GRAND CITY
Properties S.A.

DATA PROTECTION

PART 1 – UNDERSTANDING THE ISSUE

Rapid advances in technology are transforming all aspects of day-to-day life, including the ways in which people work, study, travel, shop, communicate and socialise. In the property sector, technological innovation is already changing how buildings are constructed or redeveloped, leased, sold, and managed. And more widely, the rate at which companies are collecting, storing, and managing data is rising exponentially.

This brings new challenges for companies across all sectors. The data we collect, process and store must be managed in a secure way, and we have a duty to our tenants, not just a legal obligation, to protect their personal data from misuse. Failure to do so carries significant legal and reputational risks from the threat of sanctions and fines for non-compliance with regulations such as the EU's GDPR legislation.

The protection of individual privacy is therefore an area of key importance to our stakeholders. We aim to ensure that all personal data collected and stored during our operations is protected from manipulation. As such, we strive for the best-in-class information security management system and data protection policies and procedures in line with the evolution of digital technology, work processes and legal frameworks.

PART 2 – MANAGING THE ISSUE

Management Approach

We have adopted an Information Security and Privacy Strategy to protect the confidentiality, integrity and availability of GCP's data across all business process, information gathering, storing and transmitting facilities and systems. As well as ensuring the continual improvement of controls, the strategy lays out our management framework relating to data safety and privacy commitments, including security threat monitoring, creating a security positive culture, and adherence with legal, regulatory and audit requirements.

Significantly, we took a major step forward in 2021 by achieving ISO 27001 certification for our information security management framework which adopts 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 hardware and IT systems.

The framework defines the appropriate IT security tools and processes in the event of a potential system vulnerability based on the NIST [1] Risk Management Lifecycle model: risks are identified and categorised based on business impact and severity, appropriate tools and remedial measures are identified to mitigate the risk, which are then subjected to testing prior to rollout. Ongoing monitoring is used to evaluate the residual risk factor.

The framework is aligned to our enterprise resource planning software and is supported by standard operating procedures and policies governing the use of, and access to, GCP IT systems and hardware. For example, our Patch Management Policy defines the requirements for maintaining up-to-date operating system security patches on all owned and managed workstations and servers to reduce potential IT vulnerabilities. This includes systems that contain company or customer data regardless of location. Compliance with the policy and related procedures falls under the responsibility of both the Chief Information Security Officer and the Chief Information Officer.

Our strategy and management framework are overseen by the Information Security Steering Committee who are also responsible for investigating any possible security breach. 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, and the Head of Legal, thereby ensuring information security risk management is embedded into all company process, technology and people-focussed functions. The Committee will also consult non-members such as the Head of Human Resources when required.

We use a mixture of qualitative and quantitative key performance indicators to measure our performance and assess the company's risk and maturity level across five pillars defined by the NIST Cybersecurity Framework scorecard: Identify, Protect, Detect, Respond and Recover. The framework enables us to prioritise actions based on risk-level, business need and resources. We use a scorecard to self-assess our performance against the framework and this undergoes a review by Internal Audit, the Head of the Information Steering Committee, and is subject to an additional external audit before being presented to the management committee and Board for review.

Data protection

Data protection standards and processes are fully integrated into our Information Security framework, and all departments receive guidance on the specific data protection risks and management measures that must be taken in relation to their day-to-day work.

We treat stakeholders' high expectations in this area with due consideration. We ensure that our Data Privacy Policy is available to tenants and business partners, along with information about our data processing systems; the purposes for which their data is used, and their related rights in compliance with the EU General Data Protection Regulation (GDPR). This includes the transparent handling of personal data; offering individuals a choice in how their data is processed and assessing the effectiveness of different IT-based data protection methods. Where appropriate, onsite notifications have been installed, for instance where video security systems are in use. The Data Privacy Policy also forms a component of all offers to prospective tenants.

Employee training

All staff follow video-based training units, and staff in management positions receive further input through seminars with legal experts. Our Standard Operating Procedures (SOPs) make expected courses of action in day-to-day activities clear to all parties, from saving and storing data to handling requests for information. Though not stipulated by law, we require all personnel to sign a company statement of their explicit commitment to data protection.

Our e-learning platform offers IT security training modules that are compulsory for permanent employees, as well as temporary employees and business partners who have access to GCP applications and IT systems. All staff receive training on information security and the GDPR, and this is tracked through our framework scorecard.

E-learning is supplemented by regular campaigns and communications that emphasise the need to remain

[1] National Institute of Standards and Technology

resilient and alert to potential phishing and malware attacks, and we offer a reward program for employees who identify and alert us to the most potential threats. We also provide monthly 'how to' tips that aim to reinforce security conscious behaviour at home, such as safe browsing and shopping techniques, on the premise that employees who protect their personal life are more likely to protect their work life. We also promote security awareness through a cyber magazine and animated educational videos that support our standard e-leaning modules, with the aim of making training more engaging and interactive.

PART 3 – PERFORMANCE

Long-term Goals and 2020 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:

- Ensure that all personal data stored and/or processed in the course of the Group's operations is protected from manipulation and misuse
- Maintain zero tolerance towards compliance violations

We use two key performance indicators that we track on a yearly basis to monitor our performance.

0
Compliance violations
(2019: 0)

0
Instances of data protection breach
(2019: 0)

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 2020, 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.

2020 target	Status	Progress
Ensure that all personal data stored and/or processed in the course of the Group's operations is protected from manipulation and misuse	Achieved	No confirmed incidents of data protection breaches were recorded, confirming the robustness of our Information Security Management System and Policy

Significant activities

Supporting our response to COVID-19

As COVID-19 spread, we found our Information Security systems sufficiently prepared to handle the almost overnight switch to homeworking. We had invested significantly in our network capability and VPN connectivity following a risk planning and preparedness assessment in 2018 which modelled various scenarios if access to our headquarters was restricted. Thanks to this exercise, we were able to ensure that employees who needed to work from home could do so safely without having to introduce significant changes to our operating procedures.

As part of our planning, we had already introduced measures including URL filtering, secure browsing, and end point protection for employees working remotely. Similar measures were put in place for our suppliers and business partners; we introduced security gates and checked that minimum requirements such as passwords and up-to-date antivirus software was installed as a prerequisite to connect to our applications.

In preparation for our ISO 27001 certification, we had also concluded a review of our information security and data protection policies, and we took the opportunity to re-issue the Group's acceptable use policy and 'bring your own device' procedures. The former governs our procedures and minimum standards for accessing and handling data, particularly information that is confidential and/or restricted. Our 'bring your own device' procedures govern the segregation of GCP data and applications on personal devices such as laptops and phones, enabling employees without company hardware to work effectively and securely.

Priorities for 2021

To contribute to these long-term goals and direct our efforts in 2021, we will continue to follow our risk-based approach to the identification, assessment, management, and monitoring of information security risks. Given the company's transition to a new SAP-based enterprise resource planning software, and the likely continuation of remote working for the short term at least, this will focus on continuing to ensure robust data loss prevention, threat reduction and recovery procedures, network access control and mobile device management policies. Secondly, we will also continue to build our management team's capacity by conducting technical crisis training and simulations.