**, that ensures proper uptime, performance, and functionality. • **Backup**, encompassing the backup of Customer’s business data. • **Grafana Plugin**, hosting service for providing Grafana PlugIn to the corresponding account, if desired by the Customer. • **Conditional Access**, e.g., providing the Customer with a dedicated server. • **REACH registry**, processing data in context of the feature. • **Meeting**, processing of contacts stored in the user's address book to organize meetings, e.g., sending invitations, Outlook integration, and transmission of the content data entered by the

	respective user to other users within a meeting (image and sound as well as possible transmission of the data and files). • **IoT**, processing of sensor data with TeamViewer IoT cloud and subsequent transmission through the APIs. • **Servicecamp/Service Desk**, including but not limited to ticket contents, creation and assignment of the tickets, ticket reporting, ticket status, and service instance configuration parameters. • **Automations,** connecting TeamViewer data to a wide range of solutions.
Frontline and **Assist AR**	- Hosting of the login interface, as well as administration of relevant areas, such as users, devices, systems etc. - Setup of Frontline/Assist AR workplaces (mobile as well as wearable), including the device as well as user setup. - Hosting and display of the dashboards as well as contact lists, asset management, workflow management and task deployment. - Provision of the in-built voice command recognition, if requested by the Customer. - Speech-to-text functionalities, including live captioning, transcription and translation. - Hosting of data in connection with Frontline xPick (e.g., pick-order management, workflow and task information, KPIs etc., including maintaining third-party components in workflows). - Hosting of the integration service, if requested by the Customer. - Transmission of the Frontline remote support calls. - Hosting of the remote support call recordings and remote call logs in connection with overall remote support administration, if requested by the Customer. - Services in the area of Holo-Lens technology, e.g., provision of eye-tracking functionality and augmented reality 3D points. - Provision of support services, especially with regard to the customer feedback. - Hosting and management of Twilio console, if requested by the Customer. - Third level support for Customer's server instances, if requested by the Customer. - Transmission of the content data during the virtual remote support session (image, video, and sound as well as possible transmission of the data and files). - Enabling of a chat function, including the translation of chat content. - Provisioning the Optical Character Recognition (OCR) feature.
Engage/Co-Browsing function module	- Provision of services within the scope of TeamViewer Engage/ Co-Browsing function module, including but not limited to hosting of the Customer data as well as maintenance and support services. - Provision of services within the scope of so-called video chat and live chat functionalities, including transmission and hosting of chat contents and other associated services, e.g., chatbots. - Provision of services within the scope of appointment scheduling and eSignature functionalities. - Provision of so-called software development kits (SDKs) for Customer applications enabling the integration of certain TeamViewer Engage/Co-Browsing functionalities within Customers own mobile apps (e.g., co-browsing, chats, etc.).
Classroom	- Provision of services within the scope of so-called video conference and live chat functionalities, including transmission and hosting of chat contents (including file transfer) and other associated services, e.g., conference notes. Provision of whiteboard, document sharing and tracking, polling, and breakout room services. - Provision of account services including registration and account management.
AI services	- Provision of AI assisted features, e.g., session summaries, categorization, tagging, capturing, summarizing, anonymizing, and hosting of the session data.
TeamViewer DEX/ 1E DEX	- Processing of personal data in connection with your use of the Digital Employee Experience Platform (**DEX**) modules, including but not limited to • **Endpoint Troubleshooting,** providing visibility into and control over every endpoint.

	• **Experience Analytics,** using collected device data to monitor common friction factors that affect the digital workplace. • **Endpoint Automation,** encompasses endpoint management capabilities, e.g., reducing configuration drift, identifying incident root causes, and executing self-healing remediations. • **Inventory Insights,** normalizing inventory and hardware data into vendor, product, and version records for analytical and reporting purposes. • **Application Experience Management,** providing visibility of application experience by users and making a score for user experience evaluation available. • **Patch Insights,** providing an overview of the last mile patching required on Customer's environment. • **Content Distribution,** encompasses content delivery by utilizing bandwidth effectively enabling devices to share content locally, reducing redundancy. • **Virtual Desktop Experience,** providing proactive health management, and streamlining operations. • **1E Intelligence,** multiplying IT's impact by merging edge and cloud AI for fast, precise, and deeply informed decisions and actions, e.g., Insights on emerging DEX issues, automated root-cause analyses, recommendation and remediation guidance. • **1E Catalog,** curating data for Software or Hardware information for Vendor, Title, Colloquial, Version and Edition. • **PXE Everywhere,** allowing computers to automatically boot up into Windows PE to install Windows Operating System. - Processing personal data in the scope of provisioning integration services, such as • **Automated Self Service for ServiceNow (SCC (Service Catalog Connect) and Virtual Assistant),** encompassing a set of advanced automation capabilities to extent the Service Catalog and Virtual Agent to instantly fulfill requests without making end users wait. • **Service Desk Augmentation (ITSM Connect and 1E Core),** providing real time incident investigation and remediation capabilities inside of ServiceNow. • **CMDB Connector**, providing the Device details to Service Now's CMDB. • **Service Graph Connector**, providing Device and Software details to ServiceNow CMDB. - Provisioning of SaaS solutions, e.g., • **Intune**, providing mobile device management (MDM) and mobile application management (MAM) to control device usage and manage applications on company-owned and personal devices. • **Device Refresh**, optimizing device refresh strategies on devices. • **Business Impact,** processing data when opening incident tickets in an ITSM solution or offloading data to other solutions like Splunk. • **Software Reclaim,** providing an overview of software inventory usage to unused or rarely used software from your organization's endpoints.

