



**ORGANIZATION, MANAGEMENT AND CONTROL  
MODEL – EX D.LGS 231/2001**

**Code of Ethics**



**INDEX**

• Introduction	4
• Definitions	4
• Assumptions and Purpose of the Code	4
1. General Principles	5
1.1 Compliance with laws, ethical guidelines, regulations, and procedures	5
1.2 Conflict of interest	5
1.3 Harassment and discrimination	5
1.4 Substance abuse (alcohol and drugs)	5
1.5 Smoking	5
2. Conduct Rules towards Personnel	6
2.1 Human resources	6
2.2 Personnel selection	6
2.3 Employee evaluation	6
2.4 Employee rights and duties	6
2.5 Health and safety protection in the workplace	7
3. Conduct Rules towards Public Administration	7
3.1 Relations with public administration	7
3.2 Relations with public institutions and supervisory authorities	8
3.3 Relations with the judiciary authority	8
3.4 Offering money, gifts, or other benefits	8
3.5 Influence on public administration decisions	8
3.6 Employment relations with public administration	8
3.7 Transparency in the management of public funding and contributions	9
3.8 Conflicts of interest with public administration	9
4. Conduct Rules in Relations with Suppliers and Customers	9
4.1 Selection	9
4.2 Management of contractual relationships	9
4.3 Gifts, offers, and presents	9
5. Conduct Rules in Relations with Society	10
5.1 Economic relations with political parties and trade unions at the national level	10
6. Conduct Rules in Business Activities	10
6.1 Transactions and operations	10
6.2 Purchases of goods and services and awarding of external consultancies	10
6.3 Management of IT systems	11
6.4 Use of currency, public credit cards, and stamp values	11
6.5 Tools and signs of recognition and protection of copyright	11
6.6 Terrorism and subversion of democratic order	12
6.7 Protection of individual personality	12
6.8 Activities related to receiving stolen goods, money laundering, and self-laundering	12
6.9 Transnational activities and protection against organized crime	13
6.10 Competition protection	13
7. Principles Relating to Corporate Offenses	14
7.1 Management of financial and accounting data	14
7.2 Relations with the company's supervisory bodies	14
7.3 Protection of the company's assets	14
7.4 Protection of creditors	14
7.5 Conflicts of interest for directors	14
7.6 Influence on shareholders' meetings	14
7.7 Relations with public supervisory authorities	14



**ORGANIZATION, MANAGEMENT AND CONTROL  
MODEL – EX D.LGS 231/2001**

7.8 Relations with bankers	15
7.9 Relations between private individuals	15
8. Confidentiality and Privacy Protection	15
9. The Supervisory Body	11
10. Sanctions	11
11. Whistleblowing Reports	11
12. Internal Reporting	17
13. Knowledge	17
14. Final Provisions	18
14.1 Conflict with the Code	18
14.2 Amendments to the Code	18
15. Acknowledgment Statement	18



## **Introduction**

The Code of Ethics is a document through which Zilio Industries S.p.A. specifies the values, behavioral principles, commitments, and responsibilities it assumes internally and externally.

The Code of Ethics also highlights the rights, duties, and responsibilities of all recipients. It forms an integral part of Zilio Industries S.p.A.'s organizational model.

The ethical principles outlined in this document are relevant for the prevention of offenses under Legislative Decree 231/2001 and represent a crucial element of the preventive control system.

Zilio Industries S.p.A. makes the Code of Ethics and conduct guidelines available to recipients.

## **Definitions**

**Code of Ethics:** This Code, adopted by the governing body of Zilio Industries S.p.A.

**Decree:** Legislative Decree No. 231/2001 on the administrative liability of entities.

**Recipients:** All those who act, operate, or collaborate in any capacity with Zilio Industries S.p.A. (employees, consultants, suppliers, and other third parties) and who find themselves in situations requiring the adoption of behavior relevant from an ethical and legal perspective.

**Model:** The Organization, Management, and Control Model adopted by Zilio Industries S.p.A. under Legislative Decree No. 231/2001.

**Supervisory Body:** The body established under Legislative Decree No. 231/2001, appointed by the governing body of Zilio Industries S.p.A.

**Company:** Zilio Industries S.p.A., with its premises in via Sega Vecchia n.65, 36050 Pozzoleone (VI), Italy.

**Company Management:** The governing body of Zilio Industries S.p.A.

## **Assumptions and Purpose of the Code**

### **What is the purpose of the Code of Ethics?**

This Code of Ethics aims to provide general ethical guidelines for conduct to be followed during the execution of activities, as well as to contribute to preventing the occurrence of administrative offenses stemming from crimes listed in the Decree.

### **Who is the Code of Ethics addressed to?**

The Code of Ethics is intended for all individuals who act, operate, or collaborate with Zilio Industries S.p.A. in any capacity (employees, consultants, suppliers, and other third parties) and who face situations that require behavior that is significant both from an ethical and legal perspective. The principles and rules in the Code apply: a) To all employees of the Company, regardless of their role or function; b) To members of various corporate bodies; c) To any third parties who may act on behalf of Zilio Industries S.p.A.; d) To third parties who have relationships with Zilio Industries S.p.A., such as suppliers, commercial partners, and contractual counterparts involved in negotiations or agreements with the Company.

### **What does Zilio Industries S.p.A. expect from its employees, collaborators, and partners?**

All recipients of this Code are obliged to ensure that their collaborators and interlocutors behave in accordance with the values identified by the Company and with the specific obligations arising from ethical guidelines, as well as from principles deemed necessary for the context and objectives of their work.

In the presence or absence of specific provisions, it is essential that everyone acts according to the highest ethical standards, to which the Company adheres in its conduct.

The Company does not wish to maintain relationships with parties who do not commit to respecting the values, principles, and rules outlined in this Code.

In order to ensure compliance, Zilio Industries S.p.A. includes clauses in contracts with third parties to enforce this Code.

No situation, even when believed to be in the Company's interest or benefit, can justify behavior that conflicts with the principles and values stated in this Code.

These obligations, particularly for employees, integrate the provisions of articles 2104 and 2105 of the Italian



Civil Code, as well as the applicable National Collective Labor Agreement.

The Code is an integral part of the Organization, Management, and Control Model adopted by the Company under Legislative Decree No. 231/2001.

The recipients are obligated to:

- Comply with all laws related to environmental protection and human rights;
- Strive to achieve objectives set within the framework of sustainable development strategy;
- Immediately report any violations, even if suspected, of the Code and the Company's policies.

## **1. General Principles**

### **1.1 Compliance with Laws, Ethical Guidelines, Regulations, and Procedures**

Recipients, each within their respective competence, must diligently respect all applicable laws in every country where the Company operates, the Code, any other ethical guidelines the Company adheres to, and internal regulations. Under no circumstances can the pursuit of the Company's interest justify dishonest behavior or actions that conflict with the applicable regulations or ethical guidelines.

Recipients must also comply with company operational procedures. Any legal violations must be reported to the competent authorities.

### **1.2 Conflict of Interest**

A conflict of interest occurs when someone pursues a personal interest that diverges from the Company's mission or engages in activities that interfere with their ability to make decisions in the exclusive interest of the Company, or when they personally benefit from business opportunities of the Company.

If recipients of this Code find themselves, or believe they may find themselves, in a position of conflict of interest, or if there are valid reasons for concern, they must refrain from making decisions or engaging in activities that might affect the Company directly or indirectly.

In cases of abstention, or if abstention is not possible, the recipient must inform their supervisor and/or business contact of the potential conflict, explaining the reasons for it. The supervisor must inform the Company's governance, which will assess the situation and may authorize the potentially conflicting activity only after taking necessary actions to resolve the conflict.

### **1.3 Harassment and Discrimination**

The Company:

- a. Guarantees a work environment that values the diversity of employees, in compliance with the principle of equality, ensuring the protection of the dignity and freedom of each employee in the workplace;
- b. Does not tolerate any form of discrimination based on race, gender, political, union, or religious views;
- c. Requires employees to refrain from any intimidation, harassment, or offensive behavior;
- d. Does not tolerate sexual harassment, which is defined as any unwanted act or behavior, including verbal, of a sexual nature that offends the dignity of the person subjected to it; it also does not tolerate creating a climate of intimidation for the person subjected to such harassment.

Those who believe they are victims of harassment or discriminatory behavior, or are aware of intimidation, discrimination, or harassment occurring, must inform their Supervisor, the HR Manager, or the Company Management, as well as the Supervisory Body, who will promptly and confidentially take all necessary actions to resolve the situation and restore a harmonious working environment.

### **1.4 Abuse of Alcohol or Drugs**

The Company considers it reprehensible for employees to perform their duties under the influence of alcohol or drugs, as well as using such substances during working hours.

Moreover, all personnel are urged to maintain the highest standards of integrity and fairness.

Anyone observing behaviors in conflict with the principles and rules in this Code of Ethics and/or the Organizational Model must report it to their Supervisor, the HR Manager, or Company Management, as well as the Supervisory Body, who will promptly and confidentially take any necessary actions.

### **1.5 Smoking**

Smoking is prohibited in workplaces and in areas where computer equipment is stored. Smoking is permitted outside company premises.



## **ORGANIZATION, MANAGEMENT AND CONTROL MODEL – EX D.LGS 231/2001**

Anyone observing behaviors contrary to the principles and rules outlined must inform their Supervisor, the HR Manager, or Company Management, as well as the Supervisory Body, who will take the necessary actions promptly and confidentially.

### **2. Conduct Rules towards Personnel**

#### **2.1 Human Resources**

Human resources are an essential element of the company's organization and represent the critical success factor for the company's dynamism and operations.

The Company provides equal opportunities to all employees based on merit and in compliance with the principle of equality, enabling each individual to develop their abilities, skills, and competences, offering training and/or development programs when needed.

The Company respects all forms of diversity, fostering an inclusive work environment.

All employees must be familiar with the regulations governing their functions and associated behaviors; if not, they should report the non-compliance to the HR Manager.

#### **2.2 Personnel Selection**

A mere promise of employment in exchange for favors may constitute an offense.

The personnel selection process must aim to select the most suitable candidate based on the alignment of their profile and specific competencies with the company's needs, as identified by the requesting function, always ensuring equal opportunities for all candidates.

Requested information must be strictly related to verifying the professional and psychological aspects of the profile, respecting the candidate's privacy and opinions.

Favoritism, nepotism, or clientelism in the selection and hiring phases are prohibited.

The HR Manager is responsible for verifying compliance with the principles outlined above, within the limits of available information, and for adopting appropriate preventive measures.

The Company strictly prohibits employing foreign workers without a residence permit or with a revoked or expired permit, unless renewal documentation with a receipt has been presented.

#### **2.3 Personnel Evaluation**

The Company is committed to ensuring that the set objectives for personnel do not encourage illegal behavior, but are instead achievable, specific, concrete, measurable, and related to the time frame for their completion. Any difficulties or conflicts with this principle must be reported promptly to the HR Manager and the Supervisory Body to take corrective actions.

#### **2.4 Employee Rights and Duties**

An employee of the Company is obliged to:

- a. Know and comply with current regulations, processes, procedures, company guidelines, and the principles contained in this Code;
- b. Follow the instructions and directives issued by the Company, the manager, or their respective supervisors;
- c. Fulfill all obligations necessary to protect health and safety in the workplace;
- d. Collaborate adequately with colleagues, managers, and/or supervisors, providing all relevant information and engaging in behaviors that ensure maximum efficiency in carrying out tasks and achieving common objectives;
- e. Avoid abusing or generating false beliefs regarding their position, role, or powers within the Company, and intervene immediately to correct any misunderstandings;
- f. Refrain from actions contrary to their official duties, or delay actions to obtain money or other benefits for themselves or others;
- g. Treat everyone fairly and equitably, avoid giving or receiving favors or pressure to obtain specific advantages from suppliers;
- h. Maintain confidentiality regarding company activities, financial, and economic information;
- i. Not use information obtained during their work for personal purposes or to gain financial or non-financial benefits;
- j. Promote awareness of the Code among all individuals with whom they interact in the course of their



work, both formally and informally;

- k. Not disclose any information regarding the Company's suppliers to third parties, especially to other suppliers;
- l. Never denigrate the Company or those who have had any kind of relationship with it;
- m. Avoid participating in informal meetings with individuals seeking information on relevant matters concerning their office activities unless explicitly authorized by their Supervisor;
- n. Report truthful and accurate information to the Company, such as summaries of time spent, expense reports, meeting minutes, etc.;
- o. Not use work tools for personal purposes, except in cases of emergency, and take care of company property such as offices, furniture, vehicles, or materials;
- p. Acquire the necessary professional skills for their job and maintain an adequate level of knowledge and experience throughout the employment relationship by updating their skills and attending training or requalification courses provided by the Company;
- q. Not profit from their work activities, whether directly or indirectly, with or without damage to the Company;
- r. Maintain proper conduct, language, and attire in the workplace;
- s. Fulfill obligations promptly and proactively as required by the Model (such as training courses, submitting reports, attending meetings with the Supervisory Body, etc.), avoiding obstructionist behavior that could compromise the functioning of the Model and the work of the Supervisory Body.

