General technical and organizational measures pursuant to Article 32 GDPR

Customer / Contract Data (Office)	TeamViewer Software (Data Center)
Confidentiality	
Access control to premises and facilities	
• Doors and gates at the premises are fitted with security locks and are securely locked outside of business hours. Access to the building is protected by electronic locks with different access levels as well as security guards at night. • Keys to the premises in which data is being processed are only in the possession of the responsible staff. The electronic lock system ensures that only authorized staff have access to restricted areas. • Each employee gets a key card which grants access to the premises dependent on the authorization of the respective employee. This key card also functions as an employee identity card (with picture). • Visitors of the office will be welcomed by the security service and will get a visitor pass (without picture). • The entrance areas are video monitored. • The premise is controlled 24/7 by a security service.	• Individual access control, video camera surveillance, motion detectors, 24/7 monitoring and on-site security personnel ensure access to the data center is only granted to authorized persons and guarantee the best possible security for hardware and data. There is also a detailed identification check at the entry to the data center.
Access control to systems	
• Access to data processing systems is managed through a two-step authentication with usernames and passwords. • Where enhanced access is required, two-factor authentication is enabled.	
Access control to data	
• Access to data processing systems is managed through a two-step authentication with usernames and passwords. • All staff processing personal data are adequately trained in and indentured to obey Data Secrecy pursuant to Article 32 of GDPR.	• At no point during a TeamViewer connection is TeamViewer able to view any connection content. The TeamViewer routing servers also cannot decipher the data stream. In addition, the client password is never sent directly, but only through a challenge-response procedure.

<table>
<tr><th colspan="2">Segregation control</th></tr>
<tr><td>Data is processed by separate systems, and these systems only process the data which is relevant to their purpose.</td><td>Access rights are used to ensure only data relevant to purpose is accessible.</td></tr>
<tr><th colspan="2">Integrity</th></tr>
<tr><th colspan="2">Disclosure control</th></tr>
<tr><td>Securing of electronic transmissions: external staff connects only via highly secure connections encrypted through 2048 bit RSA certificates.
Physical transport of files with personal data takes place only in closed containers.</td><td>Securing of electronic transmissions: connections to TeamViewer routing servers are only made through appropriate remote control solutions.</td></tr>
<tr><th colspan="2">Input control</th></tr>
<tr><td colspan="2">Activity logs in software applications are in place, where possible.</td></tr>
<tr><th colspan="2">Availability, resilience, ability to restore the availability and access to personal data</th></tr>
<tr><td>The following measures ensure that personal data is protected against destruction and accidental loss:
Fire safety measures: CO2 fire extinguishers for server rooms
Uninterruptible power supply (UPS) with surge protection
Air conditioning for server rooms: 9,400 watts air conditioning unit with central air conditioning acting as a backup
Use of RAID solutions: use of different RAID concepts depending on the purpose
Anti-virus concept:
Central firewall
Company-wide use of professional anti-virus software
Availability monitoring of critical systems
Host intrusion detection system</td><td>The central TeamViewer connection servers are hosted in state-of-the-art data centers with multi-redundant carrier connections and redundant power supply. Brand-name hardware is used exclusively.
Highest availability due to appropriate RAID solutions as well as daily backups in geographically separate locations.
Monitoring of the production infrastructure with Network Monitoring Software.</td></tr>
<tr><th colspan="2">Process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures</th></tr>
<tr><td colspan="2">Personal data is being processed exclusively within the scope of the instructions stipulated in this contract.
TeamViewer may only subcontract tasks related to the processing of personal data to companies with whom appropriate data processing agreements have been concluded.</td></tr>
</table>