4 Type of personal data

The following types of personal data are processed by TeamViewer as a Processor:

Product	Type of Personal Data Processed
All TeamViewer products (except Frontline, Assist AR, Engage/Co-Browsing	- Content data exchanged between TeamViewer clients during a connection session, e.g., video and audio stream (screen views and user camera), file transfers, text chat, remote control commands, ticket content, whiteboard, as well as personal data required for the establishing of the connection.

function module and Classroom, see below)	- User account information, e.g., TeamViewer ID, username, display name, email, IP address, profile picture (optional), language preference, meeting ID, location, password. The domain of the client as well as the account age (e.g., “older than 6 months”) will be shown to the session host before connection as part of our Showing Supporter Data During Connection security feature. - User account management and administration data, e.g., user profile storing and sharing, account details, contact list, contact information, chat history, file attachment. - Company profile administration and management data, e.g., company profile, company policies, associations with user accounts, user access management, connection reports. - Personal data processed in context of functionalities (available depending on your license), including without limitation: customized modules; push notifications as initiated by the users; mailing services (e.g., notifying, updating, and reporting parameters as defined by the Customer); password reset (e.g., hosting account reset and mailing service, email with reset link, assignment of the new password to the account) as well as trusted device management (e.g., email notifications to prevent misuse of a device for login); audit logs to track changes from the user. - Connection data stored locally on the user’s device (log files, txt-files with the connections). - Personal data processed in the scope of an integration service (e.g., connection data, ticket content, etc.). - Personal data processed in the scope of Customer and/or technical support. - Personal data displayed in the Connection Report (device data, text, image, audio, video and metadata of the session). - iOS In-app purchase data and subscription expiration date. - Personal data processed in connection with your use of specific features or functions (available in the respective product depending on your license), e. g.: • **Remote Monitoring:** Device information (e.g., device name, machine name, disk space, online state, event, CPU usage etc. as described in Product Specifications); Historic alert data per device (e.g., suspicious alerts or events as defined by the Customer’s individual settings; Scripting data (e.g., device name, user credentials, executed scripts per device depending on how the Customer chooses to execute the script); Content of the connections between the management console and managed devices. The content data is always encrypted, and TeamViewer can never access any of the content; Error log data stored on the user’s device; Information in connection with customized individual monitoring policies. • **Asset Management, Asset Management and Discovery:** Device information (e.g., type of the devices, device name, disk space, hardware details, installed software etc. as described in Product Specifications); and discovering devices in the network through scanner. • **Patch Management:** Device information (e.g., type of the devices, device name, machine name, disk space, online state, event, CPU usage, installed software etc. alongside with the executed patches per device. • **Endpoint Protection:** Device information alongside the security and anti-virus protection alerts per device as well as historic alert data (affected device, malware type, date etc.). • **Endpoint Protection/Endpoint Detection & Response:** Contact information, IP address and device information, License data, machine and user specific data, location data, and other data required to provide the service. Some data will be processed to improve threat identification as part of the service. • **Mobile Device Management:** certain license information, your name, email address, username, IP address, meta data, location data, login credentials and mobile device data and similar in order to activate your license, respectively link it to your account and for the use of mobile device management more broadly. In addition, data changed through linked 3rd party accounts may be synced with your TeamViewer account and merged with data in the TeamViewer service. • **Backup:** Any data that the Customer chooses to backup, e.g., various files and folders that may include personal data. All data is encrypted, and only the Customer is able to download and decrypt the content from the backup. The creation, storage, recovery, and deletion of backups is executed in line with the parameters defined by the Customer. • **IoT:** Content data exchanged between TeamViewer clients during an IoT connection session (e.g., file transfers, remote control commands); data in connection with sensor management, e.g., IoT sensor information (Sensor ID, sensor names, metric names, metric value type (i.e., Celsius, kilogram, meter), data type (text, number, etc.) as well as IoT API credentials (e.g., certificates

	and credentials used to authenticate IoT devices to push IoT sensor data); data in connection with the analysis, visualization and setting of the measurements from sensors as well as processing of this data in the TeamViewer IoT cloud managed and adjusted by the Customer. • **Meeting:** subject of meeting, time zone, meeting ID, meeting start time, meeting end time; meeting scheduling and outlook integration (e.g., time and date of meetings, participants etc.); user account information (TeamViewer ID, username, IP address, profile picture, language settings, meeting ID, phone number, location, password). • **Service Camp/Service Desk:** Personal data in connection with ticket processing and reporting (e.g., TeamViewer IDs, emails, ticket subjects, date and time of tickets, content of the tickets, assignees as well as parameters defined by the Customer); Hosting the ticket meta data (e.g., creation and closing date/time, status, assignee etc.); Personal data in connection with ticket reporting, e.g., location, status, priority, assignee, average resolution times, user activities etc. as defined by the Customer. • **Remote Scripting:** Device information, prompts, number of prompts over a timeframe, etc. • **Web Monitoring:** IP address, location data, response time, credentials, system status. • **Automations:** Depending on customer configuration, e.g. event logs, connection data, etc.
Frontline	- User account data (e.g., email, password, domain, IP address, profile picture, display name, phone number, roles and permissions, team name, role, organization, language, status (online/offline), 2-factor authentication, phone book information). - Personal data in connection with the initiated session, e.g., session ID, security tokens (login and refresh), IP address, username, start time, device information, session validity, as well as exchanged content. - Personal data in connection with the used device which enables the user to use Frontline, e.g., device ID, name, IP address, username, application version, Bluetooth MAC address, device firmware version, device logs, step counts and the achievement count (if available). - Personal data in connection with the calls made using the devices using xAssist. e.g., ID, username, team name, call link and title, start/end time and date, call event logs, multimedia asset information (video, image, text, sound etc.), call status. - Personal data in connection with the workflows, e.g., IDs, title, creation/update time and date, owner, step entry information, version number, tags. - Personal data in connection with service reports, e.g., call details, title, internal number, date/time, description, status. - Personal data in connection with assets, in particular, Frontline specific assets, incl. but not limited to workflows (.uwe), components (.uce), and application (.uab). - Picking, article and system information as well as warehouse information, as long as they contain user data. - Personal data in connection with sensor information, if any (e.g., creator, user etc.). - Personal data in connection with tasks, if any (e.g., creator, user etc.). - Personal data in connection with set cookies, which allows for personalization and improvement of the products. - Personal data in connection with the speech-to-text features, e.g., personal Identifier (Account ID) as well as the audio content of the session.
Assist AR	- Personal data in connection with the initiated session, e.g., session ID, security tokens (login and refresh), IP address, username, device information, session validity, as well as transferred stream (video and audio feeds), file transfers, text chat, remote control commands, ticket content, whiteboard, team name, call link and title, start/end time and date, call event logs, chat logs, multimedia asset information (video, image, text, sound etc.), call status. - User account information, e.g., TeamViewer ID, username, display name, email, IP address, profile picture (optional), language preference, telephone number(s), location, password. - Personal data in connection with the user account management and administration, e.g., user profile storing and sharing, account details, buddy list, contact information, chat history, file attachments, password, domain, IP address, roles and permissions, status (online/offline), 2-factor authentication, phone book information. - Personal data in connection with the company profile administration and management data, e.g., company profile, company policies, associations with user accounts, user access management.