### **2.5 Health and Safety in the Workplace**

The Company is committed to adopting all necessary measures to protect the physical and moral integrity of its workers, in compliance with current regulations.

In particular, the Company ensures that:

- a. Compliance with health and safety legislation is a priority;
- b. Risks to workers are avoided as much as possible by choosing suitable and less hazardous materials and equipment to mitigate risks at the source;
- c. Unavoidable risks are properly assessed and mitigated with appropriate collective and individual safety measures;
- d. Workers receive relevant, up-to-date, and specific information and training related to their duties;
- e. Workers' participation in matters concerning health and safety in the workplace is guaranteed;
- f. Any safety issues identified during activities or inspections are addressed quickly and effectively;
- g. Work organization and operations safeguard workers' health, as well as the health of third parties and the community where the Company operates.

Workers are required to ensure full compliance with legal requirements, the principles of this Code, and internal procedures to ensure health and safety in the workplace. They must also report any violations or behaviors that contradict the Code or Model.

## **3. Code of Conduct towards Public Administration**

### **3.1 Relations with Public Administration**

The Company's relations with Public Administration, public officials, or public service providers must be based on strict impartiality and correctness, compliance with applicable laws and regulations, and must not compromise the integrity or reputation of the Company.

Commitments and management of relations with Public Administration, public officials, or public service providers are reserved exclusively for the relevant company functions and authorized personnel.

Such individuals must diligently keep all documentation related to their relations with Public Administration.

In relations with Public Administration, public officials, or public service providers, the recipients are required to abstain from:

- a. offering, directly or through an intermediary, money, job opportunities, commercial opportunities, or any other benefits to public officials, their family members, or related individuals;
- b. seeking or establishing illicit personal relations of favor, influence, or interference that could affect the outcome of the relationship.



### **3.2 Relations with Public Institutions and Regulatory Authorities**

The Company maintains relations with public institutions based on integrity, correctness, and professionalism. Recipients must promptly comply with requests from regulatory authorities for inspections or checks, providing full cooperation and avoiding obstructive behaviors.

### **3.3 Relations with the Judiciary Authorities**

The Company operates legally and ethically, cooperating with the judiciary authorities and related authorities.

In case of any ongoing litigation, the management of the issue must adhere to the principles of legality, correctness, transparency, and all other ethical principles outlined in the Code.

All company personnel must promptly report any information related to potential or ongoing criminal proceedings concerning them or any other individual in the Company, related to their activities.

Specifically, managers, employees, and collaborators must refrain from illegal behaviors, such as:

- a. Offering or promising money or other benefits to public officials or public service providers to influence their impartiality;
- b. Sending false documents, attesting to non-existent qualifications, or providing false guarantees or statements;
- c. Deleting or destroying documents;
- d. Offering or promising money or other benefits to legal advisors of opposing companies to gain favorable results in disputes.

The HR Manager must ensure the confidentiality of information regarding ongoing proceedings, identifying who can access the information and how it will be stored.

It is forbidden for anyone to exert pressure on individuals involved in proceedings, such as:

- Promising salary increases or career advancement; or
- Threatening dismissals, pay reductions, or other forms of demotion or transfer.

Any legal proceedings related to crimes under the law must be promptly reported to the Supervisory Body.

### **3.4 Offer of Money, Gifts, or Other Benefits**

Zilio Industries S.p.A. condemns any behavior, whether undertaken by its corporate bodies and their members, or by its employees, consultants, collaborators, and third parties acting on behalf of the Company, that consists of offering or promising, directly or indirectly, money, services, benefits, or other utilities to Public Officials and/or Public Service Providers, whether Italian or foreign, except for gifts or benefits of modest value that fall within legitimate customs or practices, and do not result in an undue or illegal advantage to the company.

Gifts exceeding €150 are not considered modest in value. Any exceptions must be duly justified, tracked, and authorized by the company's senior management.

### **3.5 Influence on Public Administration Decisions**

Individuals assigned by the Company to follow any business dealings, requests, or relationships with the Italian and/or foreign Public Administration must not seek to illegally influence the decisions of Public Officials or Public Service Providers in the course of those dealings.

During business negotiations with Public Officials or Public Service Providers, the following actions are prohibited, whether directly or indirectly:

- Proposing employment or commercial opportunities that could personally benefit the Public Officials or Public Service Providers or their intermediaries.
- Offering money or any other benefits.
- Taking any actions to induce Public Officials to act or refrain from acting in violation of applicable laws.

### **3.6 Employment Relationships with Public Administration**

It is prohibited to establish employment or other forms of relationships, including consultancy contracts, with former public administration employees, whether Italian or foreign, who have participated or actively been involved in business negotiations or endorsed requests made by the company to the Public Administration, unless these relationships have been duly declared to the Human Resources Department and evaluated by the





company's senior management, and communicated to the Supervisory Body before proceeding with the hiring or establishment of such a relationship.

### **3.7 Transparency in Public Funding and Contributions Management**

The Company condemns any behavior aimed at obtaining contributions, loans, or other forms of financial support from the state, European institutions, or any public entity through falsified or altered documents, false declarations, omitted information, or other deceptive practices, including through electronic means, to mislead the funding body.

It is also prohibited to use such contributions, grants, or funding for purposes other than those for which they were granted, even if they are of modest value.

### **3.8 Conflicts of Interest with Public Administration**

The Company will not be represented in dealings with the Public Administration, either Italian or foreign, by individuals in a recognized conflict of interest unless this situation is properly disclosed to the Company's senior management and the Supervisory Body, and evaluated to determine whether such representation is acceptable.

Persons acting on behalf of the Company must refrain from engaging with the Public Administration in any case where there is a conflict of interest.

## **4. Rules of Conduct in Relations with Suppliers and Clients**

### **4.1 Selection**

In dealings with suppliers, all actions must be based on principles of honesty, fairness, good faith, balance, transparency, impartiality, and confidentiality.

Behaviors that could result in unfair favoritism towards a supplier, to the detriment of others, must be avoided. The primary objective in selecting suppliers is to avoid any discrimination and ensure maximum participation and competition among potential suppliers. Suppliers should be chosen in compliance with applicable laws and internal procedures, ensuring proper management throughout the contract execution.

Business relations should be conducted solely with reputable clients, companies, partners, and suppliers who engage in lawful commercial activities and whose income derives from legitimate sources.

### **4.2 Contractual Relationship Management**

In dealings with suppliers, the Recipients of this Code of Ethics must refrain from:

- accepting non-existent services.
- authorizing undue payments.
- engaging third parties in illegal or unethical activities.

At the same time, Recipients must:

- allow third parties to compete fairly for business with the company.
- consider potential conflicts of interest before involving third parties.
- choose qualified business partners with a good reputation for quality and honesty.
- ensure that agreements with commercial partners comply with the company's policies.

### **4.3 Gifts, Offers, and Favors**

Gifts include material goods (such as money or goods), immaterial benefits, or services and discounts on purchases.

In dealings with clients, gifts and entertainment expenses must comply with applicable laws and market practices, not exceed permitted value limits, and be approved and recorded in accordance with internal rules. No one may solicit or accept, directly or indirectly, gifts from suppliers, even potential ones, if they could be perceived as connected to the company's relationships or imply an attempt to gain undue advantages.

Gifts of symbolic or modest value may be accepted as long as they:

- comply with the law
- cannot be perceived as connected to obtaining an advantage



## **ORGANIZATION, MANAGEMENT AND CONTROL MODEL – EX D.LGS 231/2001**

- are typically offered to other individuals with similar relationships or during holidays or special occasions.

It is also prohibited to:

- offer or pay, directly or indirectly, any payments or material benefits to influence or compensate for official acts.
- engage in illegal or collusive practices, bribery, or favoritism.

Anyone receiving gifts related to their work on behalf of the Company that violate the previous rules must report it to their supervisor or senior management and, where appropriate, immediately return such gifts.

Any exceptions to these practices must be authorized by senior management and reported to the Supervisory Body.

### **5. Rules of Conduct in Relations with the Community**

#### **5.1 Economic Relations with Political Parties and Trade Unions at the National Level**

Under all circumstances, direct or indirect contributions to political parties, movements, committees, or trade unions, or their representatives and candidates, are prohibited.

### **6. Rules of Conduct in Business Activities**

#### **6.1 Transactions**

Every transaction must be lawful, authorized, consistent, documented, and verifiable at any time.

The procedures regulating transactions must allow for checks on the characteristics of the transaction, its motivations, the authorizations granted, and the execution of the operation itself.

Any person conducting transactions involving money, goods, or other economically valuable items belonging to the Company must act with authorization and provide valid evidence for verification upon request.

Each Company function is responsible for the truthfulness, authenticity, and originality of the documents produced and the information provided in the performance of its activities.

Respect for correctness, transparency, and good faith is required in dealings with all contractual counterparties.

Appointments given to any service companies and/or natural persons who look after the economic/financial interests of the Company must be drawn up in writing, indicating the contents and the agreed economic conditions. Any exceptions must be duly authorized and justified.

With reference to the commercial/professional reliability of suppliers and partners, all the information needed to assess the reputation/ethical reliability of the contractual counterparty must be requested and obtained (e.g. Model, certifications, legality rating, chamber of commerce visura, durc, etc.).

#### **6.2 Purchases of Goods and Services and External Consultancies**

Employees and others involved in purchases or external consultancy assignments on behalf of the Company must adhere to principles of transparency, fairness, economy, quality, relevance, and legality, acting with due diligence and in accordance with Company procedures and regulations.

They must ensure:

- selection of consultants based on procedures, evaluating the professional competence and reliability of candidates with formal written contracts or letters of appointment for consultants.
- clear definition of services and deliverables to allow verification of performance.
- proper archiving of all documentation, including correspondence and final versions of documents.
- delivery of the Company's Code of Ethics to consultants, ensuring a formal commitment to comply with its principles through inclusion in contracts.
- no payments or benefits to influence or compensate for official acts.
- avoidance of illegal, collusive, or unethical behavior.
- refraining from accepting excessive gifts or hospitality.
- avoiding unjustified compensation.



### **6.3 Management of IT Systems**

The Company condemns any behavior that alters the operation of an IT or telecommunication system or involves unauthorized access to data, information, or programs contained within, aimed at procuring an unfair benefit for the Company at the expense of the State.

It is forbidden to:

- install, download, and/or use computer programs and tools that allow the alteration, forgery, false certification, suppression, destruction, and/or concealment of public or private electronic documents;
- install, download, and/or use computer programs and tools that allow unauthorized access to IT or telecommunication systems protected by security measures or that allow unauthorized staying within them, in violation of the measures implemented by the data or program owner who intends to protect or maintain confidentiality;
- obtain, disseminate, share, and/or communicate passwords, access keys, or other means to allow the behaviors described above;
- use, obtain, disseminate, share, and/or communicate methods for employing devices, equipment, or computer programs designed to damage or interrupt an IT or telecommunication system;
- use, obtain, disseminate, share, and/or communicate methods for employing devices, equipment, or computer programs designed to intercept, prevent, or interrupt communications illegally, even if between multiple systems;
- destroy, deteriorate, delete, render unusable (in whole or in part), alter, or suppress other people's data or programs, or create serious obstacles to their functioning;
- use, install, download, and/or communicate techniques, programs, or computer tools that allow modifying the "Host Name" field of the server or any other related information or that allow hiding the sender's identity or modifying the settings of the IT tools provided by the Company.

### **6.4 Use of Currency, Public Credit Cards, and Stamp Duty**

The Company, sensitive to ensuring fairness and transparency in conducting business, requires recipients to comply with current regulations concerning the use and circulation of coins, public credit cards, and stamp duty. It severely penalizes any behavior aimed at illicit use and circulation of counterfeit credit cards, stamp duty, coins, and banknotes.

