How does the remote maintenance work?

We use **TeamViewer** for remote online-support.

For the supply of this programs and the data processing **TeamViewer** is responsible.

TeamViewer routs (TeamViewer GmbH, Jahnstr. 30, 73037 Göppingen, Germany) is secured using RSA public/private key exchange and AES (256 bit) session encryption. This technology is used in a comparable form for https/SSL and is considered completely safe by today's standards. As the private key never leaves the client computer, this procedure ensures that interconnected computers - including the TeamViewer routing servers - cannot decipher the data stream. Each TeamViewer client has already implemented the public key of the master cluster and can thus encrypt messages to the master cluster and check messages signed by it. The PKI (Public Key Infrastructure) effectively prevents "man-in-the-middle-attacks." Despite the encryption, the password is never sent directly, but only through a challenge-response procedure, and is only saved on the local computer. During authentication, the password is never transferred directly because the Secure Remote Password (SRP) protocol is used. Only a password verifier is stored on the local computer.

Translation of original German text from TeamViewer
https://www.teamviewer.com/de/security/

Here you will find the Security Information of TeamViewer
https://dl.tvcdn.de/docs/en/TeamViewer-Security-Statement-en.pdf

All customers are responsible to protect the data on his/her own computer.

By downloading and using the program TeamViewer you agree that this program is used by us for remote online support with you. Of course, you can end the remote online session at any time by yourself.