



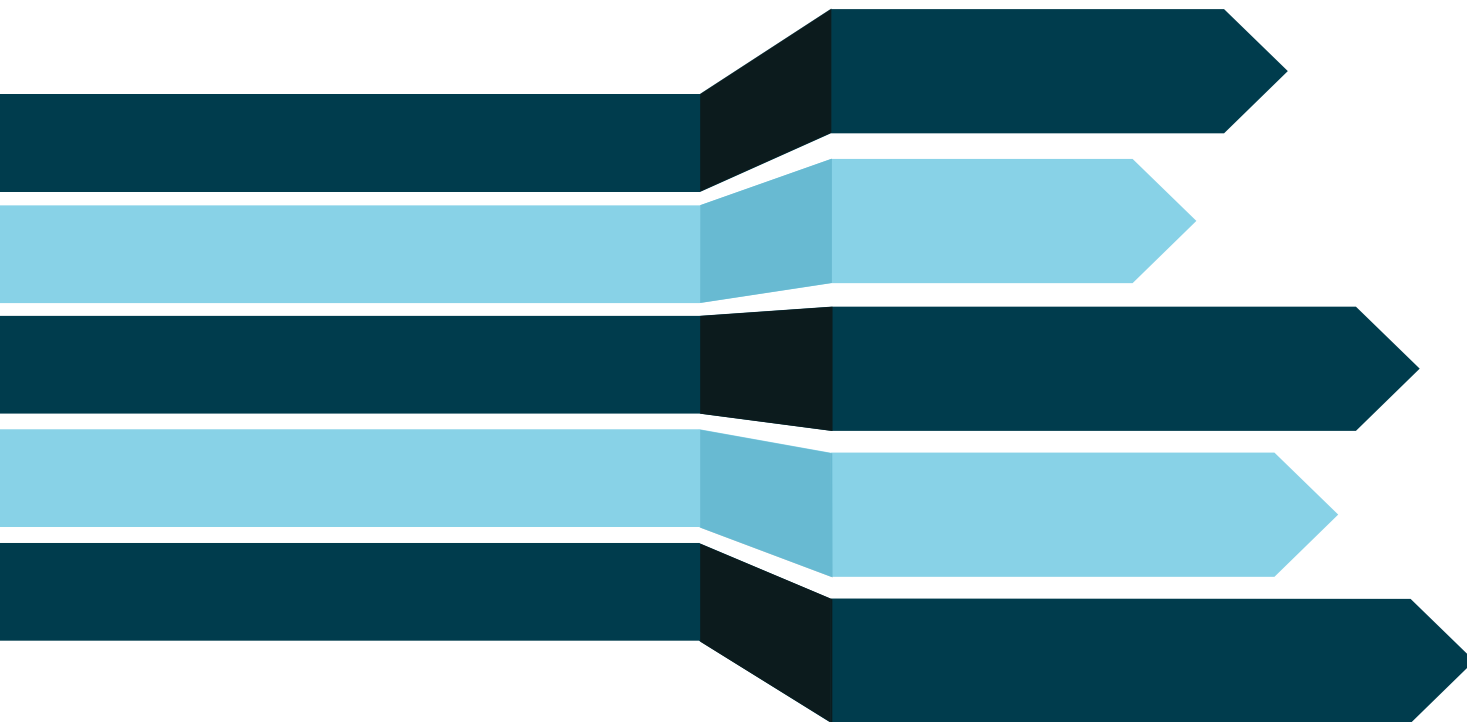
**thinkproject**

# How Thinkproject safeguards your data

Information security at its best



# Challenges



## With digitalization comes the risk for data breaches

Construction companies embracing digital transformation have found that they require multiple pieces of software such as BIM and CDE platforms to provide a complete digital construction experience. This software has to process a variety of sensitive information, from designs and 3D models to technical component data and specifications. This information is crucial for the success of any modern construction project, and, like any valuable asset, it must be protected to mitigate information risks like "unauthorized access, use, disclosure, disruption, modification, or destruction".<sup>1</sup>

A data breach could mean losing customers while at the same time posing a big risk of financial and reputational damage to the company -- along with higher-level risks associated with the disruption of sensitive projects, such as critical infrastructure, ultimately putting current and future revenue at risk.

While digital transformation is necessary for improving quality, saving time and reducing cost, it brings with it new information security challenges that requires the creation of a technical and organisational capability to control effectively.