Any individual connected to the Company who receives banknotes, coins, or credit cards in payment is required to verify their compliance with the law and, if counterfeit, inform their superior or the Supervisory Body so that appropriate reports can be made.

### **6.5 Identifying Tools and Marks and Protection of Copyright**

The Company safeguards intellectual property rights, including copyrights, patents, trademarks, and other identifying marks, adhering to policies and procedures aimed at their protection and respecting others' intellectual property.

The Company prohibits any behavior intended to cause the loss, theft, unauthorized distribution, or misuse of its own or others' intellectual property or confidential information. To this end, the Company commits to implementing all necessary preventive and subsequent controls to ensure compliance with copyright law and the protection of trademarks, patents, and other identifying marks.

The Company condemns actions such as extracting, reproducing data, or using databases for purposes other than those for which they were created, especially when contrary to copyright protection laws.

Unauthorized reproduction of software, documentation or other materials protected by copyright is therefore prohibited, and at the same time, the Recipients of this Code undertake to comply with the restrictions specified in the license agreements relating to the production/distribution of third-party products, or those concluded with their own software suppliers.

The Company also condemns the illegal acquisition of trade secrets, supplier lists, and other confidential business information.



## **6.6 Terrorism and Subversion of the Democratic Order**

The Company requires compliance with all laws and regulations prohibiting terrorist activities and subversion of the democratic order, and thus also prohibits affiliation with organizations pursuing such goals.

The Company prohibits the use of its resources for financing or carrying out any activities aimed at achieving terrorist objectives or subverting the democratic order and commits to implementing appropriate control and monitoring measures to prevent any such behavior.

Employees are expressly forbidden from engaging in any practice or action that could be considered as terrorism or subversion of the legal order.

In case of doubt or if a situation appears equivocal, each employee is called upon to contact his or her Head of Department and the Supervisory Board in advance.

## **6.7 Protection of Individual Personality**

The Company condemns any behavior aimed at committing crimes against individual personality, such as slavery, child prostitution, child pornography, access to or possession of pornographic material, or activities exploiting child prostitution, and commits to adopting appropriate surveillance measures to prevent the commission of such crimes.

## **6.8 Activities aimed at receiving stolen goods, money laundering, the use of money, goods, or services of illicit origin, and self-laundering**

Receiving stolen goods is the crime of knowingly or covertly acquiring, possessing, or concealing goods or money of illicit origin (for example, goods derived from theft).

Money laundering refers to the set of operations aimed at giving a legitimate appearance to capital whose origin is actually illicit, thus making it more difficult to identify and subsequently recover.

The Company carries out its activities in full compliance with current anti-money laundering regulations and the provisions issued by the competent authorities.

In compliance with applicable regulations, the Company commits to avoiding any suspicious transactions in terms of fairness and transparency and to conducting preventive checks on the information available about customers, suppliers, external collaborators, and agents, in order to verify the respectability and legitimacy of their activities.

All Recipients commit to acting in a way that avoids involvement in operations that may potentially facilitate money laundering from illicit or criminal activities.

Each Recipient who carries out transactions or operations on behalf of the Company involving money, goods, or other economically valuable utilities must do so with proper authorization and provide any valid evidence for verification at any time.

Monitoring the financial flow from the Group's companies and/or third parties is a mandatory measure. This includes investments necessary for business activities and capital increases by shareholders, in order to ensure the proper identification of the source of funds.

Receipts and payments must strictly be made through bank transfers and/or bank checks issued with a non-transferable clause.

All Recipients are also required:

- not to accept money when there is any doubt about its illicit or uncertain origin;
- not to accept goods, services, or other utilities without an adequately authorized order/contract;
- not to make or accept cash payments equal to or exceeding the amount set by current regulations, specifying that this also applies to payments made in multiple smaller amounts related to the same supply and totaling or exceeding the amount set by the aforementioned regulation.

Personnel working on behalf of the Company must also:

- a. verify, where possible, the available information about users, counterparts, partners, suppliers, and consultants, in order to assess their reputation and the legitimacy of their activities before entering into any relationship involving the acquisition of goods or money;
- b. act in such a way as to avoid establishing any relationship, even with the slightest doubt, that might



facilitate money laundering from illicit or criminal activities, fully respecting primary and secondary anti-money laundering regulations and the internal control procedures established for this purpose.

### **6.9 Transnational activities and protection against organized crime**

The Company condemns any conduct, both at the national level and transnationally, by individuals in both senior or subordinate roles, that could even indirectly facilitate the commission of criminal offenses such as criminal association, mafia-type association, and obstruction of justice.

The Company commits to implementing all necessary preventive and subsequent control measures (verifiability, traceability, monitoring, segregation of duties, etc.) to avoid engaging with individuals belonging to such associations.

The Company also commits to controlling any form of internal association to prevent the occurrence of internal associative phenomena aimed at carrying out illicit behaviors, which exploit the means, resources, and assets of the company for such purposes.

Finally, the Company promotes development and legality in the areas where it operates; therefore, it encourages participation in any memoranda of understanding (or similar pacts) defined between public bodies, companies, trade associations, and trade unions, aimed at preventing criminal infiltration.

Business relationships should be maintained only with clients, collaborators, partners, and suppliers of proven reputation, who engage in lawful commercial activities and whose revenues come from legitimate sources. To this end, rules and procedures are in place to ensure the correct identification of customers and the adequate selection and evaluation of suppliers or partners for collaboration.

All necessary control tools are adopted to ensure that decision-making centers act and deliberate according to codified rules and keep records of their actions (i.e. meeting minutes, reporting mechanisms, etc.).

### **6.10 Protection of Competition**

The Company and all Recipients undertake to comply with antitrust regulations (which prohibit conduct aimed at limiting competition) and to avoid any improper action against commercial counterparts (e.g. sabotage, falsification of technical, commercial and accounting documents and, in general, any scheme of fraud).

The Company undertakes not to undertake in any case aggressive or deceptive commercial policies, aimed at conditioning the consumer in the purchase of its product through any form of physical-psychological intimidation or through false communication on the product such as to mislead the customer.

The Company recognises and promotes the value of free competition in a market economy as a decisive factor for growth, and therefore undertakes to operate in compliance with the principles and laws of the European Union and national laws protecting competition. The Company intends to protect the value of fair competition by refraining from collusive and predatory behaviour.

It is forbidden to enter into agreements with competitors on prices and methods of performing services that may be detrimental to free competition.

The Company inspires its conduct towards competitors with the principles of loyalty and fairness and, consequently, stigmatises and disapproves of any conduct that may constitute an impediment or disturbance to the exercise of a business or trade or that may be connected to the commission of one of the crimes against industry and trade.

The Company undertakes not to engage in unlawful, or in any case unfair, conduct for the purpose of taking possession of trade secrets, supplier lists, or information relating to infrastructures or other aspects of the economic activity of third parties.

Furthermore, the Company does not hire employees from competing companies for the sole purpose of obtaining information of a confidential nature, nor does it induce personnel or customers of competing companies to disclose information that they cannot disclose.

Commercial initiatives such as exclusive agreements, tied purchases, etc. must be authorised by the Head of the Function involved, in agreement with the Top Management.

During meetings with competitors at events, meetings, etc. organised by trade associations, as well as on all occasions of exchange of information with competing companies (e.g. consortia), it is forbidden to behave in any way that may be judged as preparatory to activities detrimental to free competition.

It is expressly forbidden for all Recipients to

- use violence against things or use fraudulent means to obstruct the industrial or commercial activity of others



- carry out, in the exercise of an industrial, commercial or in any case productive activity, acts of competition by resorting to violence or threats
- perpetrate conduct likely to cause damage to national industries by selling or in any case putting into circulation, on domestic or foreign markets, industrial products with counterfeit or altered names, brands or distinctive signs
- delivering to the purchaser, in the context of and/or in the exercise of a commercial activity, one movable thing for another (aliud pro alio) or a movable thing which in origin, provenance, quality or quantity is different from that stated or agreed
- selling or otherwise putting into circulation intellectual works or industrial products bearing names, trademarks or distinctive signs - national or foreign - likely to mislead the buyer as to the origin, source or quality of such works or product
- industrially manufacture or use objects or other goods made by usurping or violating the industrial property title, while being aware of its existence, as well as attempting to profit from the aforementioned goods by introducing them into the territory of the State, holding them and/or putting them up for sale or otherwise putting them into circulation.

## **7 Principles Related to Corporate Offenses**

### **7.1 Management of Data and Financial Information**

The Company condemns any behavior aimed at altering the accuracy and truthfulness of data and information contained in financial statements, reports, or any other legally required communications to shareholders and the public.

All individuals involved in preparing such documents must verify, with due diligence, the accuracy of the data and information.

All budget items, the determination and quantification of which presupposes discretionary assessments by the functions in charge, must be supported by legitimate choices and appropriate documentation.

### **7.2 Relations with Company Control Bodies**

The Company requires that all personnel maintain correct and transparent behavior in performing their tasks, particularly in relation to requests from shareholders, the Board of Statutory Auditors, and other corporate bodies performing their control functions.

### **7.3 Protection of Company Assets**

It is prohibited to engage in any behavior that may damage the integrity of company assets.

### **7.4 Protection of Company Creditors**

Any behavior aimed at reducing the Company's capital or merging with another company in a way that harms creditors is prohibited.

### **7.5 Conflict of Interest of Directors**

The Administrative Body is required to disclose to the Board of Statutory Auditors any personal or third-party interest they have in any company transaction. Such notice shall be precise and to the point, i.e. it shall specify the nature, terms, origin and extent of the interest.

### **7.6 Influence on the Shareholders' Meeting**

Any act aimed at illegitimately influencing the will of shareholders to irregularly form a majority or pass a different resolution than what would have been approved is prohibited.

### **7.7 Relations with Public Supervisory Authorities**

In the event of audits and inspections by the relevant public authorities, the corporate bodies and their members, the Company's employees, consultants, collaborators and third parties acting on behalf of the Company, must maintain an attitude of utmost helpfulness and cooperation towards the inspection and



control bodies. It is forbidden to obstruct, in any way, the functions of the Public Supervisory Authorities that come into contact with the Company in the course of their institutional duties.

### **7.8 Relations with Banking Operators**

In the context of relationships with banking operators, the Company's activities must adhere to the following control principles:

- Respect for roles and responsibilities as defined by the organizational chart and the authorization system concerning the management of relationships with financial/banking operators;
- Correctness and transparency in relationships with banking institutions, in compliance with principles of proper management and transparency;
- Integrity, impartiality, and independence, not improperly influencing the counterparty's decisions and not requesting preferential treatment (prohibition of promising, granting, or receiving favors, sums, or benefits of any kind);
- Completeness, accuracy, and truthfulness of all information and data transmitted to banking institutions.

### **7.9 Relations Between Private Entities**

The Recipients of this Code of Ethics are prohibited from:

- Making financial contributions or granting other advantages of any kind (promises of employment, use of company assets, etc.) to representatives (both senior and subordinate) of other private companies in order to obtain any advantage for the Company;
- Providing services or granting benefits of any kind to representatives of business partners and/or consultants that do not have adequate justification within the context of the established relationship;
- Paying fees or granting any other kind of benefit to agents/external collaborators that are not appropriately justified in relation to the type of work to be performed and the local practices in force;
- Making financial contributions or granting other benefits to suppliers that are not adequately justified within the context of the established relationship, or that could induce them to provide an undue advantage to the Company;
- Receiving any form of benefit, exceeding normal commercial or courtesy practices, or otherwise aimed at obtaining undue preferential treatment in the conduct of any business activity, in exchange for the payment of money or benefits of any kind.

## **8. Confidentiality and Privacy Protection**

All information and documents obtained while performing activities for the Company are confidential.

In conducting its activities, the Company collects, manages, and processes personal data in compliance with applicable laws.

The Company is committed to complying with the mandatory obligations set forth by regulatory provisions concerning the protection of personal data and to adopting a privacy management system that ensures the implementation of an organizational model and controls the risks arising from the processing of personal data. The privacy of employees and collaborators is protected by adopting standards that specify the information the Company requests from the individual and the related processing and retention methods, ensuring maximum transparency for the individuals concerned and restricting access to third parties, except for justified and exclusive work-related reasons.

