Annex 1 to the TeamViewer Data Processing Agreement
Details of Data Processing – TeamViewer Remote Management

1. Subject

The general subject of data processing is described in the EULA as well as in the relevant Product Specification. The DPA is not applicable for the services provided in connection with TeamViewer web-monitoring module.

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 Customer content in connection with the purchased functionalities of TeamViewer Remote Management, including:

- Processing of the data in connection with Remote Monitoring, encompassing the monitoring of critical aspect of Customer's devices.
- Processing of the data in connection with Network Device Monitoring, encompassing the monitoring of the availability and issues of network devices, such as routers, printers, *etc*.
- Processing of the data in connection with Asset Management, encompassing visibility of all Customers IT assets.
- Processing of the data in connection with Patch Management, encompassing monitoring of vulnerabilities and patching of Customer's software and OS, as well as 3rd party applications.
- Processing of the data in connection with Endpoint Protection, encompassing the protection of Customer's devices against viruses, trojans, spyware, ransomware *etc*.
- Processing of the data in connection with Remote Management Backup, encompassing the backup of Customer's business data.
- Hosting service for providing Grafana PlugIn to access the Remote Management data to the corresponding account, if desired by the Customer.

Where the Customer has elected to purchase the additional Endpoint Protection service offered by TeamViewer in partnership with Malwarebytes Inc., the personal data will be processed solely for the purposes of providing security and data protection services, enhancing threat defenses, and providing licenses to TeamViewer and Malwarebytes products and services.

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 relevant Product Privacy Notice.

4. Categories of personal data

In connection with the use of the TeamViewer Remote Management, the following types

of personal data shall be processed by TeamViewer as Processor:

4.1. Content data that is 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).

4.2. User account information, *e.g.*, TeamViewer ID, username, display name, email, IP address, profile picture (optional), language preference, location, password.

4.3. Personal data in connection with the user account management and administration, *e.g.*, user profile storing and sharing, account details, address book, buddy list, contact information, chat history.

4.4. 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, connection reports.

4.5. Connection data stored locally on the user's device (log files, txt-files with the connections).

4.6. Push notifications as initiated by the users.

4.7. Personal data processed within the mailing services (*e.g.*, notifying, updating, and reporting parameters defined by the Customer).

4.8. Personal data processed 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).

4.9. Following Information in connection with product functionalities

No.	Functionality	Personal Data
1.	**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 Remote 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
2.	**Asset Management**	• Device information, *e.g.,* type of the devices, device name, machine name, disk space, online state, event, CPU usage, installed software etc. as described in Product Specifications. • Information in connection with customized individual monitoring policies
3.	**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.
4.	**Endpoint Protection**	• Device information alongside with the security and anti-virus protection alerts per device as well as historic alert data (affected device, malware type, date *etc*.).
5	**Endpoint Protection by Malwarebytes**	• 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.
6.	**Remote Management 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.

5. Categories of Data Subjects

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

5.1. The Customer's users (*e.g.,* end users of managed devices).

5.2. Third parties managed by the Customer / Customer's users.

Version as of 1st of March 2022