<sup>1</sup> <https://csrc.nist.gov/glossary/term/infosec>

## The construction industry is particularly at risk

According to a study conducted by **Safetydetectives.com**, construction is the third most common vertical to be targeted by hackers—more than 13 percent of the total.<sup>2</sup> When it comes to critical infrastructure, Gartner stated that attacks on organizations in those sectors has increased 3900%, from less than 10 in 2013 to almost 400 in 2020.<sup>3</sup> Construction companies find themselves a target because the information they hold can be both particularly sensitive and it is often processed with a focus on minimising friction during the project's lifecycle, rather than data protection.

The transition to remote working and the increasing involvement of third parties add to these challenges, making information security as much about handling processes and policies as physical security.

**3900%**  
increase of cyber attacks  
on organisations in critical  
infrastructure since 2013

<sup>2</sup> <https://www.equipmentworld.com/business/article/15293568/6-ways-construction-companies-are-vulnerable-to-cyber-attacks>

<sup>3</sup> <https://www.gartner.com/en/articles/3-planning-assumptions-for-securing-cyber-physical-systems-of-critical-infrastructure>

## Not only requires commitment but also considerable investment

Information security requirements often filter up from customers and vary greatly. This places significant demands on companies, especially in sectors which have not traditionally been exposed to these challenges. To properly align with the needs of many asset owners requires investment in people & controls (in the form of processes and tools). This investment will vary depending upon the information handled; its risk profile and compliance / governance requirements. However, at the very least, a level of competency and technology are essential to a reliable information security strategy.

Also, information security is not a one-time effort. This commitment must be maintained to cope with the ever-evolving information security landscape, as cyber criminals continuously search for new ways to gain access to systems and extract information. Security professionals must stay vigilant, update security policies and measures, and adapt to new threats as they evolve.

All this comes with a considerable amount of efforts and cost and requires a company's full commitment to information security.

# About the solution



## Carefully select your software provider

To ensure that information is protected at the highest level, construction companies have to make information security an integral part of their overall digitalization strategy. That includes careful management of your supply chain; selecting the right software provider, one with the appropriate skills and certifications, that can significantly enhance assurance and minimise overhead.

## Information security is top priority for Thinkproject

At Thinkproject, we understand that our clients trust us with their most valuable assets – their data. Thinkproject has taken security to heart to ensure that we support our clients' efforts to secure their data while realising the benefits our class-leading tools. Thinkproject has invested heavily in dedicated information security resources and maintain an accredited Information Security Management System (ISMS).

We continually invest in modern security technologies, monitoring, incident management, infrastructure to support data sovereignty requirements, and ongoing employee training to ensure the security of your data across our systems.



## Key role of certifications by independent auditors in InfoSec




A great way to ensure that you are covering the information security bases is to build, maintain and certify an Information Security Management System (ISMS). An audit to the international ISO27001 standard is a great way to independently verify the suitability of your ISMS and demonstrates that the organisation has implemented a comprehensive framework to manage and protect its information assets.

The audit process also includes feedback and recommendations for improvement which provides actionable advice on how to continuously enhance security and develop a proactive security culture.

