FAQ on Data Protection policy of Joineer AG

We are pleased to answer the most frequently asked questions about security as follows:

1. **How is authentication solved, how can an employee log in?**

The client registers the participating employees in the Excel file provided by Joineer with their first name, last name, e-mail address and team affiliation. For team or company administrators, this is noted accordingly. In addition, the hierarchy and questions are recorded in an iterative process with Joineer in the same Excel file. Employees do not actually register via the system, but are registered in advance. On the morning of the survey start, the participating employees will receive an automated e-mail from the sender no-reply@app.joineer.com via mg.joineer.ch. In this e-mail the participants are informed about the survey and go to our system: app.joineer.com with the personalised login link (via a button in the e-mail). If the employee has not been entered in Excel, he/she will not receive a login link and without a link he/she will not be able to access the system.

After a consent form, participants are directed to the survey. Quantitative and qualitative responses are protected during entry by the encrypted connection of the secure hypertext transmission protocol. See documents 'Data Protection policy' and 'IT architecture' of Joineer AG for information on how the web application and database are protected.

2. **Does your solution support SSO / 2FA?**

After logging into the system, participants can set up password-protected access to the tool instead of direct access via the link received by e-mail. Participants access this option via Dashboard → Profile → Enable password protection. Participants who have activated password protection now log in to the system via the URL https://app.joineer.com/ with their e-mail and password.
For storage, salting and hashing of passwords are used.

This single sign-on procedure is based on current and secure encryption algorithms and authentication methods. Sensitive data is encrypted in a one-way fashion and therefore cannot be read by Joineer AG administrators. It is protected by SSL (Secure Sockets Layer) encryption. With daily backups and several mirrored hard drives, we guarantee maximum data security.

For increased security needs, we offer two-factor authentication, whereby each participant enters his/her mobile phone number after completing the survey, in order to access the survey results later using a code.

3. How is secure access to the dashboard provided?

The first way to access the dashboard is through the survey launch email. In this email, participants are informed about the survey and can access our app.joineer.com application with the personalised login link (via a button in the email). People who have not been entered in Excel will not receive a login link and without a link they will not be able to access the system. After entering the quantitative and qualitative responses, participants are redirected to the dashboard. If there is no survey in progress, participants are directed to the dashboard via the link in the automated results e-mail. If the participant has activated password protection, he/she will be directed to the login screen via the URL https://app.joineer.com/, where he/she can log in to the system with his/her e-mail address and password. After logging in, the participant is directed to the dashboard. Here too, all activities are protected by the encrypted connection of the secure hypertext transmission protocol.

If two-factor authentication is set up, access is only possible by double authentication via the mobile phone. As soon as the user wants to view the results or change a system setting, he/she will have to confirm his/her identity with a code sent by SMS.

3. Is sensitive data encrypted? (For both transfer and storage)

All Mongo DB data is stored in a premium ISO9001 and ISO27001 certified data centre in Switzerland, which is protected 24/7 by security personnel against unauthorised physical access and major outages. ISO/IEC 27001 is the most well-known standard for information security, which places high requirements on an Information Security Management System (ISMS). The Swiss data centre meets the requirements of FINMA-RS 08/7 and 18/3.

Ansible is used as a tool to ensure uniform configuration (firewall rules, disabling unnecessary services). The operating system is Ubuntu LTS (Long Term Support), which is particularly suitable for server-based use.

Each LTS version is supported for at least 5 years after its release (security updates). Management access to the physical machine is only possible from the specific management network (no exposure to the Internet). More information on this subject can be found in the documents ‘IT Architecture’ and ‘Data Protection policy’ of Joineer AG.

The data is secured during transfer via the secure hypertext transfer protocol. If necessary, we can transmit all data to the customer in encrypted form and provide the corresponding key. This does not include sensitive raw data which we are not allowed to decrypt due to the GDPR. It must not be possible to draw any conclusions from the answers of individual persons. For this data transfer, we can offer "one-time key" encryption and send you the key, for example by mobile phone/SMS.

5. Are the encryption keys also available to the client?

We do not provide keys to a client to access the server. As mentioned above, we can transmit all data in encrypted form if the customer requests it and provides the corresponding key. Sensitive raw data, which we are not allowed to decrypt due to the GDPR, is not included. It must not be possible to draw any conclusions from the answers of individual persons. For this data transfer, we can offer "one-time key" encryption and send you the key, for example by mobile phone/SMS.

6. Is there any technical documentation for your system solution?

Yes, you can find our technical documentation in the document ‘IT Architecture’.