Therefore, all employees of the Company, and those acting on its behalf, are obligated to maintain confidentiality regarding the data and information they possess due to their role, and are prohibited from voluntarily or involuntarily disclosing such information. Examples include information related to management plans, production processes, products, systems developed or otherwise managed/maintained, as well as information about negotiated and tender procedures, in addition to databases and data regarding personnel (hereinafter referred to as "Information" for brevity).

Any data processing aimed at investigating ideas, preferences, personal tastes, or generally the private lives of collaborators is prohibited.



## ORGANIZATION, MANAGEMENT AND CONTROL MODEL – EX D.LGS 231/2001

Additionally, unless otherwise provided by law, it is prohibited to disclose/share personal data without the prior consent of the individual concerned.

It is forbidden to process data in violation of current privacy protection laws.

Regarding data processing on paper and using computer systems, it is mandatory to comply with specific security measures put in place to prevent the risk of external breaches, such as access control to premises, passwords, personal identification codes, screen savers, as well as the loss, including accidental loss, of data. All Company documentation must be stored in compliance with internal guidelines and the measures adopted by the Company for data security.

### 9. The Supervisory Body

The Administrative Body of Zilio Industries S.p.A. has appointed a single-member Supervisory Body by the resolution of the sole director dated September 4, 2024.

The Supervisory Body is responsible for the monitoring and updating of the Organization, Management, and Control Model, as well as the Code of Ethics of the Company.

The main role of this body is to ensure that business practices align with the ethical and legal principles established, and to monitor the proper application and evolution of such organizational models within the company.

The Supervisory Body has unrestricted access to company data and information.

All employees, consultants, collaborators, and third parties working for the company are expected to cooperate fully with the Supervisory Body.

### 10. Sanctions

Violating the principles in the Code may result in disciplinary measures as per the company's Disciplinary System.

The severity of the infraction is assessed based on factors such as:

- a) Timing and manner of violation.
- b) Intentionality.
- c) Extent of damage or risk to the company.
- d) Predictability of consequences.
- e) Circumstances of violation.

Recidivism leads to harsher sanctions.

The Disciplinary System is part of the organization's overall framework.

### 11. Whistleblowing Reports

In the event of news regarding potential violations of this Code and/or the operational procedures that make up the Model, or other events that could alter its value and effectiveness, each person must report the issue to their responsible manager, who will refer it to the competent management or, if this is not possible for reasons of opportunity, directly to the company's top management. In any case, the violation must also be promptly reported to the Supervisory Body.

Failure to report a violation of this Code may be considered as a form of complicity in the violation itself.

Personal investigations or reporting to individuals other than those specifically designated are not permitted. Acts of retaliation or discrimination, whether direct or indirect, against whistleblowers related, directly or indirectly, to the report, are prohibited. The Company guarantees that no retaliation will be made following a report.

As the relationships between all levels of recipients must be based on principles of fairness, loyalty, and mutual respect, the Company sanctions the abuse of the duty to inform as described here, if it is carried out for merely emulative or retaliatory purposes.

Anyone who intends to report violations of the Code of Ethics or the Organizational Model as per Article 6 of Legislative Decree 231/2001 may submit a report:

- via the email address: OdV mailbox: [odv231.zilio@gmail.com](mailto:odv231.zilio@gmail.com);
- through a sealed envelope that any employee of the Company may use to report violations as indicated



above.

- through the whistleblowing platform.

The subject of the report should describe the facts in a written, as detailed as possible, manner.

Whistleblowing is the reporting system through which a person contributes or may contribute to uncovering risks and/or potentially harmful situations, such as violations or unlawful conduct.

In line with the provisions of Legislative Decree 10 March 2023, No. 24, the Company has adopted a system for managing reports of unlawful conduct and violations (i.e., whistleblowing) and an internal channel for submitting such reports, with the general principles outlined below.

Reports may concern:

- unlawful conduct and crimes potentially relevant under Legislative Decree 231/01;
- violations of the Company's Code of Ethics and Conduct and its Model;
- violations of national legal provisions (criminal, civil, accounting, and administrative offenses);
- violations of EU legal provisions (offenses committed in violation of EU regulations, including those relating to the following sectors: public procurement; services, products, and financial markets; prevention of money laundering and terrorism financing; transportation security; environmental protection; public health; consumer protection; protection of privacy and data security; and the security of networks and information systems);
- acts or omissions that harm the financial interests of the EU (such as fraud, corruption, or any other illegal activity connected to EU expenditures);
- acts or omissions concerning the internal market that compromise the free movement of goods, persons, services, and capital (e.g., violations of competition laws, state aid, and corporate taxes);
- acts or behaviors that undermine the object or purpose of EU provisions in the sectors listed above.

Reports made via the internal channel are directed to the Report Manager, an external individual appointed by the Administrative Body, who possesses the necessary expertise to properly manage the report. If the report concerns issues under Legislative Decree 231/01, the Report Manager will forward it to the Supervisory Body (also referred to as "OdV").

For detailed information on the subject of reports, the methods of reporting, and the management of reports, please refer to the specific "Whistleblowing" procedure.

## **12. Internal Reporting**

In the event of news regarding potential violations of this Code and/or the operational procedures that make up the Model, or other events that could alter its value and effectiveness, each person must report the issue to their responsible manager, who will refer it to the competent management or, if this is not possible for reasons of opportunity, directly to the top management. In any case, the violation must also be promptly reported to the Supervisory Body.

Failure to report a violation of this Code may be considered as a form of complicity in the violation itself.

Personal investigations or reporting to individuals other than those specifically designated are not permitted. All bodies that have been made aware of the violation are responsible for protecting those who have provided information about potential violations of the Code and the Model from any pressure, intimidation, or retaliation, ensuring the confidentiality of the whistleblower's identity, except where required by law and to protect the rights of the Company or individuals who may be falsely accused or acting in bad faith.

Periodically, top management reports to the Administrative Body, the Board of Statutory Auditors, and the Supervisory Body, including regarding the activities mentioned above.

## **13. Awareness**

This Code is made known to the corporate bodies and their members, employees, consultants, collaborators, and any other third party who may act on behalf of the Company.

All the aforementioned individuals are required to understand its contents and adhere to its principles.

Any application-related doubts regarding this Code must be promptly submitted and discussed with the Supervisory Body.



**ORGANIZATION, MANAGEMENT AND CONTROL  
MODEL – EX D.LGS 231/2001**

**14. Final Provisions**

**14.1 Conflict with Code of Ethics**

If any provision in the Code conflicts with internal regulations or procedures, the Code will take precedence.

**14.2 Modifications**

Any changes to the Code must follow the same approval process as the original version.

**Acknowledgment of Receipt and Acceptance**

I, the undersigned, declare that I have received my personal copy of the present Code of Ethics approved by the Administrative Body of Zilio Industries S.p.A. \_\_\_\_\_.

I also declare that I have understood, accepted, and intend to comply with the principles and rules of conduct contained in this Code.

Finally, I commit to aligning my behavior with the rules set forth in this Code, acknowledging the responsibilities associated with any violations of these rules.

Name and Surname:

Place and Date:

Signed:



**Organization, Management and Control Model  
ex D.L.GS 231/2001**

**General Part**





## **Table of Contents**

<b>1. PREAMBLE</b>	<b>4</b>
1.1. Definitions	4
1.2. Legislative Decree No. 231 of June 8, 2001 and its subsequent amendments and integrations	5
1.3. The crimes and sanctions envisaged in the Decree	7
1.4. The Guidelines	8
<b>2. ADOPTION OF THE MODEL</b>	<b>10</b>
2.1. Purpose of the Model	10
2.2. Structure of the Model	10
2.3. Recipients of the Model	11
2.4. Approval and modification of the Model	11
2.5. Implementation of the Model	12
2.6. Review of the Model	12
<b>3. THE ELEMENTS OF THE MODEL</b>	<b>12</b>
3.1. Control Principles	12
3.2. Code of Ethics	14
3.3. Organizational and Authorization System	15
3.4. Corporate Governance	16
3.5. The Supervisory Body	17
3.6. Information Flows to and from the Supervisory Body	18
3.7. The Map of Risk Areas and Controls	26
3.8. Protocols and Procedures System	27
3.9. Disciplinary System	27
3.10. Training Plan	27
3.11. Communication of the Model	28
3.12. Information to Collaborators and Partners	29
<b>4. INTRODUCTION TO THE SPECIAL PART</b>	<b>29</b>

### **Attachments:**

Annex 1 – Organizational Chart

Annex 2 – Catalogue of Crimes envisaged in the Legislative Decree 231/2001

Annex 3 – Code of Ethics

Annex 4 – Information Flows to the Supervisory Body

Annex 5 – Risk Assessment

Annex 6 – Gap Analysis

Annex 7 – Disciplinary System

Annex 8 – Statute of the Supervisory Body

Annex 9 – Procedures

Annex 10 – Special Part MOCG 231/01



## ORGANIZATION, MANAGEMENT AND CONTROL MODEL – EX D.LGS 231/2001

### 1.Preamble

#### 1.1. Definitions

In this document, the following expressions have the meanings set out below:

- **"Crime Risk activities"**: the process, operation, act, or the set of operations and acts that may expose the Company to the risk of sanctions pursuant to the Decree due to the commission of a Crime.
- **"CCNL"**: The National Collective Labor Agreement applicable to the Company's employees.
- **"Code of Ethics"**: the document, officially desired and approved by the Company's management as explanation of corporate policy, containing the general principles of behavior—i.e., recommendations, obligations, and/or prohibitions—that the Recipients must adhere to, and whose violation is sanctioned.
- **"D. Lgs. 231/2001" or "Decree"**: Legislative Decree No. 231 of June 8, 2001, on the "Discipline of administrative responsibility of legal entities, companies, and associations, including those without legal personality, under article 11 of Law No. 300 of September 29, 2000," published in the Official Gazette No. 140 of June 19, 2001, and subsequent amendments and integrations.
- **"Recipients"**: Corporate bodies (Directors and Auditors), employees, suppliers, agents, outsourcers, and other parties with whom the Company interacts in business relationships. Recipients are required to comply with the Model, the Code of Ethics, and the preventive protocols.
- **"Employees"**: All individuals in a subordinate employment relationship with the Company.
- **"Guidelines"**: The Guidelines for the construction of organizational, management, and control models as per D. Lgs. 231/2001, published by trade associations, which were considered in the preparation and adoption of the Model.
- **"Organizational, Management, and Control Model pursuant to D. Lgs. 231/2001" or "Model"**: The organizational, management, and control model considered by the corporate bodies to be suitable for preventing crimes and, therefore, adopted by the Company under Articles 6 and 7 of the Legislative Decree, to prevent the commission of crimes by senior or subordinate personnel, as described in this document and its annexes.
- **"Corporate Bodies"**: The Administrative Body and/or the Board of Statutory Auditors of the Company, depending on the context.
- **"Supervisory Body" or "OdV"**: The body established under Article 6 of the Legislative Decree, tasked with overseeing the functioning and compliance with the organizational, management, and control model, as well as its updating.
- **"Partner"**: Entities with whom the Company interacts in business relationships, specifically dealers who rely on a network of various entities, with or without their own legal autonomy, for the sale of products and/or services. As such, the Partner is a Recipient.
- **"Personnel"**: All individuals who have a working relationship with the Company, including employees, temporary workers, collaborators, interns, and freelancers engaged by the Company.
- **"Senior Personnel"**: Individuals referred to in Article 5, paragraph 1, letter a) of the Decree, who hold representation, administration, or management roles within the Company or an autonomous



organizational unit thereof; specifically, members of the Administrative Body, the Chairman, members of any Executive Committee, potential agents, and attorneys.

- **"Personnel under the direction of others"**: Individuals referred to in Article 5, paragraph 1, letter b) of the Decree, i.e., all personnel working under the direction or supervision of Senior Personnel.
- **"Public Administration" or "P.A."**: Public Administration refers to:
  - The State (or State Administration);
  - Public Entities, as defined by law, or entities subject to a public control system, state or other administration interference in the appointment and removal of administrators, and the administration of the entity itself. Such entities are characterized by public participation in management costs, or by the directive powers held by the State or other public administration over their bodies, or by institutional public funding.
  - **Public Official**: A person who exercises a "public legislative, judicial, or administrative function." Under criminal law, a public function is defined as an administrative function regulated by public law and authoritative acts.
  - **Public Service Officer**: A person who, in any capacity, performs a public service, defined as an activity regulated in the same manner as a public function but lacking the typical powers of such a function and excluding simple administrative tasks and purely material labor.
- **"Protocol"**: The organizational, physical, and/or logical measure provided by the Model to prevent the risk of committing crimes.
- **"Crimes" or "Crime"**: The set of crimes, or a single crime, envisaged in the D. Lgs. 231/2001 (as amended and integrated in the future).
- **"Disciplinary System"**: The set of sanctions applicable in case of violation of procedural and behavioral rules established by the Model.
- **"Company"**: Zilio Industries S.p.A.