# Thinkproject's ISO27001 certification

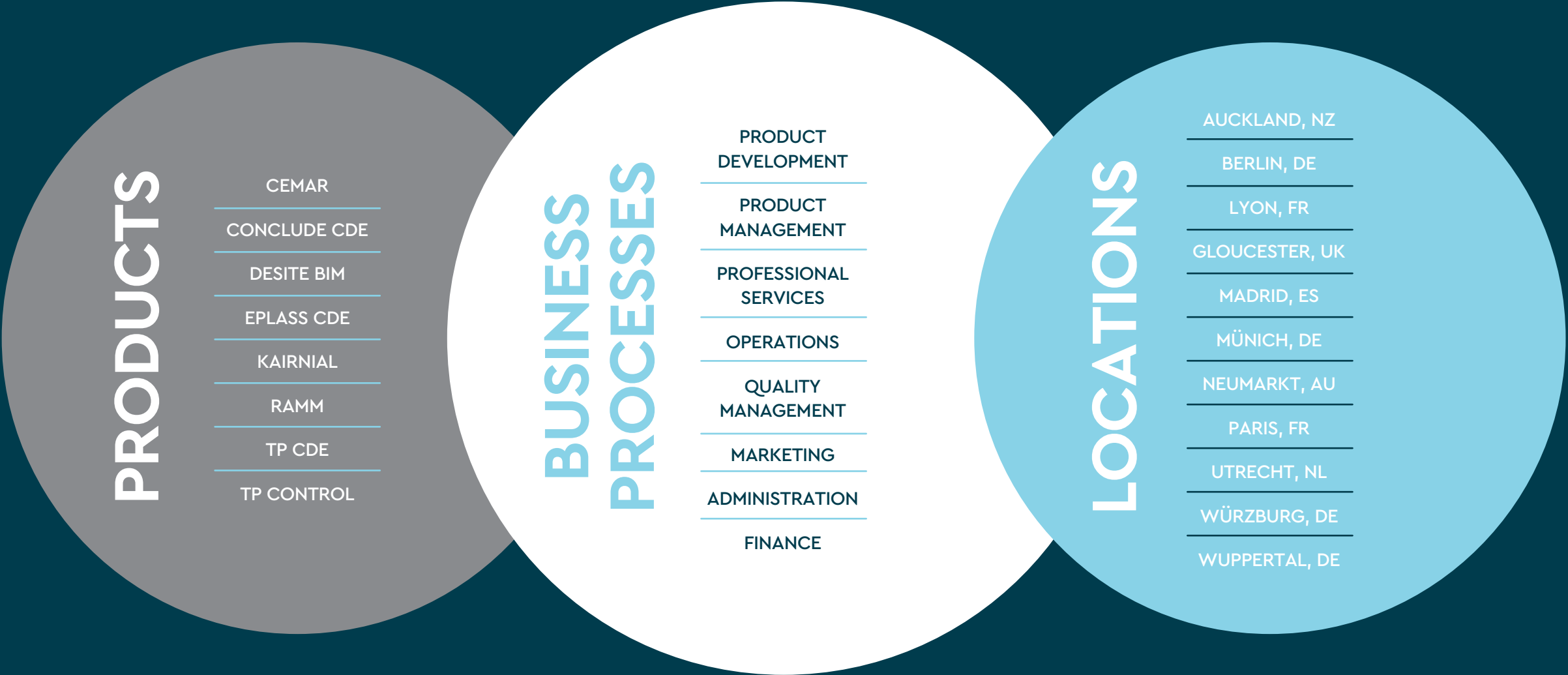
Thinkproject has implemented an ISMS that encompasses policies, processes and controls, and we have been certified to the ISO27001 standard for more than 10 years. So, we are well positioned to safeguard your data and prevent sensitive information in the case of a malicious attack. Thinkproject's ISO27001 certification spans across its corporate processes, product management, product development, professional services, and operations. Furthermore, all employees are regularly trained and tested in information security as well as our policies and processes.

This is a huge commitment and, on top of the effort our staff put in on a daily basis, it relies on our dedicated in-house compliance team to manage the required, recurring internal and external audits. Our centralized processes ensure group-wide standards for information security so that all subsidiaries operate to the same high standard. Overall, information security is a top priority for Thinkproject and we are fostering a security-conscious culture throughout the entire organization.



**Thinkproject's ISO27001  
certification spans across its  
corporate processes, product  
management, product  
development, professional  
services, and operations.**

# Overview of Thinkproject ISO 27001 certifications



AT A GLANCE

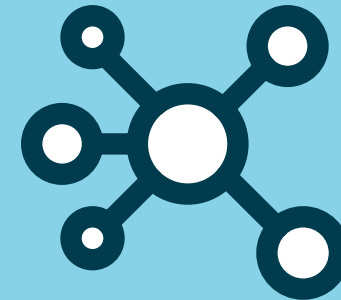
# Highlights



Protecting customer's data is a top priority of Thinkproject with robust policies, controls and processes



Thinkproject continually passes one of the highest information security standards of certification with ISO27001



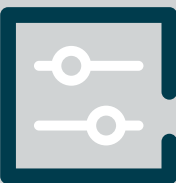
Thinkproject's ISO27001 certification spans across all its processes



Thinkproject's ISMS is regularly audited and up to date



# Information security best practises @ Thinkproject



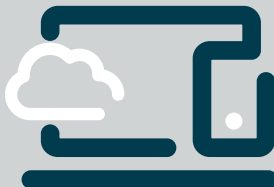
## Access Control

Thinkproject offer flexible access control to our systems. We support industry standard single sign-on connections to common identity providers, as well as supporting multi-factor authentication.



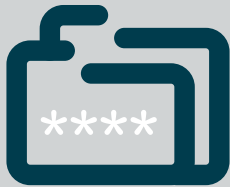
## Compliance

Thinkproject maintains ISO27001 certification by undergoing regular external and internal auditing. Additionally, Thinkproject acquires specific information and cyber security certifications tailored to the regions in which it operates.



## Data Backup & Disaster Recovery

Thinkproject ensure that your data is stored securely with reliable & tested backup and disaster recovery processes. Where our service is hosted with a public cloud provider, multiple copies of your data are stored within the same region to maximise service availability. These processes are audited as part of our ISO27001 accreditation.



