TÜVIT

Certificate

The certification body of TÜV Informationstechnik GmbH
herewith awards this certificate to the company

Certificate validity:
2024-08-21 – 2026-08-21

TeamViewer Germany GmbH
Bahnhofsplatz 2
73033 Göppingen, Germany

to confirm that the processes of its services

TeamViewer Remote and TeamViewer Tensor

fulfils all requirements of the criteria

Trusted Site Privacy, Version 2.1

of TÜV Informationstechnik GmbH. The requirements are summarised in the annex to the certificate.

The annex is part of the certificate with ID 5553.24 and consists of 5 pages.

Essen, 2024-08-21

Dr. Christoph Sutter, Head of Certification Body

To certificate

TÜV Informationstechnik GmbH
Am TÜV 1 ▪ 45307 Essen, Germany
tuvit.de

TÜVNORDGROUP

Certification Scheme

The certification body of TÜV Informationstechnik GmbH performs its certifications on the basis of the following certification scheme:

- German document: „Zertifizierungsprogramm (nicht akkreditierter Bereich) der Zertifizierungsstelle der TÜV Informationstechnik GmbH“, version 1.1 as of 2020-03-01, TÜV Informationstechnik GmbH

Evaluation Report

- German document: „Trusted Site Privacy – Gutachten Recht – TeamViewer Remote und TeamViewer Tensor“, version 1.2 as of 2024-07-17, TÜV Informationstechnik GmbH, Fachstelle für Datenschutzsachverständige

- German document: „Trusted Site Privacy – Gutachten Technik – TeamViewer Remote und TeamViewer Tensor“, version 1.2 as of 2024-07-12 TÜV Informationstechnik GmbH, Fachstelle für Datenschutzsachverständige

Evaluation Requirements

- German document: „Trusted Site Privacy, Version 2.1 Kriterienkatalog“, document version 4.0 as of 2018-01-04, TÜV Informationstechnik GmbH

The evaluation requirements are summarised at the end.

Evaluation Target

The target of evaluation „TeamViewer Remote und TeamViewer Tensor“ of TeamViewer Germany GmbH is defined in the document:

- German document: „Trusted Site Privacy – Target of Audit – Beschreibung des Prüfgegenstandes (ToA)”, version 1.2 dated 2024-07-12, TeamViewer Germany GmbH

Evaluation Result

- The Target of Evaluation fulfils all the applicable requirements of the Trusted Site Privacy criteria, version 2.1.

- The Target of Evaluation fulfils the requirements for anonymised data processing for the handling of data in the area responsibility of TeamViewer Germany GmbH.

Notes of the Certification Body

The certificate is not a certificate within the meaning of the EU General Data Protection Regulation (EU GDPR - Regulation 2016/679).

Certification in accordance with the EU GDPR by an accredited conformity assessment body requires, in accordance with Art. 42 para. 5 EU GDPR, that the competent federal or state data protection authorities or the European Data Protection Board in accordance with Art. 63 EU GDPR have approved the criteria for certification - i. e. the certification programme within the meaning of ISO/IEC 17065 in conjunction with ISO/IEC 17067 in conjunction with ISO/IEC 17067 - have been approved.

Summary of the Evaluation Requirements

1 Data protection audit

Legal requirements

On the basis of the defined target of evaluation, it is necessary to review which legal requirements apply to the processing of personal data and how these are integrated into the application context of the target of evaluation. Data protection must also be satisfied where laws, regulations and case law leave gaps and room for manoeuvre.

Permissibility of processing

After identifying the data types relevant to the evaluation, it is analysed for each data type whether the processing is permissible with regard to the purpose of the data processing. The requirements for data minimisation with regard to the state of the art are also taken into account.

Data subject friendliness

The consideration of the legitimate interests of the persons whose data is processed is checked here. Data subjects have a right to know what happens to their personal data, how it is further processed and whether there is a possibility of self-protection, i. e. influencing the processing of the data.
Data subjects should be informed about which of their data is processed and by which processes. The data subjects must be made aware of their rights, what information they can access and how their personal data is secured. Data protection must also play an important role in the drafting of contracts.
When using an IT product, the user must be informed about which functions the product has in order to be able to process personal data securely and in compliance with data protection regulations. This includes, for example, suitable product descriptions and installation instructions

or appropriate familiarisation or information provided by a company that introduces and uses an information processing product.

Transparency

The data protection policy, the data protection concepts and also the technical and organisational measures with which data protection is implemented in the company or process should be made transparent and understandable to all those affected. The focus of the investigation is that the measures taken to ensure long-term data protection must be transparent.

Data protection quality management

Changes in the area of information technology and the legal basis generally have an impact on the concept for fulfilling data protection requirements. They must be analysed and implemented regularly and in good time with regard to their impact on data protection. If necessary, analyses and action models must be adapted. The quality management measures based on this are the subject of the analysis.

Data security

The information systems used can only meet data protection requirements if appropriate technical and organisational measures have been taken with regard to data security. Appropriate concepts must be in place and corresponding trustworthy components should be used when setting up the systems.

- Access control (physical)

  Access to data processing systems with which personal data is processed or used must be effectively denied to unauthorised persons by means of suitable measures.

- Access control (authorisation)

  The use of data processing systems by unauthorised persons must be effectively prevented by appropriate measures.

- Access control (accessibility)

  Those authorised to use a data processing system should only be able to access the data subject to their access authorisation. Personal data must not be read, copied, modified or removed without authorisation during processing, use and after storage.

- Transmission control

  It must not be possible for personal data to be read, copied, modified or removed without authorisation during electronic transmission or during transport or storage on data carriers. It must be possible to check and determine to which bodies the transmission of personal data by data transmission equipment is intended.

- Input control

  It must be possible to subsequently check and determine whether and by whom personal data has been entered into, modified or removed from data processing systems.

- Order processing

  Personal data that is processed on behalf of the client may only be processed in accordance with the client's instructions. A contractor may only collect, process or use the data in accordance with the client's instructions.

- Availability control

  Personal data must be protected against accidental destruction or loss by appropriate measures.

- Separation requirement

  Suitable measures must be taken to ensure that data collected for different purposes can be processed separately.

2 Security analysis

Security of the components used as well as network and transport security

For all subcomponents that realise security functionalities, it was possible to verify that they can be classified as trustworthy on the basis of formal evaluations that have already been carried out and/or publicly available information.
The network and transport security correspond to the state of the art.

Means of system management

There are suitable configuration options, as well as appropriate monitoring and logging, which contribute to a secure operating status. The tools used for this are subject to the same security requirements as the IT product / IT system itself.

Tests und inspections

Extensive penetration tests for exploitable vulnerabilities, as well as analyses of the defence mechanisms at application level and checks of the authentication/authorisation procedures used are carried out. The vulnerabilities identified during the tests and analyses are assessed according to their level of risk.