## **1.2. Legislative Decree No. 231 of June 8, 2001, and Subsequent Amendments and Integrations**

Following a process initiated by the European Union, with the approval of Legislative Decree No. 231 of June 8, 2001, Italy introduced the administrative liability of entities arising from the commission of criminal offenses. The discipline of the Decree came into effect on July 4, 2001, introducing for the first time a specific form of liability for entities regarding certain crimes committed in their interest or to their advantage by individuals connected to the company. This liability does not replace the responsibility of the natural person who committed the criminal act but is in addition to it.

The new liability regime therefore involves punishing certain criminal offenses by impacting the entity's assets that benefited from the commission of the offenses. In case of an illegal act, a financial penalty is always applied, and in more severe cases, further serious measures are imposed, such as suspension or revocation of grants and licenses, ban from business operations, prohibition of contracting with Public Administration, exclusion or revocation of funding and contributions, prohibition of advertising goods and services, or even the receivership of the entity.

As mentioned, under Article 5 of the Decree, "the entity is responsible for crimes committed in its interest or for its benefit"; i.e., the entity is liable if it has obtained benefits from the illegal activity. The entity, however,



## ORGANIZATION, MANAGEMENT AND CONTROL MODEL – EX D.LGS 231/2001

will not be liable if the offenders acted solely in their own interest or in the interest of third parties. Additionally, under the same article, the criminal actions must be carried out:

- By individuals holding representation, administration, or management functions within the entity or an autonomous organizational unit, as well as those who de facto manage and control it;
- By individuals under the direction or supervision of the above-mentioned individuals.

However, the entity will not necessarily be liable for a Crime. It was considered appropriate to allow the entity to demonstrate in advance that it was not involved in the Crime. To this end, the adoption of behavioural models specifically tailored to the risk-crime is required, i.e. aimed at preventing, through the establishment of rules of conduct, the commission of certain Crimes. An essential condition for the entity to avoid responsibility is the effective implementation of the Models.

In other words, the entity's specific guilt arises when a crime committed by its body or subordinate is part of a business decision, or when the entity failed to adopt an organizational model capable of preventing the type of crime that occurred, or when there was insufficient or omitted supervision by the control body.

In this regard, Article 6 of the Decree stipulates that the entity will not be held liable for an offense if it can demonstrate that it adopted and effectively implemented, prior to the commission of the act, "organizational and management models suitable for preventing crimes of the type that occurred."

This provision also requires the establishment of an "internal control body" tasked with overseeing the operation, effectiveness, and compliance with the model, as well as its updating.

Therefore, the organizational models must meet the following requirements:

- Identify Crime risk activities;
- Provide specific protocols for preventing Crimes;
- Identify methods for managing financial resources to prevent Crimes;
- Require information obligations to the body responsible for controlling the functioning and compliance of the models;
- Implement an internal disciplinary system capable of sanctioning violations of the measures outlined in the model.

In conclusion, if Crimes are committed by Senior Personnel, the entity will not be liable if it can prove:

1. That the governing body adopted and effectively implemented, before the Crime occurred, an organizational and management model capable of preventing Crimes of the type that occurred;
2. That the task of overseeing the operation and compliance with the model, as well as its updating, was assigned to a body with autonomous powers of initiative and control (Supervisory Body);
3. That there was no failure or insufficient supervision by the control body regarding the model;
4. That the individuals committed the crime by fraudulently evading the model.

If the Crime was committed by individuals under the direction or supervision of Senior Personnel, the entity will only be liable if there was a failure in the obligations of direction and supervision, which will be excluded if the entity adopted, prior to the commission of the crime, an organizational, management, and control model capable of preventing Crimes of the type that occurred.



### 1.3. The Crimes and Sanctions

The entity's liability does not arise from the commission of any criminal offense by the aforementioned individuals but is limited to specific offenses defined in the Decree.

The types of crimes specified by the Decree include, but are not limited to:

1. *Illicit receipt of public funds, fraud to the detriment of the State, a public entity, or the European Union, computer fraud to the detriment of the State, or a public entity, and fraud in public supplies (Article 24 D.Lgs. n 231/2001)*
2. *Computer crimes and illegal data processing – (Article 24-bis D.Lgs. n 231/2001).*
3. *Organized crime – (Article 24-ter D.Lgs. n 231/2001).*
4. *Embezzlement, extortion, inducement to provide or promise benefits, corruption, and abuse of office – (Article 25 D.Lgs. n 231/2001).*
5. *Counterfeiting of money, public credit cards, stamp duties, and signs of recognition – (Article 25-bis D.Lgs. n 231/2001).*
6. *Crimes against industry and commerce – (Article 25-bis.1 D.Lgs. n 231/2001).*
7. *Corporate crimes – (Article 25-ter D.Lgs. n 231/2001).*
8. *Terrorist crimes or crimes aimed at subverting democratic order – (Article 25-quarter D.Lgs. n 231/2001).*
9. *Female genital mutilation – (Article 25-quater.1 D.Lgs. n 231/2001).*
10. *Crimes against individual personality – (Article 25-quinquies D.Lgs. n 231/2001).*
11. *Market abuse crimes – (Article 25-sexies D.Lgs. n 231/2001).*
12. *Other market abuse crimes (related to financial instruments) – Article 187-quinquies TUF (Testo Unico della Finanza).*
13. *Manslaughter and grievous bodily harm committed by violating safety and health regulations – (Article 25-septies D.Lgs. n 231/2001).*
14. *Receiving stolen goods, money laundering, and self-laundering of illicit funds or goods – (Article 25-octies D.Lgs. n 231/2001).*
15. *Crimes related to payment instruments other than cash – (Article 25-octies 1 D.Lgs. n 231/2001).*
16. *Other crimes related to non-cash payment instruments – (Article 25-octies 1, comma 2 D.Lgs. n 231/2001).*
17. *Copyright infringement crimes – (Article 25-novies D.Lgs. n 231/2001).*
18. *Inducement to avoid giving statements or to provide false statements to the judiciary – (Article 25-decies D.Lgs. n 231/2001).*
19. *Environmental crimes – (Article 25-undecies D.Lgs. n 231/2001).*
20. *Employment of third-country nationals in irregular situations – (Article 25-duodecies D.Lgs. n 231/2001).*

21. *Racism and xenophobia – (Article 25-terdecies D.Lgs. n 231/2001).*
22. *Fraud in sports competitions, illegal gambling, and illegal gambling devices – (Article 25-quaterdecies D.Lgs. n 231/2001).*
23. *Tax crimes – (Article 25-quinquesdecies D.Lgs. n 231/2001).*
24. *Smuggling – (Article 25-sexiesdecies D.Lgs. n 231/2001).*
25. *Crimes against cultural heritage – (Article 25-septiesdecies D.Lgs. n 231/2001).*
26. *Laundering of cultural goods and destruction or looting of cultural and landscape heritage – (Article 25-duodecimes D.Lgs. n 231/2001).*
27. *Transnational crimes – (Law 146/2006).*

The detailed list of crimes envisaged by the Decree is attached to this Model (Annex No. 1 of this Model). It should be noted that, regardless of any Administrative Responsibility of the entity, anyone who commits one of the Crimes mentioned above will still be subject to prosecution for the illegal conduct they have engaged in. Article 9, paragraph 1, of the Decree outlines the sanctions that can be imposed on the entity for administrative offenses derived from criminal acts, namely:

1. financial penalties;
2. prohibitory sanctions;
3. seizure;
4. publication of the ruling.

In particular, the “prohibitory sanctions” outlined are:

- prohibition from exercising the activity;
- suspension or revocation of licenses, permits, or grants relevant to the commission of the offense;
- ban on contracting with the Public Administration, except to obtain public services;
- exclusion from incentives, financing, contributions, or subsidies, and possible revocation of those already granted;
- prohibition on advertising goods or services;
- receivership.

#### **1.4. Guidelines**

Article 6, paragraph 3, of Legislative Decree No. 231/01 establishes that “organizational and management models may be adopted, ensuring the needs of paragraph 2, based on codes of conduct drawn up by representative associations of entities, communicated to the Ministry of Justice, which, in conjunction with the competent ministries, can issue observations on the suitability of the models to prevent crimes within thirty days.”

Confindustria has developed and communicated to the Ministry the “Guidelines for constructing organizational, management, and control models under Legislative Decree No. 231/2001,” referring only to crimes against the Public Administration, which specify the operational steps, listed below, that the company

must take to implement a risk management system consistent with the requirements set by Legislative Decree 231/2001:

- ▶ mapping of the risk areas within the company. Once the types of crimes affecting the company are identified, the activities in which such crimes can be committed are pinpointed, considering the possible ways of carrying out illegal conduct within specific company activities;
- ▶ specific protocols aimed at planning and implementing the company's decisions related to preventing Crimes. The components of a preventive control system that must be implemented to ensure the model's effectiveness are:
  - a code of ethics that defines ethical principles regarding behaviors that may constitute offenses under Legislative Decree 231/2001;
  - an organizational system that defines the hierarchy of company positions and responsibilities for carrying out activities;
  - an authorization system that grants internal authorization powers and signing powers in line with the adopted organizational system;
  - operational procedures that regulate the main business activities, particularly the risky processes and financial resource management;
  - a management control system that promptly highlights critical situations;
  - a communication and training system for employees to ensure the proper functioning of the model;
- ▶ the identification of a Supervisory Body (OdV), equipped with independent powers of initiative and control, responsible for monitoring the functioning and compliance of the models through periodic checks and ensuring updates when significant violations are discovered, or when changes occur in the organization or activities;
- ▶ specific informational obligations towards the Supervisory Body on key company matters, particularly those considered risky;
- ▶ specific informational obligations from the Supervisory Body to the company's top management and control bodies;
- ▶ a disciplinary system capable of sanctioning non-compliance with the model's provisions.

The components of the control system must be inspired by the following principles:

- verifiability, documentation, consistency, and congruence of every operation;
- separation of functions (no one should manage an entire process autonomously);
- documentation of controls.

In preparing the model, Zilio Industries S.p.A. has taken into account not only the legislation outlined in Legislative Decree No. 231/01, but also the principles expressed by Confindustria in the Guidelines approved, in their latest version, by the Ministry of Justice.

## **2. ADOPTION OF THE MODEL**

### **2.1 Purpose of the Model**

This Model is intended to:

- a) promote and enhance an even stronger ethical culture within the company, with a focus on fairness and transparency in business operations;
- b) ensure that all individuals acting by and on behalf of Zilio Industries S.p.A. are aware that violations of the provisions set out may result in criminal and administrative sanctions, not only for themselves but also for the company;
- c) emphasize that such forms of illegal behavior are strongly condemned by Zilio Industries S.p.A. because they are, even if the company could seemingly benefit from them, still contrary to legal provisions and the ethical-social principles the company adheres to in carrying out its business mission;
- d) introduce a mechanism to establish a permanent process of analyzing company activities, aimed at identifying areas where the crimes outlined in the Decree could potentially occur;
- e) introduce control principles to which the organizational system must adhere in order to effectively prevent the risk of committing the crimes outlined in the Decree in the specific activities identified during the analysis of sensitive areas;
- f) introduce a disciplinary system capable of sanctioning non-compliance with these control principles and, in particular, the measures outlined in this Model;
- g) establish the Supervisory Body (OdV) with the task of overseeing the proper functioning and compliance with the Model and ensuring its updating.

### **2.2 Structure of the Model**

The Model consists of a General Part and a Special Part, divided into distinct chapters based on the various business processes considered sensitive.

This General Part, starting from a summary overview of the Decree's content, aims to define the structure of the Model, specifying its purposes and functions, identifying the Supervisory Body, establishing an information flow system, and a disciplinary system capable of sanctioning non-compliance with the Model.

The Special Part focuses on the activities performed by Zilio Industries S.p.A. and identifies the business processes where the Crimes sanctioned by Legislative Decree No. 231/2001 could be committed. It aims to regulate the conduct of company personnel, whether senior or under supervision, to prevent the commission of criminal offenses through the development of specific rules of conduct, protocols, and procedures within the identified risk areas, based on the categories of crimes outlined in the Decree. The Model, being adopted by the company's top management (in this case, the Administrative Body), is to be considered a company directive by which the top management establishes the organizational structure and controls for overseeing risk processes.

