Anlage 1 zum Auftragsverarbeitungsvertrag
Einzelheiten der Verarbeitung - TeamViewer Remote Management

1. Gegenstand

Der allgemeine Gegenstand der Verarbeitung ist in der EULA sowie in der jeweiligen Produktspezifikation beschrieben. Der AVV gilt nicht für die in Verbindung mit dem TeamViewer Web-Monitoring-Modul erbrachten Leistungen.

2. Dauer

Die Dauer der Verarbeitung entspricht der Laufzeit der EULA.

3. Art und Zweck der Verarbeitung

TeamViewer wird personenbezogene Daten als Auftragsverarbeiter des Kunden verarbeiten, um die Nutzung der im Rahmen der EULA bereitgestellten Software und Services nach dokumentierten Weisungen (im Rahmen der Produktfunktionalität) des Kunden und/oder seiner Benutzer zu ermöglichen.

Dies umfasst im Wesentlichen die Verarbeitung von Inhalten des Kunden im Zusammenhang mit den erworbenen Funktionalitäten von TeamViewer Remote Management, einschließlich:

- Verarbeitung der Daten im Zusammenhang mit Remote Monitoring, welches die Überwachung kritischer Aspekte der Geräte des Kunden umfasst.
- Verarbeitung der Daten im Zusammenhang mit dem Network Device Monitoring, welches die Überwachung der Verfügbarkeit und Probleme von Netzwerkgeräten wie Routern, Druckern etc. umfasst.
- Verarbeitung der Daten im Zusammenhang mit dem Asset Management, welches die Sichtbarkeit aller IT-Assets des Kunden umfasst.
- Verarbeitung der Daten im Zusammenhang mit dem Patch Management, welches die Überwachung von Schwachstellen und das Patchen der Software und des Betriebssystems des Kunden sowie der Anwendungen von Drittanbietern umfasst.
- Verarbeitung der Daten im Zusammenhang mit Endpoint Protection, die den Schutz der Geräte des Kunden vor Viren, Trojanern, Spyware, Ransomware etc. umfasst.
- Verarbeitung der Daten im Zusammenhang mit dem Remote Management Backup, das die Sicherung der Geschäftsdaten des Kunden umfasst.
- Hosting-Service für die Bereitstellung des Grafana PlugIns für den Zugriff auf die Remote Management Daten auf das entsprechende Konto, falls vom Kunden gewünscht.

Wenn der Kunde sich für den Erwerb des zusätzlichen Endpoint Protection Leistung entschiedet, der von TeamViewer in Zusammenarbeit mit Malwarebytes Inc. angeboten wird, werden die personenbezogenen Daten ausschließlich zum Zweck der Erbringung von Sicherheits- und Datenschutzdienstleistungen, der Verbesserung der Bedrohungsabwehr und der Bereitstellung von Lizenzen für TeamViewer- und Malwarebytes-Produkte und -Dienstleistungen verarbeitet.

Die weitere Spezifikation der Software und der Dienste finden Sie auf der Produktspezifikationsseite.

Die Verarbeitung außerhalb des Geltungsbereichs dieser DPA ist in der jeweiligen Produktdatenschutzinformation beschrieben.

4. Kategorien von personenbezogenen Daten

Im Zusammenhang mit der Nutzung des TeamViewer Remote Managements werden folgende Arten von personenbezogenen Daten von TeamViewer als Auftragsverarbeiter verarbeitet:

4.1. Inhaltsdaten, die während einer Verbindung zwischen TeamViewer-Clients ausgetauscht werden, z.B. Video- und Audiostream (Bildschirmansichten und Benutzerkamera), Datei-transfers, Text-Chat, Fernsteuerungsbefehle, Ticketinhalte, Whiteboard.

4.2. Benutzerkontoinformationen, z.B. TeamViewer ID, Benutzername, Anzeigename, E-Mail-Adresse, IP-Adresse, Profilbild (optional), Spracheinstellung, Standort, Passwort.

4.3. Personenbezogene Daten in Verbindung mit der Benutzerkontoverwaltung und -administration, z.B. Speichern und Freigeben von Benutzerprofilen, Kontodetails, Freundesliste, Kontaktinformationen, Chat-Verlauf, Dateianhänge.

4.4. Personenbezogene Daten im Zusammenhang mit der Verwaltung und dem Management des Firmenprofils, z.B. Firmenprofil, Firmenrichtlinien, Zuordnungen zu Benutzerkonten, Verwaltung des Benutzerzugangs, Verbindungsberichte.

