Teammate360 Degree Feedback System – Data Security

Teammate360 takes the security of your information seriously. The following describes the measures we have in place to safeguard your data and the responsibilities that end users must ensure that their own security is maintained:

Physical Security

Teammate 360 is hosted on a dedicated enterprise level server at a European data centre (Nuremberg, Germany) operated by Hetzner Online. Details of the physical, electrical and electronic security measures can be found here:
https://www.hetzner.com/unternehmen/rechenzentrum

The entire data repository is backed up daily and are stored in a second storage box, escpecially tuned for backups – also in Europe. We do not store any data outside of the EU.

Access Control

Teammate360 does not have any general public facing access to its applications. The only access for users is via a logon which can only be activated via a verified email address.

Access to system administration functions is only available to our own staff on an “as necessary” basis.

We monitor industry best practice for web applications of this nature and endeavour to ensure that we always aim to comply with appropriate state of the art guidelines .

Completed reports can only be accessed by logging into the system and downloading – we do not send potentially confidential information out by email. Once a report has been downloaded it is the customer’s responsibility to keep it secure.

Questionnaires can only be accessed via an encoded and encrypted link in the invitation email they have been sent. Questionnaires cannot be accessed after the report has been generated without referring directly to our helpdesk.

We do not share email addresses or any other user information with any third party not directly involved in the operation and maintenance of the system.

We highly value your security and privacy, and to ensure it, we:

Maintain a firewall and virus-checking on all of our staff computers.

Our operating system is always up-to-date with the latest patches or security updates, which should cover vulnerabilities.

Only allow your staff access to the information they need to do their job and don't let them share passwords.

Encrypt any personal information held electronically that would cause damage or distress if it were lost or stolen.

Take regular back-ups of the information on your computer system and keep them in a separate location.

Securely remove all personal information before disposing of old computers.

Shred all your confidential paper waste.

Check the physical security of our premises.

Our staff is trained to be wary of common deception tricks.

It is mandatory to use a strong password.

We use spam filters to fight against email spam.

All data entered onto our system is on the understanding that it is confidential, and we will not divulge any such information to any person who did not enter it in the first place.

End User Responsibilities

We expect users to keep their usernames and passwords secure and to change them immediately if they suspect that they may have fallen into the wrong hands.

We expect users to provide correct email addresses to us and to ensure that any emails sent by us are not blocked by email gateways or spam filters.

We expect end users to be responsible for the security of their own email systems and mailboxes.

General Data Protection Regulation (GDPR)

We comply with the requirements of the General Data Protection Regulation (GDPR). More details can be found in our Data Processing Agreement.