

Two data centres for double security

think project! servers are hosted in two professionally-run data centres designed to the highest security standards. Both data centres are ISO/IEC 27001 certified.

The locations run in 'active-active' operation. In other words, parts of our service (instances) run in each of the data centres to spread the workload evenly. At the same time, each data centre serves as a standby for the other. Due to their identical infrastructure and hardware, as well as fully-mirrored data, either of the data centres can take on the tasks of the other within a few minutes. This means that continued operations can be ensured even in a worst-case scenario, such as the physical loss of one of the data centres.

Both locations are protected by multi-level access controls and are monitored around the clock. Fire doors, fire alarms and extinguishing equipment, and Uninterruptible Power Supply (UPS) systems ensure that our customers' data is absolutely secure.

- **High-performance Internet connection with high bandwidths**
- **Multiple-carrier redundancy**
- **Highly-available power supply via redundant connections to the power network**
- **Emergency power via UPS and diesel generators or fuel-cell power plant**
- **Three separate fire alarm systems**
- **Fire walls and doors**
- **Security personnel onsite 24 hours a day, 365 days a year**
- **Permanent video monitoring**
- **7-level access control system**
- **Continuous monitoring of temperature and air humidity**
- **Use of precision climate devices**
- **2-level air filtering**



We place maximum value on the availability, confidentiality and integrity of all customer data.

State-of-the-art equipment and seamless service

When selecting our contract partners for infrastructure and hardware, we opt exclusively for leading providers of market-tested solutions. We rely on Cisco for network and security, and on EMC² for storage. Our server hardware is provided by Fujitsu Technology Solutions.¹

The entire platform is tracked by monitoring systems around the clock. These systems check individual parameters within the platform as well as accessibility from outside. Depending on the criticality of identified events, a predefined alarm plan is activated. In order to remedy malfunctions as quickly as possible outside of standard business hours, our technical staff are available on-call around the clock.

Protection from third-party attacks

Our server farm is designed for maximum performance and security. We operate the latest multi-level security systems and have configured our platform to minimise the risk of attacks from third parties, including:

- Double firewall systems, comparable to a thick double wall
- Separation between the front and back ends of the platform, which means access from the outside is only possible via a single 'security door', with the area beyond completely sealed off.
- Physical separation of application servers and data servers, with applications running on one set of systems and customer data stored on another.

¹ All named brands and trademarks (protected by third parties where applicable) are subject, without limitation, to the provisions of the respectively applicable trademark law and the rights of ownership of the respective owners.

Protection from unauthorized access

Password-protected access

Only project team members personally invited by our customers or their representatives (for example, project administrators) can access a project. Project members' passwords are not stored with us. We only hold their 'digital fingerprint', making it practically impossible to track back to the original. This means that even our own employees do not know user passwords. Every user should, of course, keep their password safe to prevent unauthorized use.

Optional restriction of access by location

The think project! platform can be accessed from virtually anywhere via an Internet connection. However, we can also restrict usage to access from specific locations (such as your head office and site offices) if required, by specifying the relevant IP address or addresses.

Optional two-factor authentication

We use a solution from RSA Security, a worldwide leading provider of authentication technology for duplicate access protection. The SecureID token automatically generates and displays a new, six-digit combination of numbers every 60 seconds. Before they can access their account, users have to log in by entering a four-digit PIN number, followed by the six-digit pass code displayed by the token at that moment in time. This access method is known as 'two-factor security' – something you know (your PIN number) plus something you have (your token).

Measures for protection against computer viruses

Anti-virus software

Unfortunately, viruses and computer worms have become an everyday occurrence. We use reliable anti-virus software which is updated on a daily basis. As a result, new forms of computer viruses are identified immediately, minimising the risk of virus-infected files operating and spreading within think project!.



Safeguards against data loss

Hardware redundancy

Identical replacement configurations are available onsite for all servers. In addition, redundant adapters, network cards, hard disks, processors and other essential hardware components are stocked at the data centres for both our production and replacement servers.

Fully-redundant storage area network (SAN)

Our storage area network consists of a series of hard disks connected by glass fibre cable (fibre channel to disc). Around 50 terabytes of non-compressed data can be stored, with identical systems installed in each of our data centres. For added security, all data is also mirrored between the data centres, so that all customer data is saved twice.

External storage of back-up data

In addition to the mirroring of data within our mirrored storage area network, we also copy all data to external data storage media daily. Once a week, the collected media are taken and stored in a bank safe deposit box at a third location.

Secure data transfer

Encrypted communication

Unless specific measures are implemented, all data on the Internet is transmitted as plain text. This means that it is relatively easy to read, change or even delete while it is being transmitted from one computer to another. To prevent this, we use encryption procedures based on TLS (Transport Layer Security). This makes it nearly impossible to gain an unauthorized view of the data.

Two independent data centres for double security

Highly-available Internet connection and power supply

Monitoring 24/7

Encrypted data transfer

Fivefold data storage at three locations

The online project collaboration and document control system think project! is used in 40 countries by well-known clients, investors, project developers, project controllers, architecture and engineering firms, and construction companies – in more than 5,000 projects to date by over 90,000 users.

think project! simplifies cooperation in projects, provides seamless documentation and can be accessed directly via the Internet. think project! supports efficient project, information and risk management – saving time and reducing costs.

Representatives worldwide

www.thinkproject.com/network