thinkproject!

SECURITY CONCEPT

Measures to ensure the availability, confidentiality and integrity of your data

- Hosting from state-of-the-art, professionally run data centres
- High-performance equipment
- Seamless monitoring and 24/7 service
- Measures to protect against unauthorised access (password, optional two-factor authentication and/or IP restriction)
- Secure, encrypted data transfer
- Controls to protect from third-party attacks and malware
- Fully-redundant high-performance computers, storage area network (SAN) and essential components
- Multi-level back-up (mirrored data centres, mirrored main storage, mirrored back-up storage)
- Operations in conformity with German data protection law
- Certified software development, deployment and operations in conformity with the international information security standard ISO/IEC 27001:2013

HOSTING IN SECURE DATA CENTRES

The think project! cloud is operated in two separate ISO/IEC 27001 certified data centres. Both data centres run in 'active-active' operation. In other words, parts of our service run in each of the data centres to spread the workload evenly. At the same time, each data centre serves as a stand-by 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 continuous operation 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.

State-of-the-art, professionally run data centres

- Security personnel on-site 24 hours a day, 365 days a year
- 7-level access control system
- Permanent video monitoring
- Hosting in separate hardware cages, accessible only by authorised staff
- 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
- 3 separate fire alarm systems, firewalls and firedoors
- Continuous monitoring of temperature and air humidity
- Use of precision climate devices
- 2-level air filtering

State-of-the-art equipment

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

Seamless monitoring

The underlying server farm of the think project! cloud is designed for maximum performance and security. The server farm is seamlessly monitored by a comprehensive set of tools. These security tools check individual parameters within systems 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 – including during times falling outside of standard business hours – our technical staff is on-call around the clock, seven days a week.

COMPREHENSIVE SECURITY CONTROLS

Protection from unauthorised access

Password-protected access: Users require login credentials to access the think project! cloud. Furthermore, in order to gain access to a specific project they require allowance from the project owner (customer). Passwords are not stored in a readable way. We only record a 'digital fingerprint' of each password. This procedure makes it virtually impossible to track back to the original. This means that none of our employees even know what the user passwords are. Every user should, of course, keep their password safe to prevent unauthorised use.
Optional IP restriction: The think project! cloud can be accessed from virtually anywhere via an internet connection. If required, access can be restricted to specific company networks (e. g. your headquarters and your construction site office only). This is done by specifying the relevant IP address or addresses and blocking all others.
Optional two-factor authentication: We use a solution from RSA Security, a leading global provider of authentication technology, for two-factor access protection. Using this method, users must log in by entering a PIN of between four and eight digits, followed by a six-digit pass code displayed by a token at that point in time. The SecurID token automatically generates and displays a new six-digit number every 60 seconds.

Secure data transfer

Unless specific measures are implemented, all data on the internet is transmitted as plain text. This means that it is relatively easy to read, delete or even change data while it is being transmitted from one computer to another. In order to prevent this, we use encryption procedures which allow for the secure transfer of data. This makes it virtually impossible for the data to be exposed.

Protection from third-party attacks

We operate the latest multi-level security systems to protect us against the risk of third-party attacks. Our measures include:

- Double firewall systems, comparable to a thick double wall
- Separation between the front and back ends, 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

CONFORMITY WITH HIGHEST SECURITY STANDARDS

Controls to protect against malware

The spread of malware, i. e. from computer viruses, worms or trojans, is unfortunately a part of daily life. We have integrated dedicated software programs that are reliable in protecting against malware. These applications are automatically updated multiple times each day. Thus, new forms and mutations of malware are immediately detected. The processing and spread of a malware-containing file within think project! is therefore virtually impossible.

Safeguards against data loss

Redundant hardware: There are identical replacements available of the high-performance computers themselves, as well as other essential components, such as adapters, network cards, hard disks and processors.
Fully-redundant storage area network (SAN): Our SAN consists of a series of high-quality hard disks connected by glass fibre cable. There are identical SAN systems installed in each of our data centres. Around 350 terabytes of non-compressed data can be stored in each of them. For added security, all data is also mirrored between the data centres, such that all customer data is saved twice.
External storage of back-up data: In addition to the data back-up within our mirrored storage area networks, we also copy all data to external data storage media daily. Data is synchronised to a second location within the back-up system.

