Other significant Governance topics

Cybersecurity

Possible breaches in the security of networks, information systems and operational systems, threaten the integrity of the Company's data and other sensitive information, and disrupt business operations. The occurrence of such events could negatively impact the Company's reputation and its competitive position. Moreover, the Company's possible involvement in litigations with third parties, the award of damages, the imposition of fines or the loss of business (including remediation costs), could have a significant negative impact on its financial situation and operating results. In addition, the management of cybersecurity attacks or breaches may require considerable Management involvement and significant resources.

MYTILINEOS has developed an **Information Security Framework** and is committed to the implementation of a **holistic Information Security Management System,** through which the effective and efficient protection of the Company's information systems and data is achieved.

The Information Security Framework sets out a continuous cycle of improvements in the Information Security Management System, specifying activities for assessing risk, developing and implementing information security policies and cybersecurity risk mitigation standards, procedures and guidelines, and monitoring their effectiveness and efficiency.

MYTILINEOS periodically works with **independent organizations** and consultants, who evaluate the adequacy and effectiveness of the Information Security Management System and verify that an information resource or management system meets the necessary requirements specified by the respective policies for the protection of information systems and their data.

Moreover, a **regular and structured information security awareness-raising** and training program has been developed and is implemented across the entire Company on a continuous basis. The aim of the program is to ensure that all employees, contractors and relevant third parties with access to information and information systems, understand the need for information security, acknowledge the responsibilities assigned to them under the Information Security Framework, and perform their duties demonstrating a high level of professional ethics. This program is evaluated and revised, if appropriate, at regular intervals through exams, as well as through exercises simulating actual cybersecurity attacks.

Finally, to ensure business continuity and minimize the impact of a cybersecurity breach or natural disaster, a **business continuity and disaster recovery plan** has been designed and implemented, which is tested and updated on a regular basis. At regular intervals or if issues arise in the wider cybersecurity environment in which the Company operates, relevant presentations are made at the Senior Management or Audit Committee level. The Senior Management is responsible for taking appropriate measures that will guarantee business continuity according to the business needs.

Customer privacy

The protection of natural persons against the processing of personal data is a fundamental right and is of the utmost priority for MYTILINEOS. Therefore, the collection and processing of personal data is carried out only in accordance with the law and only where required in connection with business relationships and with the Company's business activity. The Company allows access to such data by authorized persons only and takes increased data security measures.

Although MYTILINEOS does not basically process special categories of data (sensitive data), the business activity of Protergia in the retail sales of electricity and natural gas as well as the size of MYTILINEOS in terms of the number of its employees and active business partners, require the processing of personal data on a large scale. MYTILINEOS remains responsible for the processing of data ("data processor") and has specific obligations and responsibilities, which also apply in cases where such processing is outsourced to third parties. In addition, transactions with business partners outside the European Union, especially in countries with less rigorous data protection legislation, create the need for transferring personal data whose protection should be ensured.

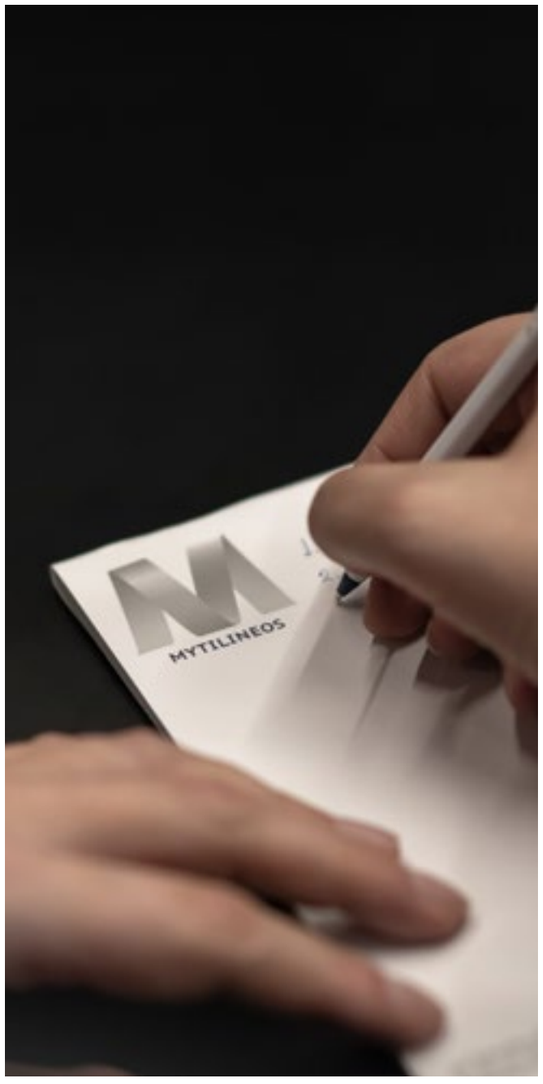
The Company may face various risks related to the protection of personal data, which may be financial in nature, such as from possible sanctions imposed by European data protection authorities or from claims of personal data subjects that have suffered damage, as well as risks related to negative publicity and reputational damage, in cases of improper retention and processing of its customers' personal data.