	- Personal data transmitted during the TeamViewer Assist AR augmented reality video feed, as well as the hosting of the content. - Personal data in connection with the SMS product invite (e.g., phone number). - Push notifications as initiated by the users. - Personal data in connection with the speech-to-text features, e.g., personal Identifier (Account ID) as well as the audio content of the session, if activated by the user. - Personal data processed within the mailing services (e.g., notifying, updating, and reporting parameters defined by the Customer). - Personal data in connection with service reports, e.g., call details, title, internal number, date/time, description, status. - Personal data in connection with assets, in particular, Assist AR specific assets, incl. but not limited to application (.uab) assets. - Personal data in connection with password reset (e.g., hosting account reset and mailing service, email with reset link, assignment of the new password to the account) as well as trusted device management (e.g., email notifications to prevent misuse of a device for login). - Personal data required for Optical Character Recognition (OCR), including video data and session metadata.
Engage/Co-Browsing function module	Personal Data processed in connection with the use of the functions: - **TeamViewer Co-Browsing:** • IP address, which is collected when establishing a connection through Co-Browsing, since the browser and server exchange IP addresses. By default, TeamViewer does not store or further process IP addresses, except to determine an approximate User location through the ISP (Internet Service Provider). • Depending on how and where a Customer uses Co-Browsing. If Co-Browsing is e.g., used during a checkout process, where the User can enter personal data such as name, email, address, payment information etc., then personal data can be made visible to the Agent. The sequences of User’s keystrokes are not put into context to identify, structure, process, categorize, nor analyze the personal data they may contain (such as name, etc.). • Co-Browsing recording, which may include personal data as described in this section (optional). • Personal data processed via so-called local storage variables and cookies, including the Session ID, acceptance of privacy policy (true/false). Such variables and cookies are by default set only for the duration of the session and are not used to re-identify the User at a later stage. More information on cookies and local storage variables are included as ***Appendix - Engage*****/*****Co-Browsing*** below. • User interactions, including mouse movements, clicks, scrolls, visited pages. • Employee personal data, e.g., name, email, language, assigned Co-Browsing sessions, Co-Browsing recordings, number of Co-Browsing sessions, activity logs, status, average co-browsing and chat durations per Employee, initiated and accepted co-browsing sessions, declined sessions, ended sessions and similar depending on Customer preferences. • Personal data included in various reports, including but not limited performance, statistical and similar reports. - **Live Chat, Video Chat, Chatbots** • IP address, which is collected when a chat conversation is initiated, since the browser and server exchange IP addresses. By default, TeamViewer does not store or further process IP addresses, except to determine an approximate User location through the ISP (Internet Service Provider). • Personal data provided by users themselves, including but not limited to names, email addresses, phone number, invoice numbers, account numbers, financial information, attachments such as pictures, files, videos and similar. • Personal data relating to Live Chat, e.g., Session ID, browser and device information, or notices made by the Customer’s Employees as well as chat recordings. • Personal data in connection with the video chat as initiated between the Customer’s users and Customer’s Employees, including audio and video transmission, as well as personal data in

