

DATENSCHUTZHINWEIS ZUR FERNWARTUNG VIA TEAMVIEWER

Nach Artikel 13 und 14 der EU-Datenschutzgrundverordnung (DSGVO) bestehen Informationspflichten bei der Erhebung personenbezogener Daten. Aus diesem Grund werden Ihnen folgende Informationen zur Kenntnis gegeben:

Zweck der Datenverarbeitung

TeamViewer ist eine sichere Anwendung zur PC-Fernsteuerung und erlaubt Ihnen, die aktuellen Bildschirminhalte zweier über das Internet verbundener PCs wechselseitig in Echtzeit zu übertragen (sog. Desktop-Sharing). Mittels TeamViewer unterstützt Sie unsere Hotline bei Fragen noch komfortabler. Während Sie mit uns telefonieren, können wir mit TeamViewer via Internet auf Ihren Bildschirm schauen und die aufwändige Schilderung des Problems entfällt. Mit Hilfe eines mausgesteuerten Zeigers können wir Ihnen gezielt Hinweise geben.

Zugriff auf Ihren PC

Der Verbindungsaufbau ist erst möglich, wenn Sie Ihre Zustimmung erteilt haben. Dafür teilen Sie uns Ihre Verbindungs-ID und das Kennwort telefonisch mit. Nach Abschluss der Online-Session wird die Verbindung automatisch beendet. Bitte stellen Sie vor Nutzung von TeamViewer sicher, dass Sie alle Anwendungen und Daten schließen, die wir nicht einsehen sollen. Zusätzlich können Sie Fernzugriff auf Ihren Rechner erlauben. Den Umfang des Fernzugriffs bestimmen Sie selbst. Der Fernzugriff erfolgt erst, wenn Sie diesem per Mausklick zustimmen. Alle Tätigkeiten können Sie auf Ihrem Bildschirm verfolgen. Durch Klicken auf das Schließen-Symbol in TeamViewer kann eine Session von beiden Seiten jederzeit beendet werden

Datensicherheit

TeamViewer-Verbindungen laufen über komplett gesicherte Datenkanäle, die mit einem 2048 Bit RSA Public-/Private Key Exchange aufgebaut und mit 256 Bit AES verschlüsselt sind.

Diese Technik wird in vergleichbarer Form auch bei https/SSL eingesetzt und gilt nach heutigem Stand der Technik als vollständig sicher. Da der Private Key niemals den Clientcomputer verlässt, ist durch dieses Verfahren technisch sichergestellt, dass zwischengeschaltete Computer im Internet den Datenstrom nicht entziffern können, das gilt somit auch für die TeamViewer Routingserver. Jeder TeamViewer Client hat bereits den Public-Key unseres Masterclusters implementiert und kann so Nachrichten an den Mastercluster verschlüsseln bzw. dessen Signatur überprüfen.

Die Public-Key-Infrastruktur verhindert effektiv „Man-in-the-middle-Attacken“. Das Kennwort wird trotz Verschlüsselung niemals direkt, sondern im Challenge-Response Verfahren übertragen und ist nur auf den lokalen Computern gespeichert. Bei der Authentifizierung wird das Kennwort aufgrund der Verwendung des Secure Remote Password Protokolls (SRP) niemals direkt übertragen und es wird lediglich ein Passwort-Verifier auf dem lokalen Computer gespeichert. Mehr Informationen dazu finden Sie unter <https://dl.teamviewer.com/docs/de/TeamViewer-Security-Statement-de.pdf>

Empfänger der erhobenen Kontaktdaten

Es erhalten diejenigen Stellen Zugriff auf Ihre Daten, die diese zur Erfüllung Ihrer Aufgaben benötigen. Eine Weitergabe der Daten erfolgt ausschließlich an den Anbieter der Fernwartungssoftware, TeamViewer Germany GmbH, Bahnhofsplatz 2, 73033 Göppingen.

Rechtsgrundlage der Datenverarbeitung

Rechtsgrundlage ist Ihre Einwilligung gem. Artikel 6 Abs. 1 lit. a) DSGVO und/ oder Artikel 6 Abs. 1 lit. b) DSGVO, die Erfüllung eines Vertrags oder die Durchführung vorvertraglicher Maßnahmen auf Anfrage der betroffenen Person.

Speicherdauer

Die Speicherung erfolgt bis zur abschließenden Bearbeitung Ihres Anliegens. Nach Beendigung der Session wird der Verbindungsaufbau gelöscht. Sie sind zudem aufgefordert, evtl. während der Session -ungewollt-kompromittierte Passwörter unverzüglich zu ändern. Die Online-Session wird nicht aufgezeichnet.

Rechte der betroffenen Personen

Werden Ihre personenbezogenen Daten verarbeitet, so haben Sie das Recht Auskunft über die zu Ihrer Person gespeicherten Daten zu erhalten (Art. 15 DSGVO). Sollten unrichtige personenbezogene Daten verarbeitet werden, steht Ihnen ein Recht auf Berechtigung zu (Art. 16 DSGVO). Liegen die gesetzlichen Voraussetzungen vor, so können Sie die Löschung oder Einschränkung der Verarbeitung verlangen sowie Widerspruch gegen die Verarbeitung einlegen (Art. 17, 18 oder 21 DSGVO). Wenn Sie in die Datenverarbeitung eingewilligt haben, steht Ihnen gegebenenfalls ein Recht auf Datenübertragbarkeit zu (Art. 20 DSGVO). Weiterhin besteht ein Beschwerderecht bei der zuständigen Aufsichtsbehörde.

Widerruf bei Einwilligung

Wenn Sie in die Verarbeitung durch eine entsprechende Erklärung eingewilligt haben, können Sie die Einwilligung jederzeit für die Zukunft widerrufen. Die Rechtmäßigkeit, der aufgrund der Einwilligung bis zum Widerruf erfolgten Datenverarbeitung wird durch diesen nicht berührt. Der Widerruf kann formfrei erfolgen und sollte möglichst gerichtet werden an: info@frey-systeme.de

Stand: 30.06.2023