



WHITEPAPER

Privacy & Security

Privacy & Security

TeamViewer solutions are used by 45 million users at any given point a day. Our solutions offer powerful functionalities to connect with colleagues, customers, devices and more – in video conferences, via remote access or further digital solutions – it is our utmost priority to keep these connections safe. We are committed to compliance, security and privacy in everything we do. Millions of users worldwide only trust a secure solution, and only a secure solution assures our long-term success as a business.

Data Protection

TeamViewer is a global organization and for us it is important that the personal data of our customers and our own employees is handled in accordance with GDPR. As part of our continuous focus on information security and data privacy our GDPR readiness activities were delivered through a managed program of activities in the following areas:

Privacy by design

Integrating data protection, privacy, and security requirements into product design and development methodologies. Embedding privacy requirements in the development cycle from ideation to launch, to validation. In short, we use privacy engineering techniques to evaluate and build better offerings to turn privacy by design policies into actions and tangible improvements.

Third-Party Management

Ensuring that TeamViewer's valued partners and suppliers are best able to meet their obligations with respect to data privacy and establishing transparent arrangements through appropriate information sharing agreements. When we work with new suppliers or with long-established strategic partners we look to apply industry-leading standards that safeguard personal information.

Documented Internal Policies and Procedures

Reviewing standards and processes to define the personal information lifecycle and help ensure data transparency, accuracy, accessibility, completeness, security, and consistency. Our Privacy Policy reflecting GDPR requirements sets the context for how we obtain, store and use information relating to our customers and our own people.

Information Security

Reviewing and improving our enterprise-wide information security framework, ensuring that incident response process remains effective and that confidentiality, integrity, and availability of personal information is assured through appropriate technical and organizational measures.

Information Governance

Mapping our data and identifying what we have, what we are doing with it, where it is, where it flows, and who has access to it. We classify data based on risk and sensitivity in context. The risk classification is based on data and person perspectives. This allows us to focus on the outcome and purpose of processing, leading to a more holistic risk profile and helping us inform our customers.

Further Informationen

- Data Processing Agreement (DPA)
(<https://www.teamviewer.com/en/eula/?t=1629882255052>)
- Technical and Organizational Measures
(<https://static.teamviewer.com/resources/2020/12/TeamViewer-Technical-and-Organizational-Measures.pdf>)

TeamViewer Engage Product Privacy Policy

At product level, TeamViewer Engage enables the administration of personal data through different functionalities such as defining the storage time of video conference recordings, chat histories, masking of personal data during Co-Browsing and more. To comply with all GDPR regulations, data is only being hosted within the EU.

Hosting

TeamViewer Engage is being hosted by TeamViewer Austria (as subcontractor) for TeamViewer Germany in an ISO 27001 certified, German data center. We are renting a dedicated Root Server from our data center that allows us to manage a self-administered, fail-safe Cloud.

Privacy Policy by Functionality

At functionality level, our customers have different options to fulfil their data subject rights as well as comply with their responsibilities regarding the GDPR agreement. Key features such as Live Chat, Video Chat and Co-Browsing offer the following possibilities:

- Encrypted connections and transmission (see 2.1)
- Possibility to record and/or archive interactions and personal data (specifically for audit purposes, e.g. MiFID II)
- Defining the storage time and/or automatic deletion of archived data
- Manual deletion of archived data
- Export possibilities of archived data (API)

Moreover, TeamViewer Engage offers an extensive Role and Rights Management, which limits the users' accessibility according to their actual necessities. Activity logs record any changes within the application to ensure audit compatibility.

Security

Encryption

All connections with TeamViewer Engage services are always SSL/TLS (Transport Layer Security) encrypted or in case of audio/video streams protected by DTLS/SRTP (Secure Real-Time Protocol, "Encryption in transit"). Moreover, stored data can be encrypted with the RSA 2048 Standard ("Encryption at rest").

Authentication

The authentication between Server-to-Server and Server-to-Client (User) takes place through JWT-Tokens (JSON Web Tokens). These tokens (auth + csrf) are securely transmitted through XHR-Requests using a HTTP Header and a "Secure Cookie". For user authentication, TeamViewer Engage supports various SSO-Standards (LDAP, OAuth, SAML2, Kerberos).

Security-first Development

To ensure the security of our software during the continuous development, we follow the best practices of modern software development. Our measures include internal guidelines for reviews (every new feature is reviewed by at least one Senior Software Developer and a central Product Security Team) and automated security software tests, which regularly review the different components' security risks of our application.

Certification

TeamViewer and its solutions are certified according to the following internationally recognized standards:

- ISO/IEC 27001 (Data Center)
- ISO 9001
- SOC 2 Type 2
- HIPAA/HITECH
- TISAX

To ensure the early detection of weak spots and guarantee the security of TeamViewer Engage, penetration tests are regularly conducted by external security specialists. In case a conference is recorded, it is necessary to temporarily store data in the cloud. Deletion of the data occurs when the recording is successfully pushed back to the on-premises installation.



TeamViewer Germany GmbH

Bahnhofsplatz 2, 73033 Göppingen, Germany
contact@teamviewer.com
www.teamviewer.com