	connection with their interaction, involving e.g., whiteboard, screensharing, or documents, as applicable. • Personal data processed via so called local storage variables and cookies, including the Session ID, acceptance of privacy policy (true/false), interaction with chat. Such variables and cookies are by default set only for the duration of the session and may be used to re-identify the User at a later stage, depending on Customer's default configurations. More information on cookies and local storage variables are included as ***Appendix – Engage/Co-Browsing*** below. • Chat history stored in the data center for certain period of time by the Controller's Customers. • Employee personal data, e.g., name, email, language, assigned Chats, number of chats, activity logs, status, number of chats, chat durations per Employee, number of conversations by Employee and similar depending on Customer's preferences. Further information may include how long did it take for an Employee to open an assigned chat, how much time did he spend reading the chat, how much time did he spent answering (also how many text blocks/message templates did an employee use) etc. depending on Customer's default configurations. • Personal data included in various dashboards and reports, including but not limited performance, statistical and similar reports. - **Appointment Scheduler** • Contact information of Customer's Users (e.g., name, email address, phone number). • Sending out and hosting of appointment confirmations as well as reminders. • Hosting of appointment information and history. • Personal data included in various dashboards and reports, including but not limited performance, statistical and similar reports.
Classroom	- IP address, which is collected when a session with TeamViewer's services is established, this is because the browser and server exchange IP addresses. By default, TeamViewer does not store or further process IP addresses, except to determine an approximate User location through the ISP (Internet Service Provider). - Personal data provided by users themselves, including but not limited to names, email addresses, attachments such as pictures, files, videos and similar. - Personal data relating to the Video Conference session, e.g., Session ID, browser and device information, or notices made by the Customer's Employees as well as chat recordings. - Personal data in connection with the Video Conference as initiated between the Customer's users and Customer's Employees, including audio and video transmission, as well as personal data in connection with their interaction, involving e.g., whiteboard, screensharing, or documents, as applicable. - Personal data processed via so called local storage variables and cookies, including the Session ID, acceptance of privacy policy (true/false), interaction with chat. Such variables and cookies are by default set only for the duration of the session and may be used to re-identify the User at a later stage, depending on Customer's default configurations. More information on cookies and local storage variables are included as ***Appendix - Classroom*** below. - Chat history stored in the data center for certain period of time by the Controllers Customers. - Employee personal data, e.g., name, email, or language, activity logs. - Video conference recordings if Customer chooses to record and store then.
AI services	- User interactions during the session. - Data entered or generated, depending on the features in use.
TeamViewer DEX/ 1E DEX	- Device data processed by all DEX modules and on-device clients, including but not limited to device identifiers, network adapter information, time zone. - Personal data processed in connection with your use of specific modules: • **Experience Analytics:** usage data, e.g., device interaction data, browser interaction data and replies to user surveys. • **Application Experience Management:** software data e.g., software publisher and version, software interaction data, software crash and hang data.

	• **Virtual Desktop Experience:** virtual desktop infrastructure data, including connection start and end timestamps. • **1E Intelligence:** personal data including instruction metadata and author. • **Patch Insights:** missing and applied patches. • **Integration services:** e.g., device information, usernames. - **SaaS solutions:** device information, including but not limited to software inventory, audit logs (non-persistent) domain, email address, persona (if configured by the solutions admin).

5 Categories of data subjects

The following categories of data subjects are affected by the data processing:

Product	Categories of Data Subjects
All TeamViewer products (except Engage/Co-Browsing function module, Classroom, see below)	- Customer (to the extent that the Customer's personal data is processed in accordance with section 4) and, if applicable, Customer's users, including end users of managed devices. - The connection partners of Customer/Customer's users. - Third parties managed by Customer/Customer's users, or third parties whose personal data is passed on by Customer/Customer's users.
Engage/Co-Browsing function module /Classroom	- Users (Customer's customers, website visitors, prospects, third parties). - Customer's Employees (Agents).
AI services	- Customer (to the extent that the Customer's personal data is processed in accordance with section 4) and, if applicable, Customer's users, including end users of managed devices. - The connection partners of Customer/Customer's users. - Third parties managed by Customer/Customer's users, or third parties whose personal data is passed on by Customer/Customer's users.
TeamViewer DEX/ 1E DEX	- Customer (to the extent that the Customer's personal data is processed in accordance with section 4) and, if applicable, Customer's users, including end users of managed devices. - Third parties managed by Customer/Customer's users, or third parties whose personal data is passed on by Customer/Customer's users.

Appendix - Engage/Co-Browsing **to Annex 1**

1. Local Storage as website integration

Key	**Related Feature/ Plugin**	**Purpose/Description**	**Lifespan**
cvvid	/	VisitorId - can be assigned temporarily or permanently	Session or permanent
CV_i	Live Chat	"true" if privacy policy has been accepted in chat.	Session
cv_sp	Live Chat	Indicator whether a message has been sent or an interaction (*e.g.*, button click) has taken place by the User.	Session
visited	Live Chat	"true" as soon as the User interacts with the WebChat for the first time - *e.g.*, to trigger a chatbot only once.	Session
cvsid	Co-Browsing	SessionId to ensure the continuity of a co-browsing session when changing pages or across multiple tabs.	Session
cv-shrid	Co-Browsing	5-digit numerical code through which an employee can connect to an employee by co-browsing.	Session
cv-s	Co-Browsing	"true" as soon as customer releases his session or has requested co-browsing.	Session
cv-lvcs	Co-Browsing	Indicator that the session has been closed - necessary to end the co-browsing session across multiple open tabs.	Session
CV_LVD	Co-Browsing	Temporary data for switching between two tabs - to ensure continuity of co-browsing session	Session

2. Cookies for website integration

In order to enable continuous sessions not only on the same domain (*e.g.,* user switches from yourwebsite.com to yourwebsite.com/imprint) but also across various Customer domains (*e.g.*, user switches from yourwebsite.com to wiki.yourwebsite.com), the local storage variables are "converted" into cookies. In this case the purpose and naming remain the same as for the Local Storage Variables.

Key	**Related Feature/ Plugin**	**Purpose/Description**	**Lifespan**
cvsid	Co-Browsing	SessionId to ensure the continuity of a Co-Browsing session when changing pages or across multiple tabs.	Session
cv-shrid	Co-Browsing	5-digit numerical code through which an employee can connect to an employee by Co-Browsing.	Session
cv-s	Co-Browsing	"true" as soon as customer releases his session or has requested Co-Browsing.	Session
cv-lvcs	Co-Browsing	Indicator that the session has been closed - necessary to end the Co-Browsing session across multiple open tabs.	Session
CV_LVD	Co-Browsing	Temporary data for switching between two tabs - to ensure continuity of Co-Browsing session.	Session

