Data Protection

Understanding the Topic

The volume of data collected, stored and managed by companies increases every year, as technology reaches further into all parts of our lives. In the real estate sector, data-driven innovations have become central to the way companies design, lease and manage properties, and the transformation of workplaces by remote working has taken businesses from every sector online.

For all companies, this raises the challenge of data security. All the data we handle on behalf of our tenants, employees and wider stakeholders comes with a duty to protect that data from misuse. Moreover, in many cases this duty is underlined by a legal obligation to implement adequate standards of data protection.

We therefore take the trust placed in us by our stakeholders to protect the confidentiality of their data very seriously. As such, we strive for best-in-class data protection policies and procedures, in line with the evolution of digital technology, work processes and legal frameworks.

Managing the Topic

We have developed our Information Security and Privacy Strategy to protect the confidentiality, integrity and availability of GCP's data across all business processes. Our strategy and management framework is spearheaded by our in-house information security experts, and overseen by the Information Security Steering Committee. The Committee is led by the Chief Compliance Officer (who is a member of the Board) and includes the Chief Information Officer, Chief Information Security Officer, Chief Capital Markets Officer and the Head of HR, to ensure that information security risk management is embedded into all processes, technology and people-focused functions. The Committee also consults with non-members, such as external specialists and relevant business managers like the COO. To reflect data security considerations in our top-level risk management systems, our in-house cybersecurity leads sit on our board-level Risk Committee.

Our continuous efforts to improve this strategy were rewarded in 2021 with our achievement of the ISO 27001 certification for our Information Security Management System (ISMS). We were the first of our near peers to achieve this certification for our leading edge ISMS, which has been embedded across the Group's business divisions. Accordingly, a key goal in 2022 was to maintain this ISO 27001 certification, and validate the integration of the system. The surveillance audit to renew the certification took place in December, and was passed with no issues for correction raised. The certification only applies to our head office, but our local German offices fall under the same implementation scope, and apply all relevant policies and procedures. For operational reasons, all digital information flows through Berlin, making this the most material location to focus our certification effects.

Compliance with the ISO 27001 standard encompasses a risk-based approach to the identification, assessment, management and monitoring of information security risks, covering business critical IT systems, employees and partners who have access to GCP's hardware and IT systems. The framework defines the appropriate Information Security tools and processes in the event of a potential system vulnerability according to an ISO 27001 based Risk Management Lifecycle model: risks are identified and categorized based on business impact and likelihood, and appropriate tools and remedial measures are identified to mitigate the risk, which are then subject to testing prior to rollout.

Ongoing monitoring is used to evaluate the residual risk factor. We use a carefully selected set of KPIs and Key Risk Indicators (KRIs) to continuously self-assess our performance against predefined target values and assess the company's risk and maturity level across internal and external procedures. These indicators are reviewed by Internal Audit, the Information Security Steering Committee, and an additional external audit to actively engage in continual improvement.

Risk Monitoring

As part of our proactive approach to risk identification, in 2022 we conducted internal risk audits in the Netherlands, London and our regional offices. These were designed to

compare the effectiveness of measures at these offices to the implementation at our HQ, to ensure that application of our procedures is unified across our business locations. The results demonstrated good levels of compliance across the organisation, and opportunities to improve practice at these sites further were identified. A new team member joined our data protection team in 2022, increasing our resources and expertise for such data protection audits. Our goal is to continue to conduct more audits, to pinpoint weaknesses before they can become threats. We will also be increasing the frequency of our third-party cyberattack simulations to being conducted quarterly, rather than semi-annually.

Real-time, 24/7 monitoring of potential IT vulnerabilities is provided by a third party, whose security analysts work closely with our incident response teams to investigate each event and determine the appropriate response. This ensures that risks are identified early, and recovery times are kept to a minimum, significantly reducing costs and lost productivity.

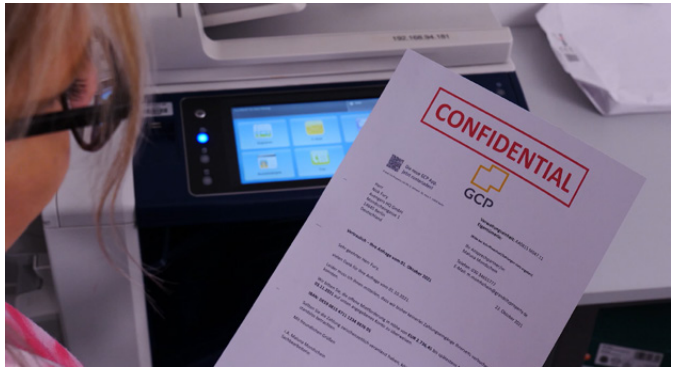
To test the effectiveness of our security and monitoring procedures, in 2022 we commissioned an external party to conduct eight simulated attack drills. We use these drills to assess the effectiveness of both our digital and human procedures, and look for ways to improve our readiness for such cybersecurity events.

