DATA PROTECTION

1. UNDERSTANDING THE TOPIC

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 socialize. 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 General Data Protection Regulation (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 data protection policies and procedures in line with the evolution of digital technology, work processes and legal frameworks.

2. MANAGING THE TOPIC

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

Following the work commenced in 2020, in 2021 we were proud to achieve the ISO 27001 certification for our information security management system (ISMS), covering the Aroundtown headquarters in Berlin. We are the first amongst our near peers in the real estate industry to achieve this certification and feedback from our auditor suggests that our ISMS is advanced compared to other companies of our size. We appointed additional resources and dedicated time to reviewing our policies, conducting audits, introducing enhanced cybersecurity measures, and generating greater awareness across the business to ensure that our systems were compliant with this robust standard. Consequently, we have stronger, rigorously documented procedures in place and a more integral approach to data protection that is streamlined across the Group's different business divisions under the umbrella of our Group risk management framework. We have also established a data protection forum to unify policies and protocols between the four Group companies. Whilst it is important for us to maintain separate data protection teams between the companies, the use of common procedures and tactics enables us to increase efficiencies and benefit from shared know-how.

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 Aroundtown'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.

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, Aroundtown's 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 their location. Compliance with the policy and related procedures falls under the responsibility of both the Chief Information Security Officer, the Chief Information Officer and Chief Technology Officer with support from the recently established Cyber Security Assurance team.

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. It ensures that risks are identified early, and recovery times are kept to a minimum, significantly reducing costs and lost productivity. Our strategy and management framework are overseen by the Information Security Steering Committee, who is also updated about any possible security breaches. 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, Head of HR and the Head of Legal, thereby ensuring that information security risk management is embedded into all processes, technology and people-focused functions. The Committee will also consult with non-members such as relevant business managers such as the COO and external specialists.

We use a mixture of qualitative and quantitative key performance indicators (KPIs), as well as key risk indicators (KRIs) to measure our performance and assess the company's risk and maturity level across internal and external procedures. The underlying framework is based on the ISO 27001 norm to ensure conformity with this international standard and to pursue compliance with information security management best practice. We use a carefully selected set of KPIs and KRIs to continuously self-assess our performance against predefined target values, which undergo a review by Internal Audit, the Information Security Steering Committee, and is subject to an additional external audit to actively engage in continual improvement.

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 into consideration in their day-to-day work. We treat stakeholders' high expectations in this area with due diligence. 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's 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

Employees follow mandatory video-based training units, and staff in management positions receive further input through seminars with subject matter 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 Information Security training modules for temporary employees and business partners who have access to Aroundtown's applications and IT systems, and permanent employees must complete the mandatory trainings every 18 months. All staff receive training on information security and the GDPR, which is tracked through our KPI framework. E-learning is supplemented by regular campaigns and communications that emphasize the need to remain 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 behavior at home, such as safe browsing and shopping techniques, on the premise that employees who protect their personal data are more likely to protect the company's data. We also promote security awareness through animated educational videos that support our standard e-leaning modules, with the aim of making training more engaging and interactive.

3. PERFORMANCE

Long-term Goals and 2021 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

There are several key figures which we track on a quarterly basis to monitor our performance and contribute to our long- term goals:

0

COMPLIANCE VIOLATIONS
(2020: 0)
TARGET VALUE: 0

0

INSTANCES OF DATA PROTECTION BREACH
(2020: 0)
TARGET VALUE: 0

90%

CYBER AND GDPR COMPLETION RATE
(2020: 90%)
TARGET VALUE: < 90%

4

NUMBER OF NON-CONFORMITIES
(2020: 4)
TARGET VALUE: < 12[1]

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 2021, 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.

[1] Whenever non-conformities are identified through internal or external audits, immediate remediation is initiated.

Significant Activities

Strengthening existing procedures

In 2021, we introduced several new cybersecurity awareness measures and significantly improved existing procedures. Among these changes was the use of gamification to enhance the impact of the Group's phishing prevention campaign and the production of a compelling video, developed in-house and featuring well-known Aroundtown employees, to educate staff about physical security risks in a more engaging and memorable format.

We also conduct technical crisis training and simulations to confirm the strength of our procedures in practice and analyze and improve our preparedness in the event of a cybersecurity attack. In 2021, we conducted a simulated ransomware attack with impressive results: the attack was identified after just one hour - compared to an average identification time of 207 days - and with all IT and information security procedures smoothly executed, the total recovery time was just 6.5 hours. We are now in the process of preparing another type of simulation to be carried out in 2022.

Priorities for 2022

We continually aspire to improve our ISMS, maintain our ISO 27001 certification, and keep up our awareness raising efforts. In 2022, we will continue to issue more frequent and compelling email updates on cybersecurity and data protection to engage our employees and we will assign additional resources to conduct a higher number of audits so that we can pinpoint any weaknesses in our processes before they become threats. Building on the additional security measures deployed in the context of the pandemic-led move to remote working, we will introduce new controls to protect data and information on mobile devices and we will work with external advisors to review and enhance our data loss prevention strategy more widely. We have also established a data protection forum to unify policies and protocols across the group. Whilst it is important for us to maintain separate data protection teams between the companies, the use of common procedures and tactics enables us to increase efficiencies and benefit from shared know-how.

Berlin