

Data protection (GRI 418)

Taking responsibility for data is more than data protection. AURELIUS has established a data governance approach that covers not only legal but also cultural and organisational aspects. The aim is to handle data responsibly in the interests of all stakeholders. The company is committed to following and implementing the data protection standards relevant to the company.

The respective data protection officers in the Group carry out the legally required tasks for compliance with data protection regulations. In doing so, the respective applicable data protection regulations are considered. Internal guidelines and the General Data Protection Regulation limit and regulate the collection, use, storage and disclosure of personal data in the interest of data subjects. Data is only used and stored for the purpose stated to data subjects.

In the event of changes to the company's data protection guideline or if unauthorised use of their data is identified, the individuals or organisations concerned will be informed immediately. All notifications and complaints about possible violations are reviewed, processed, and documented. In 2021, there were no complaints about possible data breaches.

Ensuring data security for all corporate data and processes and respecting and protecting the privacy of employees and all stakeholders is a top priority for AURELIUS. The security of corporate data and the trust of employees and stakeholders are crucial to the success of the company.

When deploying and using IT equipment, the aim is to ensure confidentiality and data protection is in place for all natural and legal persons who have a business relationship with AURELIUS as well as to safeguard the corporate interests and ensure compliance with legal, contractual and professional regulations.

This applies to all temporary and permanent employees of the AURELIUS Group, regardless of location, as well as to all employees working under consulting or service contracts. AURELIUS is supported in this by an external service provider.

Data is a sensitive asset worthy of protection and is subject to strict legal requirements. The data protection sphere has seen a significant increase in regulatory requirements in recent years. For example, the European Union's General Data Protection Regulation (GDPR) has defined additional obligations for companies in dealing with personal data. Simultaneously, public awareness of the issue has also increased. In the current environment, responsible handling of data has become a decisive competitive factor.

Personal data is treated confidentially by AURELIUS as a matter of principle. We comply with the protection of this data in accordance with the applicable legal requirements.

Data security and cyber security

Data security in the Group and the prevention of unauthorised external access to company and customer data (cybersecurity) are increasingly becoming a focus. AURELIUS works continuously on the security of our digital technologies and systems in order to address cyber risks as best as possible and avert damage to our stakeholders and our Group.

The aim of reviews is to identify vulnerabilities and points of attack, but also to review the effectiveness of protective measures that have already been implemented. For AURELIUS, increasing the resilience of its IT infrastructure is an important topic in 2022.