COMPLIANCE PROGRAM

Presentation

ARQUIMEA

CONTENTS

1. What is a Compliance Program?

- A Compliance Program is an integrated group of rules and procedures to identify and manage risks within a company through an internal control system.

  As a result, a Compliance Program constitutes a guarantee of the commitment to comply with company rules regarding both crime prevention and the regulation of ethical, organizational, governance and work processes at the company.

- Why implement a Compliance Program? Basically, for three reasons:

  a) Because at ARQUIMEA — as is reflected in its Code of Ethics — we are firmly committed to certain values and behaviour guidelines based on professional and human ethics that encourage a culture of strict compliance with the law and standards internally and with respect to our customers, suppliers and collaborators.
  b) Because at companies such as ARQUIMEA, which are characterized by a great diversification of their business activities, the implementation of a Compliance program is not only an essential driver of cohesion among their employees with regard to common values and styles, but also a factor that strengthens transparency and internal communications among them.
  c) Finally, because the implementation of a Compliance system is also necessary for legal reasons (see the Appendix), meaning that a company needs to implement a permanent activity and business process control system that allows its executives and employees to prevent, detect and correct any risks that could compromise the proper operation of the organization.

- What are those risks? There are essentially two types of criminal risks to which a company could be exposed:

  a) Criminal risks inherent to company's business model

  In order to effectively focus the Compliance program a company must identify those criminal risks that must necessarily be prevented and which are associated with its specific business activity. The case of ARQUIMEA, the identification of risks is particularly essential due to the great diversification of its business activities:

  - **Aerospace&Defence**

    The development of highly reliable systems, components and applications for the aerospace, defence and security industry.

  - **Space**

    Thermal control hardware and engineering solutions for satellites and spacecraft. Management of the complete project chain: conceptual and final design, manufacturing, assembly, testing, etc.

- **AgroTech**

  R+D applied to the development of seed analysis systems, animal reproduction and the bio-engineering area, as well as environmental solutions for cattle, agriculture and forestry.

- **HealthCare**

  The management of protocols and services for COVID-19 diagnostics — PCRs, Rapid Antigen Tests and Rapid Antibody Tests — for individuals, airports, organizations and private events and public administrations, as well as the development of new solutions for human DNA tests and assisted reproductive technologies.

- **Fintech**

  The development of Technological Sponsorship as a manner of encouraging the R&D&i ecosystem in Spain, obtaining private investments to finance R&D&i projects.

- **Innovation**

  The encouragement, development and investigation of ideas and projects with a high technological impact through the Arquimea Research Centre, a private R&D&i centre where innovative ideas in various areas are developed and researched: Electronics, Microelectronics, Photonics, Physics, Artificial Intelligence and Biotechnology.

The specific criminal risks involved with each of these business areas must be identified in order to define a response.

b) Common (transversal) criminal risks at any type of company

These types of risks are common to any company merely due to its existence. For example, in the case of ARQUIMEA one of the risks to be identified and prevented relates to compliance with Data Protection and Information Security Regulations.

In order to guarantee the effective implementation of ARQUIMEA's Compliance Program, the position of Compliance Officer has been created. This position not only guarantees the supervision of the Program's operation, but is also the person that promotes initiatives to update that Program within the company.

2. Elements of Arquimea's Compliance Program

Arquimea's Compliance Program is made up of the Internal Information System and a set of policies and procedures aimed at guaranteeing adequate regulatory compliance and an ethical culture within the company.

a) Internal Information System

The main objective of Arquimea's Internal Information System ("IIS") is to protect people who, in a work or professional context, detect serious or very serious criminal or administrative infringements and report them through the mechanisms regulated for this purpose, as well as to strengthen and promote the culture of information as a mechanism to prevent and detect irregular conduct, all in accordance with the provisions of Law 2/2023 of 20 February, regulating the protection of people who report regulatory infringements and the fight against corruption.

Arquimea's IIS is mainly composed of the following:

- *Internal Information System Policy*

  This policy sets out the principles that inspire Arquimea's Internal Information System and the issues set out in Law 2/2023, of 20 February, regulating the protection of people who report regulatory infringements and the fight against corruption.