3. Local storage for video chat and video consultations

Key	**Related Feature/ Plugin**	**Purpose/Description**	**Lifespan**
jitsiMeetId	Video Chat & Video Consultation	Unique id for Video Chat session	Session
language	Video Chat & Video Consultation	Specifies and maintains language of user interface	Session
features/base /settings	Video Chat & Video Consultation	Technical variable	Session
features/base /known-domains	Video Chat & Video Consultation	Technical variable	Session
features/dropbox	Video Chat & Video Consultation	Technical variable	Session
features/calendar-sync	Video Chat & Video Consultation	Technical variable	Session
features/recent/list	Video Chat & Video Consultation	Technical variable	Session

features/video-layout	Video Chat & Video Consultation	Technical variable	Session
callStatsUserName	Video Chat & Video Consultation	Technical variable	Session
cvvid	Video Chat & Video Consultation	VisitorId - can be assigned temporarily or permanently	Session or permanent
CV_DOC_UID	Video Chat & Video Consultation	VisitorId – for documents feature	Session
cv-t	Video Chat & Video Consultation	TabID – defines on what tab in the video chat the user currently is (Video, Document, Whiteboard, Co-Browsing)	Session
cv_sp	Video Chat & Video Consultation	Indicator whether a message has been sent or an interaction (e.g., button click) has taken place by the User.	Session

Appendix - Classroom to Annex 1

1. **Local storage for video conferences**

Key	**Related Feature/ Plugin**	**Purpose/Description**	**Lifespan**
jitsiMeetId	Video Conference	Unique id for Video Conference session	Session
language	Video Conference	Specifies and maintains language of user interface	Session
features/base /settings	Video Conference	Technical variable	Session
features/base /known-domains	Video Conference	Technical variable	Session
features/dropbox	Video Conference	Technical variable	Session
features/calendar-sync	Video Conference	Technical variable	Session
features/recent/list	Video Conference	Technical variable	Session
Features /video-layout	Video Conference	Technical variable	Session
callStatsUserName	Video Conference	Technical variable	Session
cvvid	Video Conference	VisitorId - can be assigned temporarily or permanently	Session or permanent
CV_DOC_UID	Video Conference	VisitorId – for documents feature	Session
cv-t	Video Conference	TabID – defines on what tab in the video chat the user currently is (Video, Document, Whiteboard)	Session
cv_sp	Video Conference	Indicator whether a message has been sent or an interaction (e.g., button click) has taken place by the User.	Session

TeamViewer

Overview of Technical and Organizational Measures

Version as of 17 March 2025

Content

1 Access Control

1.1 Data Centers

TeamViewer does not own, lease or operate any TeamViewer server infrastructure for its offices or production environment. The TeamViewer corporate environment is a purely cloud-based infrastructure hosted in data centers provided by third parties. All third parties are certified under ISO 27001 standard.

TeamViewer has access control measures in place to prevent unauthorized access to data processing equipment where personal data is stored or processed.

1.2 TeamViewer Offices

Only authorized persons have physical access to premises, buildings or rooms where the personal data is processed. TeamViewer facilities are protected by key systems, intrusion detection systems, access control measures and active key management. Access rights are granted to authorized staff on an individual basis, including visitors who must be accompanied by authorized personnel. Employees and visitors are required to wear their badges visibly at all times when on the premises.

2 System Access and Access Control

TeamViewer relies on the following system access control measures to prevent unauthorized persons from using data processing systems where personal data is stored or processed.

2.1 Network and Hardware Security

The TeamViewer corporate network is protected from the public network by firewalls and threat detection as well as subsequent removal systems. The latest anti-virus/malware detection software is used to detect, remove and prevent malicious code. Security patch management is implemented and remote access to the TeamViewer corporate network is protected by strong authentication mechanisms and a Virtual Private Network (VPN).

TeamViewer uses a role-based security architecture and requires that users of the system be identified and authenticated before they can use system resources. Resources are protected by native security and add-on software products that identify and authenticate users and validate access requests against users' authorized roles in access control lists.

All resources are managed in the asset inventory system and each resource is assigned an owner. The owners are responsible for approving access to the resource and performing checks on access by role.

Employees log in to the TeamViewer network with an Active Directory user ID and password. Users must also log in separately to any systems or applications that do not use Active Directory's split sign-on functionality. Passwords must meet defined password standards and are enforced by parameter settings in Active Directory. These settings are part of the configuration standards and force users to change passwords at a defined interval. User IDs are locked after a certain number of unsuccessful logins attempts to prevent access to system and resources. Additionally, after a defined period of inactivity, users' screens are locked automatically.

TeamViewer has a password policy that governs the proper use and setup of passwords, including the frequency with which they must be changed, minimum requirements, and complexity.

Employees accessing the system from outside, the TeamViewer network must use a VPN tunnel and two-factor authentication system. Employees are issued VPN certificates when they are hired, and access is disabled when they leave.

TeamViewer employees access the two-factor authentication services over the Internet by using the Secure Socket Layer (SSL) functionality of their web browser. The employees first enter a valid user ID and password to gain access to TeamViewer cloud resources. The passwords must match the password configuration requirements configured on the virtual devices using the virtual server administration account. Virtual devices are initially configured according to TeamViewer configuration defaults, but these configuration parameters can be changed using the virtual server administration account.

TeamViewer maintains a Security Operations Center (SOC) that monitors critical systems and alerts around the clock to manage security incidents. These services are operated in a compliant and data protection-friendly manner while ensuring a threat response that is appropriate to the organization's risk level.

TeamViewer employees can log in to their systems via virtual server administration accounts. These administration accounts use a two-tier authentication system based on digital certificates.

User IDs and access rules are defined according to the role of each employee. Access rules are predefined based on the defined roles. When changes are made to a position, the associated rights and access rules are changed accordingly.

Regularly, access rights are reviewed by technical owners on the basis of team needs, tasks to be separated, and risks associated with access rights.