The company's Administrative Body is then responsible for integrating the Model, adding new criminal offenses to the Special Part in response to any further legislative interventions on crimes envisaged by the Decree (see paragraph 2.5).



### **2.3 Recipients of the Model**

The rules contained in this Model apply to:

- Individuals involved in management, administration, direction, or control functions in the company.
- Employees, consultants, collaborators, and third parties who act on behalf of the company in activities that are considered "at risk of crime."

These Recipients must comply with the Model's provisions, fulfilling duties of loyalty, fairness, and diligence in their relationships with the company.

### **2.4 Approval and Modification of the Model**

Organizational models, pursuant to Article 6, paragraph 1, letter a) of the Decree, are acts issued by the Administrative Body in its collegial capacity. Therefore, the approval of this Model is the exclusive prerogative and responsibility of the Administrative Body of Zilio Industries S.p.A. (hereinafter also referred to as the "Administrative Body"). Any modifications and additions to the Model is the sole responsibility of the Administrative Body, even upon the recommendation of the Supervisory Body (OdV), with regard to the following elements:

- The modification of the document "Bylaws of the Supervisory Body";
- The provision of the necessary powers to the Supervisory Body to carry out its oversight functions;
- The provision of an appropriate budget and resources to the Supervisory Body for the correct performance of its tasks;
- The inclusion/integration of principles from the Code of Ethics;
- Modifications or additions to the Disciplinary System;
- The adjustment and update of this Model.

Modifications/additions to the Map of risk areas and organizational procedures, which are considered an integral part of the Model, can be approved by the Administrative Body upon the proposal of the Supervisory Body, which is tasked with ensuring the continuous updating of the Model and formulating proposals for modifications.

The Administrative Body must then be informed of any change made.

Operating procedures are control elements for sensitive activities, identified following the Mapping of risk areas. Therefore, any proposal or suggestion for integration and modification of the Model's procedures must be communicated to the Supervisory Body, which will also inform the Administrative Body in the context of the annual/semi-annual information report.

Substantial modifications and/or additions concerning the organizational system and, thus, the company's organizational chart, must be approved by the Administrative Body.

Regarding the process of modification and updating of the Mapping of risk areas, reference is made to the protocol described in the specific section of this Model.

As clarified by the Guidelines, the Administrative Body, even with the establishment of the Supervisory Body pursuant to the Decree, retains all the powers and responsibilities provided by the Civil Code and the



Company's Bylaws, to which are now added those related to the adoption and effective implementation of the Model, as well as the functioning of the Supervisory Body.

## **2.5 Implementation of the Model**

The implementation of this Model is a dynamic process that begins with the approval of the Model by the Administrative Body.

For the implementation phase of the Model, the Administrative Body and the Company Representative, supported by the Supervisory Body (OdV) within the limits of its institutional duties, will be responsible, within their respective areas of competence, for the implementation of the various elements of the Model, including the organizational procedures.

In any case, the Company wishes to reaffirm that the correct implementation and the control of compliance with company provisions, and therefore with the rules contained in this Model, are an obligation and duty of all employees, and in particular of each Head of Department/Function/Service or Office, who is entrusted with the primary responsibility for monitoring activities within their area of competence, with particular attention to those at risk.

## **2.6 Review of the Model**

- The 231 Model must be reviewed annually to ensure its effectiveness and adequacy.
- The review is necessary in response to:
  - a) Legislative changes regarding corporate responsibility for Crimes.
  - b) Organizational changes within the Company.
  - c) Significant violations of the 231 Model or effectiveness issues.

The review process of 231 Model involves

- the Administrative Body;
- the OdV;
- relevant company personnel.

## **3. Elements of the Model**

### **3.1 Control Principles**

Zilio Industries S.p.A., with this Model, intends to give concrete application to the control system centred on the principles represented below, as also requested by Confindustria in its Guidelines

Within each identified activity at risk, the Company must put in place specific controls. The degree of control that Zilio Industries S.p.A. has established to implement for each risk activity is in function, in addition to an evaluation in terms of cost-benefit, of the risk threshold considered acceptable by the entity itself for that specific activity.

To this end, the Company has taken as its control framework the one that today represents the commonly accepted international reference as a model for governance and internal control, i.e. the well-known 'CoSO Report', produced in the USA in 1992 by Coopers & Lybrand (now PricewaterhouseCoopers) on behalf of the Committee of Sponsoring Organisations of the Treadway Commission (with the Institute of Internal Auditors

and the AICPA among the Sponsoring Organisations), which adopted and proposed it as a reference model for the control system of companies. National regulations in all major countries have been inspired by it.

Based on this 'reference framework', the elements that make it up are set out below, with a brief description aimed at defining, for the purposes of this Model, its substance and characteristics. The elements listed and described below have been placed at the basis of the assessment of the controls in place in the map of areas at risk and referred to in the Special Part:

- ▶ regulation: sensitive processes/activities must be regulated by specific corporate provisions duly formalised and communicated to all personnel. For the purposes of this Model, said regulation may take place by means of
  - behavioural rules contained in the Code of Ethics and in the Special Part of this Model;
  - organisational procedures;
- ▶ communication: company provisions and rules must be promptly and formally communicated to all recipients, so that the burden of proof can be discharged in the event of disputes against persons who engage in conduct in violation of them
- ▶ traceability: the activities of which the corporate processes are composed, and in particular those of control, must be traced in such a way as to allow verification also a posteriori (e.g. *auditing/testing*). This element is better guaranteed by the use of specific application systems (e.g.: management software);
- ▶ *reporting*: the control system must be supported by suitable *reporting* systems that allow top management to be aware of the activities performed and those planned, thanks to structured *reports* that guarantee the reliability of the information contained therein, so as to be able to guide the strategic choices of top management;
- ▶ monitoring: a valid system of controls must be constantly monitored by a specific independent function appointed for this purpose, which checks the correct application of and compliance with the rules adopted by the Company
- ▶ reaction to violations: finally, the control system must be supplemented by an effective system of sanctions designed to ensure compliance with the rules adopted.

Further control principles, which must be ensured in all "at-risk activities," consist of the following:

- Guarantee integrity and ethics in carrying out activities, through the establishment of appropriate behavioral rules aimed at regulating each specific activity considered at risk (for example, in relations with Public Administration);
- Formally define the tasks and responsibilities of each Department/Function/Service or Office involved in at-risk activities;
- Assign decision-making responsibilities proportionate to the level of responsibility and authority conferred;
- Define, assign, and correctly communicate authorizing and signing powers, specifying approval thresholds for expenses where required, so that no individual is given unlimited discretionary powers;

- Ensure the principle of role separation in managing processes, assigning different individuals to the crucial phases of the process, particularly the authorization, execution, and control phases;
- Regulate at-risk activities, for example through specific procedures, providing appropriate control points (checks, reconciliations, balances, informational mechanisms, etc.);
- Ensure the verifiability, documentability, consistency, and appropriateness of every operation or transaction. To this end, activity traceability must be guaranteed through adequate documentation that allows for control at any time. It is important that for each operation, it is easy to identify who authorized the operation, who carried it out, who registered it, and who conducted the control over it. The traceability of operations is more reliably ensured through the use of information systems capable of managing the operation while ensuring compliance with the above requirements;
- Ensure the documentation of the controls performed. To this end, the procedures by which controls are carried out must guarantee the ability to trace the control activities, allowing for the assessment of the consistency of the methodologies applied and the correctness of the results obtained;
- Ensure the presence of appropriate reporting mechanisms that allow for systematic reporting by the personnel performing the at-risk activities (written reports, memos, etc.);
- Guarantee the reliability of financial reporting to the company's senior management;
- Provide moments of control and monitoring over the correctness of activities performed by individual Departments/Functions within the process (compliance with rules, proper use of signing and spending powers, etc.).

The principles described above must be adhered to in all company processes, particularly in processes identified as sensitive in the mapping attached to this Model. It will be the responsibility of the Supervisory Body (OdV) to verify that the competent company functions promptly verify and adjust their processes to the principles outlined above.

The outcome of this verification and adjustment process must be subject to specific periodic reporting by the company's Departments/Functions within their area of responsibility, according to the methods and timeline established by the OdV.

### **3.2 Ethical Code**

In compliance with good governance criteria, Zilio Industries S.p.A. has adopted its own Code of Ethics (Annex 3 to this Model) with the goal of ensuring the adherence to certain principles and rules of conduct that contribute to the prevention of crimes as set out by Legislative Decree no. 231/2001.

The Code of Ethics adopted by the Company is a general document as it contains a series of behavioral principles (such as ethical standards applied to professional activity) that the Company recognizes as its own and calls for the observance of by all its Employees and by all those who, even externally, act in its interest or to its advantage (Recipients).

The Code of Ethics serves as a reference point for directing the behavior of Recipients and those acting in the interest or to the benefit of the Company, in the absence of specific preventive Protocols.

The Company is committed to effectively disseminating, internally and to those who collaborate with it, the information regarding the regulatory discipline and the behavioral and procedural rules to be followed, to ensure that business activities are carried out in compliance with the ethical principles outlined in the Code





of Ethics. The latter is periodically updated and may be expanded to incorporate legislative changes or modifications to the Company's operations and/or internal organization.

#### Responsibility

Any modification of the Code of Ethics is the exclusive responsibility of the Administrative Body.

#### Recipients

The Code of Ethics applies to both individuals directly employed by the Company, to whom Zilio Industries S.p.A. can require adherence to the ethical provisions, and to consultants, collaborators, agents, attorneys, and third parties who may perform activities on behalf of the Company.

Therefore, the Code of Ethics is directly applicable to those individuals for whom adherence to ethical principles can be contractually agreed. It is the responsibility of the Supervisory Body (OdV) to identify and assess, with the support of the relevant company functions, the appropriateness of inserting specific clauses in contracts regulating the relationship with these parties, in light of the company's activities that are potentially exposed to criminal risks.

In the event that any provision of the Code of Ethics conflicts with provisions contained in internal regulations or procedures, the Code will prevail.

#### Control

The Supervisory Body (OdV) is responsible for overseeing the functioning and compliance with the Code of Ethics in relation to the specific activities of the Company, and is tasked with promptly communicating any inconsistencies or necessary updates to the Administrative Body.

Any doubts regarding the application of the principles and rules contained in the Code of Ethics must be promptly discussed with the OdV. Similarly, anyone becoming aware of violations of the Code of Ethics or other events that may affect its scope or effectiveness must promptly report them to the OdV.

### **3.3 Organizational and Authorization System**

#### The Organizational System

As clarified by the Guidelines, the organizational system must be sufficiently formalized and clear, especially regarding the allocation of responsibilities, lines of hierarchical dependence, and the description of duties, with specific provisions for control principles, such as, for example, the separation of functions.

The organizational structure of Zilio Industries S.p.A. is formalized in a company organizational chart (Annex 3 to this Model), which identifies the roles of each organizational unit, the lines of hierarchical dependence, and the functional relationships between the various positions that make up the structure.

The company organizational chart, which graphically represents the organizational structure of the Company, must be a document issued by the Administrative Body containing all existing Departments/Functions/Services or Offices.

#### Authorization System and Delegation of Powers

The Guidelines also clarify that authorization and signing powers must be assigned in alignment with the defined organizational and managerial responsibilities, specifying, when required, approval thresholds for expenses, especially in areas considered "at-risk" of crime.



The Administrative Body of Zilio Industries S.p.A. is the body responsible for formally conferring and approving delegations and signing powers, assigned in alignment with defined organizational and managerial responsibilities, specifying approval thresholds for expenses.

The powers thus conferred are periodically updated in response to organizational changes within the Company. To this end, information flows must be established for the update of the Model:

1. From the Administrative Body to the OdV;
2. From the HR Manager to the OdV.

### **3.4 Corporate Governance**

Zilio Industries S.p.A. adopts a traditional governance structure, with the presence of an Administrative Body and a Board of Statutory Auditors, whose members are appointed by the Shareholders' Meeting.

The following sections address the different actors present in the organizational and control system adopted by the Company, specifying their roles and interrelationships, also by referring to specific documents.

#### Administrative Body

The Administrative Body (also referred to as the "Administrative Body") of the Company is composed of a sole Director.