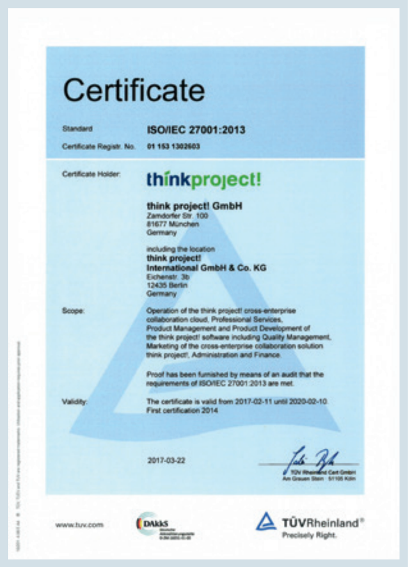
Operations in conformity with data protection law

think project! undertakes the collection, processing, storage and use of personal data based on commissioned data processing in accordance with the German Data Protection Act (§ 11 BDSG). Authority of organisation and information remains with the customer.

Our data centres are located and run in Germany. Data will be processed and stored within the territory of Germany. think project! employees are obliged to adhere to data protection according to the German Data Protection Act (§ 5 BDSG) and to maintain confidentiality of telecommunications according to the German Telemedia Act (§ 88 TMG). Key employees additionally possess a security clearance according to the German Review Safety Act (SÜG).

Operations and development in conformity with international information security standards

Our security standards for software development and software deployment are as high as for operations. Software updates are completed in continuous delivery on a monthly basis. These updates comprise corrections and new features. All updates are tested and approved by our quality team. Software tests are carried out by state-of-the-art test automation tools and are also conducted manually. Manual tests follow standard procedures to make sure that nothing falls through the cracks. Major changes, e.g. amendments of the user interface, are additionally tested on a so called staging platform on which selected customers, usually heavy users, put the new version through a final and thorough test. Only once these tests are passed successfully are updates deployed.



Certificate

Standard ISO/IEC 27001:2013

Certificate Registr. No. 01 153 1302603

Certificate Holder: thinkproject!

think project! GmbH
Zamdorfer Str. 100
81677 München
Germany

including the location
think project!
International GmbH & Co. KG
Eichenstr. 3b
12435 Berlin
Germany

Scope: Operation of the think project! cross-enterprise collaboration cloud, Professional Services, Product Management and Product Development of the think project! software including Quality Management, Marketing of the cross-enterprise collaboration solution think project!, Administration and Finance.

Proof has been furnished by means of an audit that the requirements of ISO/IEC 27001:2013 are met.

Validity: The certificate is valid from 2017-02-11 until 2020-02-10. First certification 2014

2017-03-22

TÜV Rheinland Cert GmbH
Am Grauen Stein · 51105 Köln

www.tuv.com

DAkkS

TÜVRheinland®
Precisely Right.

INTERNATIONAL INFORMATION SECURITY STANDARDS

Our business success, like that of our customers, is highly dependent on accessible information and efficient data processing. Ensuring the confidentiality, availability and integrity of data is a must. Information security is therefore an integral part of our corporate strategy. The Information Security Management System (ISMS) deployed by think project! covers all products, services and corporate processes, and is certified according to the international standard ISO/IEC 27001:2013.

TÜVRheinland®
ZERTIFIZIERT
Management
System
ISO 27001:2013
www.tuv.com
ID 0024070852

thinkproject!

50 countries

10,000 projects

› 150,000 users

About think project!

The global construction industry faces many challenges, such as pressure to deliver projects in time and on budget, as well as the increasing data volumes generated by an ever increasing number of parties involved on construction and engineering projects.

As a result, there is an emerging need for digital construction solutions such as think project! that facilitate cross-enterprise collaboration and overall information management.

think project! addresses today's digitalisation challenges in construction and engineering by providing state-of-the-art software solutions as well as industry expert consulting and services.

think project! – your partner for digital transformation

Representatives worldwide
www.thinkproject.com/contact-us