4.5. Lokal auf dem Gerät des Benutzers gespeicherte Verbindungsdaten (Log-Dateien, txt-Dateien mit den Verbindungen).

4.6. Push-Benachrichtigungen, wie von den Benutzern initiiert.

4.7. Personenbezogene Daten, die im Rahmen der Mailing-Dienste verarbeitet werden (z.B. Benachrichtigungs-, Aktualisierungs- und Reporting-Parameter, wie vom Kunden definiert).

4.8. Personenbezogene Daten, die im Zusammenhang mit dem Zurücksetzen von Passwörtern verarbeitet werden (z.B. Hosting-Service zum Zurücksetzen von Konten, E-Mail mit Rücksetzungslink, Zuweisung des neuen Passworts zum Konto) sowie sog. Trusted Device Management (z.B. E-Mail-Benachrichtigungen zur Verhinderung des Missbrauchs eines Geräts für den Login).

4.9. Folgende Informationen in Verbindung mit Produktfunktionalitäten

Nr.	Funktionalität	Personenbezogene Daten
1.	**Remote Monitoring**	• Geräteinformationen, z.B. Gerätename, Maschinenname, Festplattenspeicherplatz, Online-Stand, Ereignisse, CPU-Auslastung usw. wie in den Produktspezifikationen beschrieben. • Historische Alarmdaten pro Gerät, z.B. verdächtige Alarme oder Ereignisse, wie sie durch die individuellen Einstellungen des Kunden definiert sind. • Scripting Daten, z.B. Gerätename, Benutzeranmeldeinformationen, ausgeführte Skripte pro Gerät (je nachdem, wie der Kunde das jeweilige Skript ausführen möchte).

		• Inhalt der Verbindungen zwischen der Remote Management Konsole und verwalteten Geräten. Die Inhaltsdaten sind immer verschlüsselt, sodass TeamViewer niemals auf die Inhalte zugreifen kann. • Fehlerprotokolldaten, die auf dem Gerät des Benutzers gespeichert sind. • Informationen in Zusammenhang mit maßgeschneiderten individuellen Überwachungsrichtlinien (Policies)
2.	**Asset Management**	• Geräteinformationen, z.B. Typ der Geräte, Gerätename, Maschinenname, Festplattenspeicherplatz, Online-Stand, Ereignisse, CPU-Auslastung, installierte Software usw. wie in den Produktspezifikationen beschrieben. • Informationen in Zusammenhang mit maßgeschneiderten individuellen Überwachungsrichtlinien (Policies)
3.	**Patch Management**	• Geräteinformationen, z.B. Typ der Geräte, Gerätename, Maschinenname, Festplattenspeicherplatz, Online-Stand, Ereignisse, CPU-Auslastung usw. sowie die ausgeführten Patches pro Gerät.
4.	**Endpoint Protection**	• Geräteinformationen zusammen mit den Sicherheits- und Virenschutzwarnungen pro Gerät sowie historische Warndaten (betroffenes Gerät, Malware-Typ, Datum usw.).
5.	**Endpoint Protection von Malwarebytes Inc.**	• Kontaktinformationen, IP-Adresse und Geräteinformationen, Lizenzdaten, maschinen- und benutzerspezifische Daten, Standortdaten und andere Daten, die zur Bereitstellung des Dienstes erforderlich sind. Einige Daten werden zur Verbesserung der Bedrohungserkennung als Teil des Dienstes verarbeitet.
6.	**Backup**	• Alle Daten, die der Kunde zur Sicherung auswählt, z.B. verschiedene Dateien und Ordner, die auch personenbezogene Daten enthalten können. Alle Daten werden verschlüsselt, und nur der Kunde ist in der Lage, den Inhalt aus der Sicherung herunterzuladen und zu entschlüsseln. Die Erstellung, Speicherung, Wiederherstellung und Löschung von Backups erfolgt in Übereinstimmung mit den vom Kunden definierten Parametern.

5. Kategorien von betroffenen Personen

Die folgenden Kategorien von Personen sind von der Verarbeitung betroffen:

5.1. Die Benutzer des Kunden (z.B. Endbenutzer von verwalteten Geräten).

5.2. Dritte, die vom Kunden / den Nutzern des Kunden verwaltet werden.

Stand vom 1. März 2022