The revocation of rights and access as well as the deactivation of the account in the event of an employee's departure ("offboarding") or in the event of a change of position is carried out by the IT Service Desk to delete the employee's access or adjust the access rights.

Reporting Line Managers review the lists and enter the required changes into the event management record. The record is returned to the security help desk for processing. The IT Service Desk Manager identifies any records that have not been returned within two weeks and contacts the manager.

Only authorized persons can access systems that process personal data. TeamViewer uses multiple authorization levels when granting access to systems. All employees access TeamViewer's corporate systems via a personalized account (user ID) and have access only to the systems they need to access to perform their duties. Authorizations and privileges are reviewed on a regular basis. Similarly, rights to access systems are reviewed when the employees are assigned new roles or leave TeamViewer.

2.2 Hiring ("Onboarding") and Departure ("Offboarding") of Employees

When an employee is hired, they are assigned to a position in the HR management system. Before the employee's start date, the HR team creates a so-called "onboarding" ticket that contains the employee's user IDs and the access rights to be granted. The ticket is used by the IT service desk to create user IDs and access rules. The access rules are defined according to the minimal principle (each employee is granted only the permissions he/she needs to perform his/her task). In addition, the ticket system contains a template for employees who change their position and the associated rights, which must be changed accordingly within the existing access rules.

Access rights of technical owners are reviewed regularly to determine if they need to be revoked. When evaluating access rights, team leaders consider the job description, the tasks to be separated, and the risks associated with access rights.

After an employee's employment ends, the HR department creates an offboarding ticket. These tickets are processed automatically to remove the employee's access in all systems. The IT Service Desk uses the tickets to lock user IDs and delete all access roles from IDs owned by the ticket's employee. TeamViewer will carry out regular checks into these lists to ensure that automated corrections have been implemented correctly.

2.3 Data Access Control

TeamViewer controls access to systems containing personal data through a mixture of role-based access control (RBAC) and user rights management. This ensures that access to and use of data is minimized, both in terms of general processing and in terms of the list and scope of access for TeamViewer employees. These access controls vary depending on the sensitivity of the data stored and operational requirements. In addition to granting access to individual employees, for some systems, specific access can be granted for a limited amount of time with an approval process. Also, workload identity federation is being used to grant access to resource on specific systems.

2.4 Data Separation

The networks are segregated and segmented. This works within RBAC to minimize risks in line with sound security and data protection practices. For example, data for different products/purposes are processed separately where possible, including by separating production and test environments. Where appropriate, data is processed separately to avoid unnecessary mixing of data and processing beyond the purpose.

2.5 Pseudonymization

TeamViewer uses pseudonymization where it can be applied without affecting the efficiency of processes and/or where it is necessary to protect data in the event that disclosure is required. Where possible as part of the disclosure process, anonymization is used. Data that can identify data subjects contained in pseudonymized data is stored separately and encrypted where possible.

TeamViewer has a process for assessing internal data sharing and uses pseudonymization to limit the use of personal data for certain purposes.

3 Measures to Establish the Integrity

3.1 Transfer Control

TeamViewer has transfer controls in place to ensure that data is secure during transmission and that the level of protection does not fall below a minimum standard once it leaves the perimeter.

These security measures include securing transmissions with SSL/TLS, https, etc. and the use of VPNs throughout the organization. TeamViewer maintains firewalls and other standard security systems to protect its operations and data.

Firewall systems are in place to filter unauthorized incoming network traffic from the Internet and to deny any type of network connection that is not explicitly authorized.

3.2 Data Input Control

TeamViewer has systems in place to log who has accessed or modified personal data, including linking such controls to individual accounts.

4 Data Availability and Resilience of the Systems

TeamViewer creates backups of critical data in accordance with common practice and ensures that these backups act as a reliable failover in the event of a catastrophic failure.

Customer data is backed up and monitored by Operations staff for completeness and disruptions. In the event of a disruption, the Operations staff performs troubleshooting to identify the root cause and then reruns the backup job immediately or as part of the next scheduled backup job. Backup infrastructure is physically secured in locked cabinets and/or caged environments within third-party data center. The backup infrastructure resides on private networks that are logically secured from other networks.

Incident response policies and procedures are in place to guide the personnel in reporting and dealing with information technology incidents. Procedures are in place to detect, report, and respond to system security breaches and other incidents. Incident response procedures are in place to detect and respond to incidents on the network.

TeamViewer monitors the utilization of physical and computer infrastructure, both internally and for customers, to ensure that service delivery meets service level agreements.

TeamViewer evaluates the need for additional infrastructure capacity in response to the growth of existing customers or the addition of new customers. Infrastructure capacity monitoring includes, but is not limited to, the following:

- Data center space, power, and cooling
- Disk storage
- Tape storage
- Network bandwidth

TeamViewer has implemented a patch management process to ensure that the customer relevant and infrastructure systems used for the service on the TeamViewer side are patched in accordance with operating system patches recommended by the respective vendor. TeamViewer system owners review proposed operating system patches to determine if the patches are applied.

TeamViewer is responsible for determining the risk of applying or not applying patches based on the security and availability impact of these systems and any critical applications hosted on them. TeamViewer staff will verify that all patches have been applied and that a reboot has been performed, if applicable.

Redundancy is built into the system infrastructure that supports the data center services to ensure that there is no single point of failure, which includes firewalls, routers, and servers. If a primary system fails, the redundant hardware is configured to take its place.

Penetration testing is performed to measure the security posture of a target system or environment. The commissioned third-party vendor uses an industry-standard penetration testing methodology specified by TeamViewer. The third-party vendor's approach begins with a vulnerability assessment of the target system to determine what vulnerabilities exist on the system that can be exploited through a penetration test, simulating a disgruntled/affected insider or an attacker who has gained internal access to the network.