- *Whistleblower Channel*

  It is a tool open not only to ARQUIMEA employees and managers, but also to its customers, suppliers, collaborators and business partners, which allows any serious non-compliance that may be detected in relation to ARQUIMEA's operations to be reported anonymously. It is accessible through the Arquimea website.

- *Internal Information System Manager*

  This is the person responsible for diligently assuming, and in the absence of conflict of interest, the resolution of the procedures initiated as a result of the information received through the established Ethical Channel, ensuring the proper application of the SII Procedure.

- *Procedure for the management and processing of the information received in the Internal Information System*

  This policy sets out the procedure to be followed for processing communications received through the Ethical Channel.

On the other hand, with regard to the policies that make up Arquimea's Compliance Program, it is necessary to clarify that it is approached from three different but complementary perspectives: Ethical Compliance, Criminal Compliance and Operational Compliance.

b) Ethical Compliance

This consists of a group of ethics and business conduct and good practices guidelines to which ARQUIMEA is committed when carrying out its business. The elements of Ethical Compliance are as follows:

- *Code of Ethics*

  The Code of Ethics and Business Conduct is an express statement of the Values that guide the Approach and activities of ARQUIMEA, as well as of the principles and

standards of conduct that must guide the behaviour of all of its employees, executives and directors (accessible on the website).

- *Clauses for contracts with third parties.*

  Internal. These consist of clauses that are included in all of ARQUIMEA's contracts concluded with suppliers, customers and other agents that report the Compliance Program and, specifically, the Code of Ethics, and their commitment to collaborate with its compliance is requested.

c) Criminal Compliance.

These are the specific mandatory rules and procedures for each of the ARQUIMEA companies that are associated with the various business activities carried out by each one and they guarantee their exoneration from potential criminal liability. The elements of Criminal Compliance are as follows:

- *High Importance Risk Prevention Procedures Guide*

  (Internal). This Guide is a catalogue of the internal practices that the persons responsible for each of the ARQUIMEA companies have identified as priorities within those companies to prevent any failure to comply with the regulations that are very directly associated with the business activity carried out by their company. They are therefore specific to each of those companies.

- *Anti-Bribery and Anti-Corruption Prevention Policy*

  (Available on the website). This is an express statement of ARQUIMEA's commitment to continuously monitor, and even impose penalties if necessary, any internal or external fraudulent behaviour as well as its commitment to develop a business culture based on ethics and regulatory compliance by implementing the rules of conduct that serve as a guarantee.

- *Quarterly Report on Incidents*

  (Internal). This is a system (two forms) that allow the persons responsible for ARQUIMEA companies to report quarterly to the Compliance Officer any Compliance Program incident that may have arisen or that is taking place.

d) Operational Compliance.

This is the group of corporate rules and procedures intended to prevent any failure to comply in the functional areas and business units at the companies and ARQUIMEA as a whole. The elements of Operational Compliance, which are internal and common to all companies, are as follows:

- *Information Security and Data Protection Rules*

  These rules make up a group of corporate procedures established for all ARQUIMEA companies that ensure compliance with all Data Protection regulations and, in the event of any incident or security breach, allow it to demonstrate to the Spanish Data Protection Agency the measures that have been implemented.

- *Travel and Expense Policy*

  Defined by the Financial area at ARQUIMEA, this is the group of procedures to manage employee and executive travel at all companies and the settlement of the associated expenses.

- *Payment Process*

  Defined by the Financial area at ARQUIMEA, this is the group of procedures that define the payment policy for all companies, as well as the process for managing supplier invoices.

- *Working day and schedule*

  Defined by the Human Resource area at ARQUIMEA, this is the group of criteria established to manage work schedules, working time and working days for company employees applying criteria concerning efficiency and family/work reconciliation.

- *Occupational Hazard Prevention Policy*

  This describes the group of practices, procedures, processes and actions that are necessary to adequately manage occupational hazard prevention at each of the ARQUIMEA companies in order to comply with all of the provisions of Law 54/2003 and Royal Decree 604/2006 on Occupational Hazard Prevention.

- *Insurance Policy*

  This describes the group of procedures to be followed when obtaining, renewing or terminating insurance policies covering ARQUIMEA companies, as well as the process to be followed in the event of an insured loss.