The aspects regarding the appointment methods of directors, the requirements of integrity, professionalism, and independence, as well as the functioning (meetings, resolutions, representation of the company), are governed within the Statute of Zilio Industries S.p.A., to which reference is made.

#### Board of Statutory Auditors

The Board of Statutory Auditors (also referred to as the "CdS") of Zilio Industries S.p.A. consists of 3 standing members and 2 alternate members.

According to Article 2403 of the Italian Civil Code, the CdS "supervises compliance with the law and the statute, the observance of the principles of proper administration, and in particular the adequacy of the organizational, administrative, and accounting structure adopted by the company and its effective functioning."

The role of the CdS, according to the law, is therefore to control the administration. In particular, the CdS must:

- Verify that the Administrative Body informs the CdS, with the frequency established by the Statute, about the general management trends and major operations;
- Assess, based on the information received from the relevant bodies, the adequacy of the Company's organizational, administrative, and accounting structure;
- Ensure compliance with Article 2391 of the Civil Code in the event that the Sole Director has an interest in a particular operation, and ensure that the Administrative Body properly justifies the reasons for the operation (conflict of interest situations);
- Ensure that strategic, industrial, and financial plans are drafted, at least when deemed appropriate (judgment of opportunity);

- Supervise the execution of shareholders' resolutions, at least to ensure that there is no contradiction between those resolutions and the management actions;
- Supervise the actual examination by the directors of the functioning of the OdV pursuant to Legislative Decree no. 231/2001;
- Supervise the correct functioning of the administrative-accounting system, in terms of the procedures and methods adopted (adopted schemes, filing, and publication), the completeness and clarity of the information provided in the notes to the financial statements and the management report, and the accurate reflection of individual business cycle processes in the administrative-accounting system itself. Thus, the CdS is tasked with providing an analysis of the Company's performance and expressing its views on how the financial statements reflect that performance. Additionally, the CdS is responsible for a detailed analysis of the overall data in the financial statements and their correct recording, as this body fulfills the obligations arising from the legal audit of the accounts.

Regarding the evaluation of the organizational structure, it is important to clarify that the "organizational structure" refers to the "set of directives and procedures established to ensure that decision-making power is assigned and effectively exercised with an appropriate level of competence and responsibility." The adequacy requirements for such a structure are summarized as follows:

- compliance with the size of the Company, the nature, and the means of achieving the corporate purpose;
- company organizational chart with clear identification of lines of responsibility;
- the direction of the company is effectively exercised by the Administrative Body;
- documentation of company directives and procedures and their actual knowledge;
- personnel with the appropriate competence to carry out the assigned functions.

For coordination with other controlling bodies, the following is established:

- the CdS evaluates the proposals formulated by the auditing firm for their assignment and the results presented in the report and the letter of suggestions prepared by the appointed auditor;
- the CdS maintains information flows with the various control actors (i.e., Administrative Management).

For aspects relating to the appointment and functioning of the CdS and for all matters not specified in this section, reference is made to what is defined in the "Statute of Zilio Industries S.p.A."

### **3.5 The Supervisory Body**

Article 6, paragraph 1, letter b) of Legislative Decree No. 231/2001 provides that one of the essential requirements for exemption from liability arising from the commission of crimes is the establishment of a supervisory body (hereinafter also referred to as the "OdV") endowed with autonomous powers of initiative and control, tasked with overseeing the operation and compliance of the Model and ensuring its updates.

The Administrative Body, in selecting the Supervisory Body, has deemed it appropriate to evaluate, for each of the proposed solutions, the existence of the following characteristics:

- Autonomy and independence of the body and its members, understood as:
  - autonomous functional subjectivity of the organization itself;

- possession of independent powers of initiative and control;
- absence of operational tasks;
- placement in a staff position within the Administrative Body;
- ability to communicate directly with the Board of Statutory Auditors;
- Professionalism, understood as a body of knowledge, adequate specialized competence in audit and consulting activities, tools and techniques that the Body, through its members, must possess;
- Continuity of action, achieved by the support of an internal person dedicated to the monitoring activities of the Model.

Therefore, as part of aligning its organizational and control system with the provisions of Legislative Decree No. 231/2001, the Company has established a single-member supervisory body tasked with monitoring the adequacy and functioning of the present Model.

Regarding the characteristics, duties, and operation of the Supervisory Body, refer to the following paragraph and the document “Bylaws of the Supervisory Body” (Appendix No. 8 of this Model), approved by the Administrative Body, and the document “Regulations of the Supervisory Body,” which will be adopted by the Supervisory Body itself.

### **3.6 Information Flows to and from the Supervisory Body**

The Supervisory Body periodically reports the results of its activities to the Administrative Body and the Board of Statutory Auditors, particularly regarding the implementation of the Model and any issues related to it.

Regarding this form of reporting to the Administrative Body and the Board of Statutory Auditors, the Supervisory Body prepares a summary report of the Supervisory Body's actions (activities performed in total, activities not performed due to justified reasons related to time and resources, necessary and/or appropriate corrective/improvement interventions to the Model and their status of implementation) on the results achieved by the activities performed and the work plan for the subsequent reference period (audit plan).

Meetings with the corporate bodies to which the Supervisory Body reports must be recorded, and copies of the minutes are kept by the Body in the appropriate archive following the procedures and timelines established by the Body itself.

The Supervisory Body may be summoned at any time by the aforementioned bodies and may, in turn, request such a meeting to report on the functioning of the Model and specific situations, both directly and indirectly related to the application of the Model and/or the implementation of the Decree.

The Supervisory Body must also coordinate with the relevant technical structures within the Company for various specific areas.

#### **Information Flows to the Supervisory Body**

Article 6, paragraph 2, letter d) of Legislative Decree No. 231/01 mandates the inclusion of informational obligations in the "Organizational Model" towards the Body responsible for overseeing the functioning and compliance of the Model.

The obligation for a structured information flow is designed as a tool to ensure the supervisory activity over the effectiveness and efficiency of the Model and for the possible retrospective verification of the causes that made the commission of the crimes outlined in the Decree possible.

The information provided to the Supervisory Body aims to enhance its planning activities for controls and does not imply a detailed and systematic verification of all the phenomena represented. The obligation for a structured information flow, aimed at the business functions at risk of committing a crime, must concern the following two macro-areas:

1. The periodic results of the control activities undertaken to implement the models (summary reports of the activities carried out, monitoring activities, final indices, etc.);
2. Anomalies or irregularities found within the available information (a fact that may not be relevant when considered alone could assume a different evaluation when considering its repetition or the extent of the area where it occurred).

### Types of Information Flows

There are various types of communications to the Supervisory Body:

- a) Event-driven: information flows that occur when a specific event arises that must be reported to the Supervisory Body;
- b) Periodic: information flows on a periodic basis established by the Company;
- c) Whistleblowing: "whistleblowing" refers to a report made to the Supervisory Body concerning violations related to the crimes specified under Legislative Decree No. 231/01, as well as violations of this Model.

In particular, the following information must be promptly transmitted to the Supervisory Body by each relevant company function:

#### a) Event-driven Flows:

- Actions and/or news from law enforcement or any other authority indicating that an investigation has been initiated for the crimes under the Decree, even if against unknown parties;
- Decisions related to requests, disbursements, and use of public funding;
- Any violation of the Model and its constituent elements and any other aspect potentially relevant to the application of Legislative Decree No. 231/2001;
- Delegations regarding safety and appointments of the RSPP and competent doctor;
- Any violations by personnel regarding safety regulations;
- Any event, act/omission that may harm the guarantee of worker protection and any other aspect related to anti-accident measures potentially relevant for the application of Article 25-septies of Legislative Decree 231/2001;
- Any impediment to the exercise of the RSPP's, RLS's (Worker Safety Representative), and competent doctor's duties to ensure subsequent decisions are adopted;
- In case of administrative inspections related to the obligations under Legislative Decree 81/2008, any inspection activity, as well as the findings from the supervisory authority;

- Legal assistance requests made by managers and/or employees under investigation for crimes under the Decree;
- All disciplinary proceedings carried out and any sanctions imposed, or reasoned decisions to archive disciplinary proceedings;
- Any modification and/or integration to the delegation and procurement systems;
- The existence of company activities perceived as lacking appropriate and/or adequate regulation (total or partial absence of specific regulation, inadequacy of the Code of Ethics principles and/or operational procedures, etc.);
- Any issuance, modification, and/or integration carried out or deemed necessary to the operational procedures and the Code of Ethics.

***b) Periodic Flows:***

- A report from the RSPP regarding the results of scheduled and surprise inspections;
- The program of courses and training activities related to applicable accident prevention regulations;
- A report from the RSPP concerning compliance with contracts with contractors or self-employed workers;
- A copy or summary of the minutes from the annual meeting between the employer, RSPP, and the competent doctor;
- A copy of the approved financial statement, including the Notes to the Financial Statements and the Management Report, along with the Certification Report prepared by the auditing company;
- A detailed report from each function's responsible on the implementation status of the Model and its control principles, with the periodicity and standard contents of this report to be specifically determined and communicated by the Supervisory Body to all function heads.

The Supervisory Body acts to protect whistleblowers against any form of retaliation, discrimination, or penalization, while also ensuring the confidentiality of the whistleblower's identity, subject to legal obligations and the protection of the rights of the Company or the persons involved, as well as the reputation of the person(s) reported.

In the procedure for Information Flows to the Supervisory Body (Appendix 4 to the Model), the specific information flows and the responsible function will be outlined. The periodicity of such flows is determined by the Company based on the relevant function and the type of communication.

***c) Whistleblowing***

***Reports of potential illegal acts (so-called whistleblowing)***

On March 10, 2023, Legislative Decree 24/2023 was published for the implementation of Directive (EU) 2019/1937 of the European Parliament and Council, dated October 23, 2019, regarding the protection of persons reporting violations of Union law and containing provisions for the protection of those reporting violations of national regulations ("Whistleblowing Decree").

This decree regulates the protection of individuals who report violations of national or EU law that harm the public interest or the integrity of public administration or private entities, which they have become aware of in a public or private workplace context.

Moreover, with reference to Legislative Decree 231/2001, this decree, by collecting all the material regarding reports of illegal conduct, has amended paragraph 2-bis and repealed paragraphs 2-ter and 2-quater of the mentioned decree.

### Reporting Subjects

With reference to the individuals who, in the private sector, can make reports pursuant to Legislative Decree 24/2023, the provisions of this decree apply to the following subjects:

- Subordinate workers of private sector entities, including those whose employment relationship is governed by Legislative Decree No. 81 of June 15, 2015, or Article 54-bis of Decree-Law No. 50 of April 24, 2017, converted, with modifications, by Law No. 96 of June 21, 2017;
- Self-employed workers, including those referred to in Chapter I of Law No. 81 of May 22, 2017, as well as those with a collaboration agreement as per Article 409 of the Civil Procedure Code and Article 2 of Legislative Decree No. 81 of 2015;
- Workers or collaborators who carry out their work at entities that provide goods or services or perform works for third parties;
- Freelancers and consultants;
- Volunteers and interns, both paid and unpaid;
- Shareholders and individuals holding administrative, management, control, supervision, or representation functions, even when such functions are exercised de facto.

The protections for whistleblowers provided by Legislative Decree 24/2023 also applies if the report, complaint to the judiciary or auditing authorities, or public disclosure of information occurs in the following cases:

- a) when the legal relationship with the entity has not yet started, if information about violations was acquired during the selection process or other pre-contractual phases;
- b) during the try-out period;
- c) after the termination of the legal relationship, if the information about violations was acquired during the relationship itself.

Finally, the protections provided by the aforementioned decree also apply to:

- a) Facilitators (the decree defines the facilitator as “a person who assists a whistleblower in the reporting process, operating within the same working context, and whose assistance must remain confidential”);
- b) Persons within the same working context as the whistleblower, the person who made a complaint to the judicial or auditing authorities, or the person who made a public disclosure, and who are closely related by emotional or family ties up to the fourth degree;
- c) Colleagues of the whistleblower or the person who made a complaint to the judicial or auditing authorities, or made a public disclosure, working in the same workplace and maintaining a regular relationship with them;
- d) Entities owned by the whistleblower or the person who made a complaint to the judicial or auditing authorities, or made a public disclosure, or for which these individuals work, as well as entities operating in the same working context.

### Scope of Application (Objective)

From an objective perspective, the new regulations apply to violations of national and EU legislative provisions that harm the public interest or the integrity of public administration or private entities, of which whistleblowers become aware in a public or private work context.