Once the vulnerabilities are identified, the third-party vendor attempts to exploit the vulnerabilities to determine if unauthorized access or other malicious activity is possible.

Penetration testing includes testing of the network and application layers, as well as testing of the controls and processes around the networks and applications. Testing is performed both externally (external testing) and within the network.

Vulnerability scans are performed daily by TeamViewer in accordance with its internal policies. Upon request by a customer and at TeamViewer’s discretion, a penetration test may also be performed by a third-party vendor in accordance with TeamViewer policies. The third-party vendor uses industry standard scanning technologies and a formal methodology specified by TeamViewer. These technologies are customized to efficiently test the organization's infrastructure and software while minimizing the potential risks associated with active scanning.

Retests and on-demand scans are performed as needed. Vulnerability Scans are performed outside of peak business hours.

Tools that need to be installed in the TeamViewer system are implemented via the change management process. Scanning is performed with approved scan templates and with bandwidth throttling options enabled.

4.1 Incident Response Management

TeamViewer maintains contingency plans to respond to potential security threats. The incident response plan has defined processes to detect, mitigate, investigate, and report security incidents. It includes incident verification, attack analysis, containment, data collection, and problem remediation.

If TeamViewer becomes aware of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data of Customer while processed by TeamViewer, TeamViewer will notify Customer of such a security incident, provide information about the security incident and take appropriate measures to mitigate adverse effects and to minimize any damage from the security incident, according to the stipulations in the Data Processing Agreement.

To be notified of recent security updates, a security bulletin is available for subscription.

5 Data Protection Management

TeamViewer maintains comprehensive privacy policies and procedures for which the Data Protection Officer (DPO) and TeamViewer management are ultimately responsible. TeamViewer continually updates its privacy and security measures in accordance with updated policies, applicable laws and best practices. This includes regular reviews of documentation of procedures, training, and technical and organizational measures, maintaining and creating records of processing activities, and conducting data protection impact assessments, including other relevant assessments, as appropriate.

TeamViewer has processes, policies and procedures that describe physical security, logical access, computer operations, change control and data communication standards. All employees are obliged to adhere to TeamViewer policies and procedures that define how services are to be delivered. These are located on the company intranet and can be viewed by any TeamViewer employee.

The Employees receive regular data protection training and are bound to confidentiality. TeamViewer conducts regular awareness training for employees at least once a year, but the frequency may increase as needed.

TeamViewer designates at least one person per department who is responsible for compliance and implementation of the requirements of the General Data Protection Regulation (GDPR). All responsible data protection staff members have at least one IAPP CIPP qualification (or equivalent) relevant to their area of work.

A review of the effectiveness of the technical and organizational measures is carried out at least annually. Data protection impact assessments and other relevant assessments are carried out when necessary.

There is a formalized policy for handling data subject requests under the GDPR.

All employees are trained internally in accordance with Art. 32 (4) GDPR and are obliged to ensure that personal data is handled in accordance with data protection requirements.

After termination of the contractual relationship with the employee, the data will be deleted in accordance with the principles of data protection with data minimization taken into account.

5.1 Subprocessors

TeamViewer enters into a Data Processing Agreement (DPA) with all subprocessors of personal data. Furthermore, TeamViewer ensures that all subprocessors comply with the relevant security and data protection standards and that these requirements and obligations are included as part of the DPA. DPAs meet the requirements of the GDPR including (where applicable) the latest version of the Standard Contractual Clauses.

In the case of long-term cooperation, there is an ongoing review of subprocessors and the level of protection afforded to data processed with each one.

6 Data Protection by Design and by Default

Personal data is collected and processed only to the extent necessary for the prescribed purpose. Data subjects have a simple way to exercise their rights.

Data protection principles are already observed during software development. In particular, the employees are encouraged and trained to implement technical and organizational measures as part of product development that ensure compliance with the requirements of GDPR and, specifically the rights of data subjects. The software is designed in such a way that the amount of data collected as well as the scope of processing is limited to the extent necessary. Insofar as various settings options exist within the software, the setting in which the smallest possible amount of personal data is processed is always selected in the delivery state, excluding core functionalities. Development teams work in close relation with the privacy team to ensure data protection requirements are implemented in TeamViewer's products.

With respect to change control, TeamViewer maintains documented Software Development Life Cycle (SDLC) policies and procedures to guide personnel in documenting and implementing application and infrastructure changes. Change control procedures include as follows: Change request and initiation processes, documentation requirements, development practices, quality assurance testing requirements, and required approval procedures.

A ticketing system is used to document change control procedures for changes in the application and implementation of new changes.

Quality assurance tests and results are documented and maintained along with the corresponding change request. Development and testing are performed in an environment that is logically separated from the production environment. Management approves changes prior to migration to the production environment and documents these approvals in the ticketing system. Version control software is used to manage source code versions and migrate source code through the development process to the production environment. Version control software maintains a history of code changes to support rollback capabilities and tracks changes for developers.

All infrastructure changes to the environment are reviewed and approved by the Change Advisory Board (CAB). The CAB consists of, at a minimum, the Head of the IT Infrastructure, the Head of the Application and Demand Management, a member of the IT Security Team, and the change requestor. This ensures that all changes are reviewed, and that the quality of the implementation is maintained.

TeamViewer

Annex 3 to the Data Processing Agreement

Subprocessor List

Version as of 17 March 2025

The following entities may process your personal data as subprocessor or further subprocessor, depending on your contractual partner.