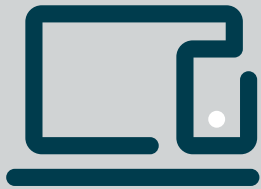
## Data Encryption

Data is encrypted to ensure that it cannot be intercepted by an unauthorised 3rd party. Our ISMS defines standards for encryption and key management, as well as secure storage of data.



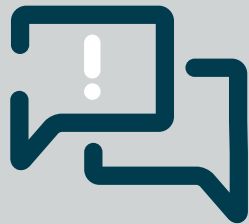
## Employee Training & Awareness

Thinkproject makes it a requirement for all employees to undergo annual mandatory training covering various topics, such as cyber security and data protection. Additionally, each employee must attest to all policies as part of the compliance process.



### Endpoint Protection

Thinkproject uses a variety of tools and policies to ensure a secure desktop and server environment. We use a combination of web content filtering, secure VPN, application control, automated & manual patching, MDM, EDR and virus protection tools to provide broad protection for our assets.



### Incident Response Plan

Thinkproject has a well-established Incident Management Procedure that undergoes regular testing and evaluation to ensure it enables swift responses to any incidents that may arise. We also offer comprehensive training to employees on how to report incidents effectively through our whistleblower portal and the OneTrust platform.



### Operational Security

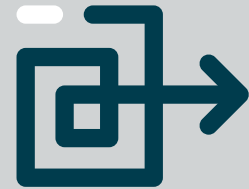
The secure operation of our offices, data centres and cloud environments are audited as part of our ISO27001 accreditation. We ensure that we implement appropriate controls to minimise operational risk and ensure the security of data. These include:

- Network segmentation through firewalling
- Intrusion detection & prevention systems
- System hardening & attack surface reduction
- Regular penetration tests
- DDoS protection
- Logging / Monitoring of relevant log data and more



### Physical Security Measures

Thinkproject offices are equipped with door control systems, ensuring secure entry, with robust sign in and out processes for visitors. Additionally, we implement CCTV security monitoring as an added layer of protection. To promote environmental sustainability and enhance data security, we maintain a paperless office policy.



### Privacy and Data Protection

Ensuring GDPR compliance for Thinkproject companies and their products is our utmost priority. Regular data protection audits are integral to our Data Protection Management System, and we enforce mandatory annual GDPR training for all employees. We strictly adhere to our comprehensive groupwide Data Protection Policies.



Security  
Incident History

Any incidents are tracked with the OneTrust tool.

For every incident, root cause analysis and lessons learned are implemented according to our Incident Management Procedure.



Secure Development  
Practises

Thinkproject operates a modern DevOps structure, adhering to CI/CD (Continuous Integration/Continuous Deployment) principles to achieve consistent deployments. Throughout the development process, we align with industry standards such as OWASP (Open Worldwide Application Security Project) and utilize tools to identify vulnerabilities and detect coding errors, ensuring that robust and secure software is deployed.



Service Level  
Agreements

All Thinkproject products have SLAs that can be provided on request.



Third-party Risk

We have a Supplier Management Process that adheres to our ISMS requirements. This includes review of any external suppliers with our compliance team, NDAs, GDPR checks and other measures to ensure compliance with our standards.

Our third-party vendors are regularly assessed to ensure they remain compliant.



Vulnerability Management  
& Software Updates

Thinkproject maintains systems which monitor our infrastructure for vulnerabilities and missing patches, and we regularly update, patch and test our software to keep the risk of compromise as low as possible.





**Dr. Ralf Hundhammer,**  
**Chief Technology Officer**  
**at Thinkproject**

“ For us, certification according to ISO/IEC 27001 is simply a necessity. In an increasingly digitized economy, information security becomes a decisive factor. This also applies to software providers and users in the construction industry. Especially when companies use their software in a SaaS model, i.e., do not manage the operation themselves, they must be able to rely on the security measures of the provider. That is why we already underwent our first ISO 27001 certification ten years ago. Since then, we have been constantly expanding the scope of certification. ”

# thinkproject

Thinkproject is Europe's leading SaaS provider for Common Data Environment, Asset, BIM and Field Management, and Project Controlling. Thinkproject has been digitising construction companies, builders, project managers and planners for more than 20 years with powerful, flexible technology in combination with consulting expertise from knowledge of complex large-scale projects.

With 650+ employees worldwide, Thinkproject offers digital solutions that cover the entire life cycle of a construction project.

[Thinkproject.com](https://thinkproject.com)

# 75,000

PROJECTS

# 3,250

CUSTOMERS

# 300,000

USERS

# 60

COUNTRIES

# 650<sup>+</sup>

CUSTOMER-ORIENTED  
EMPLOYEES

# 23

OFFICES