Appendix: Legal basis for the criminal liability of companies

Companies may be criminally liable.

- On 23 December 2010, the reform of the Criminal Code entered into force through Organic Law 5/2010 (22 June).

  That reform gave rise to the elimination of the traditional principle under Spanish criminal law according to which legal persons (companies) could not be criminally liable with the presupposition that crimes could only be attributable to natural persons, although with certain nuances. After Organic Law 5/2010 entered into force, legal persons (companies) are criminally liable for certain crimes committed by de facto and de jure directors when performing their duties and by anyone subject to their authority.

- Organic Law 1/2015, which amends the Criminal Code, subsequently introduced significant changes compared to the preceding regulation after entering into force on 1 July 2015. Specifically, Article 31 bis establishes that legal persons (companies) are criminally liable for:

  A. Crimes committed in the name of or on behalf of companies and to their direct or indirect benefit, by their legal representatives or by anyone, acting individually or as part of a body at the legal person, that is authorized to take decisions in the name of the legal person or hold organizational and control authorities within the company.

  B. Crimes committed during the performance of the business activities and on behalf of and to the direct or indirect benefit of those companies, by anyone subject to the authority of the natural persons mentioned in the preceding paragraph (A), that may have carried out the activities by seriously failing to comply with the duty of supervising, monitoring and controlling the business, based on the specific circumstances of the case concerned.

How can companies be exempt from criminal liability?

This point is important since it serves as a basis for the Compliance programs at the companies. Article 31 bis of the Criminal Code also provides that companies will be exempt from liability in the following cases:

CASES	A COMPANY IS EXEMPT FROM LIABILITY WHEN....
IN CASES OF CRIMES	

COMMITTED BY THE PERSONS IDENTIFIED IN POINT A.	1. The governing body has adopted and effectively executed, before the crime is committed, organization and management models that include suitable monitoring and control measures to prevent crimes of the same nature or to significantly reduce the risk of them being committed. 2. The supervision of the operation of and compliance with the prevention model is entrusted to a company body with autonomous authority to take initiatives and apply controls, or which is legally charged with supervising the effectiveness of the company's internal controls. 3. The material authors committed the crime by fraudulently avoiding the organization and prevention models. 4. Whenever there has been no omission or insufficient fulfilment of the supervisory, monitoring and control duties by the responsible body.
IN CASES OF CRIMES COMMITTED BY THE PERSONS IDENTIFIED IN POINT B.	…before the crime is committed, the company has adopted and executed an organization and management model that is adequate to prevent crimes of the same nature that was committed, including the following measures: 1. Identification of activities in which crimes must be prevented, i.e., identification of criminal risks. 2. Establishment of protocols or procedures that specify the process through which the company's decision was taken and their execution; i.e. self-regulation. 3. Existence of models for managing the financial resources to impede the crimes that may be committed. 4. Impose the obligation to report possible risks and failures to comply. 5. Establish an adequate disciplinary system. 6. Perform regular verifications of the model and of any future modifications when any relevant infractions of the model's provisions are revealed or when there are changes in the organization, in the control structure or in the business activity that make such changes necessary.

All of these matters, which form part of the companies' Compliance models were supplemented by the State Prosecutors Office through Circular 1/2016 that emphasizes the importance of promoting a true business ethics culture, for which that Office advised including the following in those models:

- A risk assessment by type of customer, country or geographic area.
- The establishment of a procedure and deadline for review.
- The training of executives and employees.

Furthermore, the Prosecutor's Circular made a distinction between two possible reasons for the criminal prosecution of a company:

- It is defective corporate organization, which would lead to the consideration that the infraction has been committed as a result of inefficient control over the company.

- The failure to comply with the duties of supervision, monitoring and control, which would mean that the prosecution of the company would be the result of the conduct of its managers or the failure to comply with their obligation to control employees.

Conclusion

In order to extend criminal liability to companies when a crime is committed within its organization, the absence of effective guidelines or regulatory compliance programs must be proven. For this reason, having an effective Compliance program is a fundamental element to decide whether or not the organization is liable.

ARQUIMEA

arquimea.com