1. Subprocessors for TeamViewer's products (except Frontline, Engage/Co-Browsing and Classroom, see separate Sections below)

Name	Location	Provided Service
Anexia Internetdienstleistungs GmbH	Feldkirchnerstrasse 140, 9020 Klagenfurt, Austria	Hosting
Amazon Web Services EMEA Sarl *(except Assist AR)*	38 Avenue John F. Kennedy, L-1855 Luxemburg	Hosting
Microsoft Ireland Ltd.	South County Business Park, One Microsoft Place, Carmanhall and Leopardstown, Dublin, D18 P521, Ireland	Hosting
Google Ireland Ltd.	Gordon House, Barrow Street, Dublin 4, Ireland	Hosting
Schwarz IT KG	Stiftsbergstraße 1, 74172 Neckarsulm, Germany	Hosting
TeamViewer Greece EPE	Leoforos Dodonis 147, 45221 Ioannina, Greece	Maintenance and Development
TeamViewer Portugal, Unipessoal Lda	Rua Manuel Pinto de Azevedo, 860, 7º, 4100-320 Porto, Portugal	Maintenance and Development
TeamViewer Austria GmbH	Graben 5, 4020 Linz, Austria	Maintenance and Hosting
TeamViewer Germany GmbH	Bahnhofsplatz 2, 73033 Goeppingen, Germany	TeamViewer Products and Services

Additional Features, against separate order or activation of function modules		
Malwarebytes Inc. *(only applicable for the function modules Endpoint Protection/Endpoint Detection & Response by Malwarebytes)*	3979 Freedom Circle, Santa Clara, CA 95054, USA	Endpoint Protection; Endpoint Detection & Response *(optional)*
Lansweeper NV (*only applicable for the Asset Management and Discovery*)	Fraterstraat 212, 9820 Merelbeke, Belgium	Asset Management and Discovery *(optional)*
Ivanti UK Limited *(only applicable for the Mobile Device Management)*	3 Arlington Square Downshire Way, Bracknell, RG12 1WA, United Kingdom	Mobile Device Management *(optional)*
1E Limited	8 Devonshire Square, Wework, London, EC2M 4YJ, United Kingdom	TeamViewer DEX/ 1E DEX Products (*optional*, hosting locations as agreed)
Workato, Inc.	215 Castro St., Suite 300, Mountain View, CA 94041, USA	Automations (*optional*, EU hosting location)
Exclusively for connections from and to China		
Alibaba.com (Europe) Limited	Herengracht 448, 1017 CA, Amsterdam, the Netherlands	Hosting

2. Subprocessors for TeamViewer Frontline

Name	**Location**	**Provided Service**
Microsoft Ireland Ltd.	South County Business Park, One Microsoft Place, Carmanhall and Leopardstown, Dublin, D18 P521, Ireland	Hosting
TeamViewer Greece EPE	Leoforos Dodonis 147, 45221 Ioannina, Greece	Maintenance and Development
TeamViewer Portugal, Unipessoal Lda	Rua Manuel Pinto de Azevedo, 860, 7º, 4100-320 Porto, Portugal	Maintenance and Development
Google Ireland Ltd.	Gordon House, Barrow Street, Dublin 4, Ireland	Hosting
TeamViewer Germany GmbH	Bahnhofsplatz 2, 73033 Goeppingen, Germany	TeamViewer Products and Services
Additional Features, on specific request or under special circumstances		
Twilio Inc. *(only if requested by the Customer)*	375 Beale Street, Suite 300, San Francisco, CA 94105, USA	Hosting of the video and audio feed (*optional*)
Business Objects Software Limited (“SAP”) *(only applicable for the Customers using the SAP Global Partner Support Center)*	1012 - 1014 Kingswood Avenue, Citywest Business Campus, Dublin 24, Ireland	Hosting of customer support portal (*optional*)

3. Subprocessors for TeamViewer Engage/ Co-Browsing/ Classroom

Name	Location	Provided Service
Amazon Web Services EMEA Sarl	38 Avenue John F. Kennedy, 1855 Luxemburg	Hosting
Hetzner Online GmbH	Industriestraße 25, 91710 Gunzenhausen, Germany	Hosting
TeamViewer Greece EPE	Leoforos Dodonis 147 45221 Ioannina, Greece	Maintenance and Development
TeamViewer Portugal, Unipessoal Lda	Rua Manuel Pinto de Azevedo, 860, 7º, 4100-320 Porto, Portugal	Maintenance and Development
TeamViewer Austria GmbH	Graben 5, 4020 Linz, Austria	Maintenance and Hosting. Hosting locations for Engage/Co-Browsing: for all customers – EU; only for Japanese customers – Japan Hosting location for Classroom: EU
TeamViewer Germany GmbH	Bahnhofsplatz 2, 73033 Goeppingen, Germany	TeamViewer Products and Services

4. Subprocessors for TeamViewer DEX/ 1E DEX

Name	Location	Provided Service
Atlassian Pty Ltd.	350 Bush Street Floor 13 San Francisco, CA 94104 United States	Customer Support AI Services
Datadog Inc.	620 8th Ave 45th Floor, New York, NY 10018, United States	Monitoring and Logging
Microsoft Ireland Ltd.	South County Business Park, One Microsoft Place, Carmanhall and Leopardstown, Dublin, D18 P521, Ireland	Hosting
Outsystems Inc.	55 Thomson Place, 2nd floor, Boston MA 02210, United States	Development platform used to design and deploy DEX applications
Pendo.io, Inc.	Raleigh, 301 Hillsborough St, Suite 1900, United States	1E Application UI
1E Limited	8 Devonshire Square, Wework, London, EC2M 4YJ, United Kingdom	TeamViewer DEX/ 1E DEX Products (hosting locations as agreed)

5. Professional Services, Service Level Support

Name	Location	Provided Service
TeamViewer Affiliates	Affiliated Companies	Professional Services, Service Level Support