Data Protection

Underlying our information security procedures are sophisticated digital systems to protect the data we store against vulnerability or loss. In 2022 we upgraded our main firewall to a new system, which provides us with unique capabilities to support the company's digital resilience. It will allow us to improve our redundancy in case our main data centre is down, detect sophisticated network threats better, connect to multiple tenants from the same computer, and more.

Another key channel of risk to our systems and networks is via mobile devices. In light of the move to remote working, spurred by the pandemic, we have introduced new controls to ensure that all external connections are secure. BeyondTrust is used as our security layer for external IT service providers which enforces MFA, session recording, least privileges and requires approval before each session. For our external business service providers, we have implemented DUO, which checks the compliance of the operating systems that connect to ensure that they are well protected with a recent operating system, a malware solution and encryption. External service providers can only connect if all these standards are fulfilled.

To ensure adequate security in our processes for saving and sharing information, all documents are labelled with an information security classification, from Public to Restricted, which requires password protection for the document. In 2022 as part of our ongoing Data Loss Prevention Project, we analysed all data on its keywords and attributes to create a system to automatically attribute this security label in the footer of all documents. This considerably streamlines the workload of these security procedure, allowing for standardised information control across the organisation.



Employee Training

To embed our data protection system across the Company, we place great importance on training and awareness for our staff. All our employees are required to complete video-based training modules on data protection, and staff in management positions receive further input through seminars with subject matter experts. Our training courses are regularly developed to keep the content provided up-to-date. A new course on the GDPR was launched on our e-learning platform CREA (the Contemporary Real Estate Academy) in October 2022, after extensive consideration of tens of available modules. CREA also offers Information Security training modules for temporary employees and business partners with access to GCP's IT systems. All personnel are required to sign a company statement of their commitment to data protection.

Beyond initial training on our data protection procedures, we emphasise continued learning and awareness efforts. GCP's Company Standard Operating Procedures (SOPs) set out expected courses of action for day-to-day activities, such as saving and storing information or handling requests for data. Permanent employees must complete mandatory refresher trainings every 18 months, to reinforce their knowledge of these procedures and awareness of data protection risks. We issue regular internal campaigns and communications emphasizing alertness to phishing and malware attacks. We strongly believe in taking a personalized approach to promoting awareness of information security, to make our initiatives more relatable and resonant with employees' experiences. We produce educational videos featuring employees of the Company, such as a new awareness video on the importance of data protection at work which was produced in 2022, which support our standard e-learning modules to make training more engaging and informative.

Performance

To guide the implementation of our sustainability strategy and track our progress, we have developed several long-term goals that we are continuing to work towards:

- Confidentiality: encryption wherever data is stored or accessed
- Integrity: establishing procedures to prohibit unauthorized personnel to alter information
- Availability: designing systems to minimize downtime
- Security: securing business information pertaining to company operations
- PII: enforcing the security and confidentiality of processed personal information
- Regulations: satisfying regulatory (such as GDPR) and other information security requirements
- Awareness: training employees on how to identify threats and act according to company guidelines
- Resilience: protecting our systems and networks as well as the data contained therein from malicious activities
- Information Assets: ensuring that all networks, systems and applications comply with confidentiality, integrity and availability

To achieve our long-term goals, we will:

- Conduct further technical crises training and simulations to enhance our ability to respond to cybersecurity events
- Work with an external partner to improve our data loss prevention strategy
- Carry out additional audits on our ISMS to ensure that it conforms to all relevant criteria
- Deploy advanced security technologies
- Introduce a digital "Welcome Day" to provide assistance and guidance to new employees
- Maintenance of ISO 27001 certification: surveillance audit, office audits to assess effectiveness of measures, general description of the ISO standard requirements, governance within AT.

There are several key figures we track each quarter to monitor our performance and contribute to our long-term goals:

1

NUMBER OF REPORTABLE DATA PROTECTION BREACH INSTANCES

(2021: 2)

0

ISO 27001: NUMBER OF MAJOR NON-CONFORMITIES

(2021: 4)

6

ISO 27001: NUMBER OF MINOR NON-CONFORMITIES

(2021: -)

90

% OF CYBER AND GDPR TRAINING COMPLETION RATE

(2021: 90)

We monitor potential security incidents and data protection breaches (defined as the misuse or corruption of personal data) as an indicator of the effectiveness of our operating procedures. In 2022, no such confirmed breaches resulting in a serious incident, sanction or fine were reported. In the event of any confirmed incident, a committee is formed to immediately investigate the matter and recommend remedial actions to prevent a similar occurrence.

Non-conformities are issues which can be raised in the course of audits for our ISO 27001 certification. A minor non-conformity is an observation as to how compliance to the standard could be improved, which does not have any material consequences to the business. A major non-conformity is a violation of the ISO standard sufficient to prevent the company from being certified as ISO 27001 compliant.

Priorities for 2023

We continually aspire to improve our ISMS and maintain our ISO 27001 certification. We will keep up our awareness raising efforts through new initiatives and campaigns. A particular focus will be the integration of our Data Loss Prevention Project with our existing information control processes. We also intend to conduct a greater number of simulated attacks and penetration tests, against a greater variety of systems, to further strengthen our security processes.