For this reason, MYTILINEOS has taken a number of steps to ensure, as far as possible, the protection of the personal data it manages. More specifically:

- has a **Data Protection Officer** (full-time employee) since 2018 and has duly notified the competent Authority of the details of this person,
- has carried out a **study on the deviations** from the General Data Protection Regulation and has taken appropriate corrective action since 2018,
- has established a **data protection policy** for all its employees and subsidiaries, as well as for its business partners, and has communicated it to all the parties concerned,
- has completed **impact studies** (Data Privacy Impact Assessments) regarding the processings required,
- has established and operates a **mechanism for recording any breaches** of personal data and for notifying them to the competent Data Protection Authority as well as to the affected data subjects, if required, while
- in terms of **training,** it has provided by the end of 2021 face-to-face as well as online trainings to over 850 employees who either process personal data or supervise their processing.

In addition, the risks related to the protection of personal data are included in the Company's Risk Management System and are continuously monitored. In 2021, the audits for the protection of personal data in the Metallurgy and Power & Gas Business Units were completed by the Company's internal audit function without significant findings. During 2021, the Company carried out a total of 10 in-depth checks of processors to verify their compliance with the General Data Protection Regulation (GDPR). **ASI**

MYTILINEOS' compliance with the applicable legislation and the implementation of controls to confirm observance of the rules concerning its activity, **resulted in the absence of significant incidents involving a breach of personal data during 2021**. Moreover, in 2021, eight (8) incidents involving the mailing of contracts / bills to the wrong recipients occurred in the Power & Gas Business Unit, in response to which additional technical and organizational measures were implemented to eliminate such occurrences altogether. These incidents, which are not considered significant, were reported to the competent Authority within the prescribed deadline and the data subjects were immediately informed, where required. In addition, there have been three (3) confirmed cases of promotional calls from external business partners of MYTILINEOS to telephone numbers of subscribers falling under Article 11 of Law 3471/2006 on "unsolicited communication". Finally, three complaints were forwarded to the Company by the competent Authority. **[GRI 418-1]**



Enterprise Risk Management

[GRI 102-11] [GRI 102-15]

The activities of MYTILINEOS are affected by multiple risks, whose occurrence may impact its activities, its business presence, its financial performance and the achievement of its strategic goals.

In 2021, MYTILINEOS, considering the nature and extent of the risks it is faced with in an ever-changing economic and business environment, **proceeded to reassess the main business risks,** which it classified in the following main categories:

- Financial risk
- Market risk
- Legal & Regulatory Compliance risk
- Operational risk
- Strategic risk

MYTILINEOS implements an **Enterprise Risk Management System** for the identification, analysis, assessment, monitoring and reporting of risks, in order to limit the likelihood and the impacts of risks and to maximize the benefit from the opportunities presented. In this context, an **Enterprise Risk Assessment** methodology has been adopted, which is based on best international practices and is tailored to the needs of MYTILINEOS, promoting a unified culture that integrates risk management and decision-making in its procedures and activities.

This methodology (top-down & bottom-up) is **followed by all Business Units**, Central Services and Support Services of MYTILINEOS and consists of the following steps:

- Identification and classification of key risk factors
- Assessment of the risk's likelihood of occurrence and impacts
- Assessment of the adequacy of risk mitigation mechanisms
- Assessment of residual risk
- Risk monitoring

The responsible Executives of the General Divisions are involved in the systematic identification and assessment of risks affecting business activities, as well as in the assessment of the adequacy of the risk mitigation mechanisms. They also supervise the formulation and timely implementation of the risk management plans. For every risk, a Risk Owner has been assigned, whose responsibilities are the implementation of the risk assessment methodology and the formulation of the risk response plan. In addition, in each General Division the role of Risk Partner has been established, whose responsibilities are the development and updating of the Risk Register, as well as the monitoring of the progress made in the implementation of each risk management plan.

The risk assessment results are communicated by the Enterprise Risk Management Division to the Executive Committee and the Audit Committee of the Board of Directors of MYTILINEOS.

Finally, **internal audits** are carried out at MYTILINEOS to ensure the proper and effective implementation of the risk management procedures.