In particular, reports can concern the following violations:

a. *Violations of National Legislative Provisions*

This category includes criminal, civil, administrative, or accounting offenses, other than those specifically identified as violations of EU law, as well as:

- Crimes related to the application of Decree 231;
- Violations of the organizational and management models provided for in Decree 231, which are also not related to violations of EU law as defined below.

b. *Violations of European Legislation*

This includes:

- Offenses committed in violation of EU legislation listed in Annex 1 of the Decree and all national provisions implementing it (even if not explicitly listed in the annex). It is specified that the provisions in Annex 1 should be understood as a dynamic reference and must be adjusted to the evolving legislation. Specifically, this includes violations in the following sectors: public procurement; financial markets and products, prevention of money laundering and terrorism financing; product safety and compliance; transport safety; environmental protection; nuclear safety; food safety and animal health; public health; consumer protection; protection of privacy and data security; security of networks and information systems. For example, environmental crimes such as the discharge, emission, or release of dangerous materials into air, soil, or water, or the illegal collection, transport, recovery, or disposal of hazardous waste;
- Acts or omissions that damage the financial interests of the European Union (Article 325 of the TFEU regarding fraud and illegal activities that harm the financial interests of the EU), as identified in EU regulations, directives, decisions, recommendations, and opinions. For example, fraud, corruption, and any other illegal activity related to EU expenditures;
- Acts or omissions related to the internal market that undermine the free movement of goods, people, services, and capital (Article 26(2) of the TFEU). This includes violations of EU laws regarding competition, state aid, business taxation, and mechanisms aimed at obtaining a tax advantage that undermines the applicable business tax regulations;
- Acts or behaviors that nullify the objectives or purpose of EU provisions in the sectors listed above. This includes abusive practices, as defined by the European Court of Justice, such as a dominant company using abusive pricing practices or anti-competitive behaviors that undermine fair market competition.

For the private sector, reports can concern violations of national regulations only with reference to crimes under Decree 231 and violations of the Organizational Model 231, as well as those related to European law in the specified areas. Secondly, the following reports are excluded from the scope of the new regulations:

- Personal Interest of the Whistleblower: Reports related to personal work relationships, such as disputes, discrimination, interpersonal conflicts, or data processing issues within an individual's work relationship, provided there is no violation of public interest or the integrity of the private entity or public administration, as the new regulations aim to protect the integrity of the legal entity and address situations where actions in the public and private sectors deviate from their intended purposes or hinder proper functioning.

Reports based solely on the whistleblower's personal interest will not be considered as whistleblowing and can be treated as regular reports where appropriate.

In fact, it is possible that companies, especially the more structured ones, already contemplate procedures and channels for the internal reporting of violations that do not fall within the scope of the whistleblowing discipline, but which are relevant in that they violate principles or requirements





contained, for example, in the Code of Ethics or the Staff Regulations. Therefore, such violations may be reported through the procedures already previously adopted by the entity or which the entity intends to adopt;

- National Security and Defense;
- Reports already regulated in specific sectors, for which specialized reporting regulations continue to apply (e.g., financial services, money laundering, terrorism, transport security, environmental protection).

This is without prejudice to the rules on: (i) classified information; (ii) medical and forensic secrecy; (iii) secrecy of court deliberations; (iv) rules of criminal procedure on the obligation of secrecy of investigations; (v) provisions on the autonomy and independence of the judiciary; (vi) national defence and public order and security; (vii) as well as the exercise of the right of workers to consult their representatives or trade unions.

#### Reporting Channels

To facilitate compliance with reporting obligations, Zilio Industries S.p.A. has set up various channels through which whistleblowers can make reports. The Company has established an internal reporting channel to ensure the confidential and effective handling of reports. The available reporting options include:

- Written form, via an online platform;
- Oral form, through voice messages on the same online platform;
- In-person meetings between the Whistleblowing Manager and the Whistleblower, upon request.

Whistleblowers may also use external reporting channels when conditions outlined by law apply.

In line with applicable regulations, Zilio Industries S.p.A. guarantees the possibility of anonymous reporting, provided the information is adequately detailed and verifiable. Although anonymous reports can be accepted and processed, the company encourages and promotes identified reports, as these are generally more effective and are encouraged wherever possible. However, anonymous whistleblowers are advised, when possible, to provide supporting evidence or as much detail as possible.

#### a) Internal Reporting Channel: Online Platform

The internal reporting channel used by Zilio Industries S.p.A. allows for both written and oral reports, including anonymous ones. The system is based on an advanced web platform, separate from the company's internal IT systems, hosted on an independent server, and meets all applicable regulatory requirements. The platform is accessible via a link available on the company's website (also reported in the section on 'information flows').

#### a.1. Written Report

Upon accessing the platform, in the case of anonymous reporting, the whistleblower enters the observed violation into the "reporting" section, filling in all required fields and possibly attaching supporting documentation. In case of an identified report, the whistleblower includes their personal details in the appropriate fields and describes the observed violation, again attaching relevant documentation.

Through the platform, both anonymous and identified whistleblowers can communicate with the Whistleblowing Manager.

The platform allows the Whistleblower to submit a report by selecting the type of illicit conduct. Upon receiving the report, the platform anonymizes the data of both the Whistleblower and the Subject of the Report, and automatically places them in a separate archive managed – through digital means – by the



Whistleblowing Manager, accessible only to this individual, where the data will be stored. The personal data in each archive is encrypted using dedicated and different encryption keys.

The platform then displays an initial notice confirming the receipt and taking charge of the report and provides a unique identification code for the report, through which the Whistleblower can access the platform to verify any clarification requests and the status of the report evaluation. This code does not allow the identification of the Whistleblower, who therefore remains anonymous while being able to access the report, check its status, and respond to any clarification requests.

It is the duty of each Whistleblower to carefully safeguard the unique identification code of the report, not to share it with others, and not to allow third parties to access information regarding the report.

#### a. 2 Oral Reports

Through the platform described in the previous paragraph, it is also possible to make an anonymous oral report in one of the following ways:

- By recording an audio file via the platform. The platform allows, through a special software, to mask the voice of the Whistleblower.
- By requesting a direct meeting with the report manager via the platform, within a reasonable timeframe, no later than 7 (seven) days from the request. In this case, the complete and accurate documentation of the meeting is retained, on durable media, ensuring access to the information, upon the express consent of the Whistleblower. Oral reports made via a meeting, subject to the Whistleblower's consent, can be documented by the report manager through a suitable recording device or minutes. If the content of the meeting is verbalized, the Whistleblower can verify, amend, and confirm the meeting minutes by signing them.

Additionally, regardless of the method (oral or written) used to make the report, if the Whistleblower has provided their contact information, a receipt notice of the report will be sent to the Whistleblower within 7 (seven) days from its receipt.

To ensure traceability, all reports submitted outside the digital platform will be entered by the report manager within 48 (forty-eight) working hours from receipt onto the dedicated platform, highlighting their origin.

Similarly, employees of the Company, other than the report manager, who receive reports in any form, are required to maintain the absolute confidentiality of the acquired information and must ensure that the report is forwarded to the report manager within 3 days from receipt, without retaining a copy and attaching any supporting documentation.

#### b. External Reporting Channels

As per Legislative Decree 24/2023, ANAC activates an "external reporting" channel (referenced here: <https://www.anticorruzione.it/-/whistleblowing>) which guarantees the confidentiality of the Whistleblower, the person involved, and the person mentioned in the report, as well as the content of the report and related communication.

Private sector entities may submit a report using the aforementioned external channel when one of the following conditions is met:

- The Whistleblower has already submitted an internal report, using the tools described in the previous sections, but this has not been followed up on.



- The Whistleblower has valid reason to believe that an internal report would not be effectively followed up on or that it could lead to retaliation.
- The Whistleblower has valid reason to believe that the violation could present an imminent or obvious danger to the public interest.

Regarding the External Report received, ANAC:

- Issues a receipt notice to the Whistleblower within 7 days of receiving the External Report, unless the Whistleblower explicitly requests otherwise, or unless ANAC believes that issuing the notice would compromise the protection of the Whistleblower's identity.
- Provides feedback to the Whistleblower regarding the received report within 3 months of the receipt notice or, if there is no such notice, within three months from the expiry of the 7-day period following receipt of the report. If justified and motivated reasons exist, feedback is provided within 6 months from the receipt notice or, in the absence of this notice, within 6 months from the expiry of the 7-day period from receipt of the report.
- Communicates the final outcome of the report to the Whistleblower.

#### c. Public Disclosure

The Whistleblower may make a public disclosure through the press, electronic media, or other means of communication capable of reaching a wide audience, under the conditions and in the manner specified by Legislative Decree 24/2023.

In particular, public disclosure of violations and illicit conduct is allowed if at least one of the following conditions is met:

- The Whistleblower has previously made both an internal and external report, or has made a direct external report, and has not received feedback within the prescribed timeframes.
- The Whistleblower has valid reason to believe that the violation could present an imminent or obvious danger to the public interest.
- The Whistleblower has valid reason to believe that the external report could lead to retaliation or would not have effective follow-up due to specific circumstances, such as the risk of evidence being concealed or destroyed, or where there is reason to fear that those receiving the report might be colluding with the perpetrator or involved in the violation itself.

#### *Communication Channels with the Supervisory Board (OdV)*

Zilio Industries S.p.A. has established two communication channels:- Email address for the Supervisory Board (OdV):

The OdV email, in addition to traditional communication methods already in place within the company, allows employees to report to the Supervisory Board behaviors not in line with established behavioral standards, or to communicate any doubts or concerns related to the application of the principles defined in the Model during their work activities.

The email has been set up outside the company network to avoid generating any concerns for potential Whistleblowers about their information being known or revealed by internal personnel responsible for managing such systems (i.e., system administrators).

- Postal address for paper reports: the submission is made in a sealed envelope, addressed to the OdV.

The reports received by the OdV are collected and stored in a special archive, accessible only by members of the Board. The Board is obligated not to disclose the information and reports acquired in the exercise of its functions, ensuring confidentiality and refraining from using them for purposes other than those specified by Article 6 of Legislative Decree 231/01. In any case, all information in the possession of the Board is processed in compliance with applicable legislation, particularly in accordance with privacy laws.

### **3.7 Risk Area Mapping and Controls**

Article 6, paragraph 2, letter a), of the Decree requires that the Model include a mechanism to "identify activities where crimes may be committed."

Identifying areas where crimes may occur involves a detailed evaluation of all business processes, to verify the abstract applicability of the criminal offenses foreseen by the Decree and the suitability of existing control elements to prevent them. This analysis results in a company document called "Risk Area Mapping and Controls" (referred to as the "Risk Map"), which is kept both by the relevant company office and by the OdV.

The Risk Mapping ("Risk Assessment - Risk Area Mapping Document," attachment no. 5 of this Model) forms the foundational basis of this Model, determining the scope and effectiveness of all its components. The creation of this document and its updating require the implementation of a real company process, which this protocol aims to regulate.

Consequently, with this Model, Zilio Industries S.p.A. mandates that the preparation and constant updating of the Risk Mapping is the responsibility of the Sole Administrator, delegated operationally to the OdV. The OdV, with the assistance of subject matter experts if deemed necessary, will conduct a preliminary analysis to identify and justify which criminal offenses are abstractly applicable to the company's reality and for which detailed analysis is deemed necessary, and those for which the risk is considered non-existent.

Following this "preliminary analysis" – the outcome of which is contained in a preliminary document to the mapping – the responsible entity will carry out a detailed analysis, assisted by management, to ensure the following objectives:

- Identify the company departments/functions that, based on their tasks and responsibilities, could be involved in "crime risk" activities;
- Specify the types of crimes considered;
- Specify the concrete ways the crime could be realized;
- Identify the control elements in place to oversee the identified crime risks;
- Determine the probability and severity of risks emerging from the self-assessment conducted by company management.

The results from the Risk Mapping and its related controls will be updated by company management under the guidance of the OdV, also with the help of experts in mapping techniques, and reviewed whenever there are substantial changes in the company's organizational structure (e.g., the creation/modification of organizational units, the initiation/modification of company activities), or when there are significant legislative changes (e.g., the introduction of new criminal offenses to which the legislation applies).

The results from the verification of the Risk Mapping and related controls will be specifically communicated by the OdV to the Administrative Body, which will make appropriate resolutions regarding the update of the Model.



### **3.8 Protocols and Procedures System**

Zilio Industries S.p.A., in compliance with the principles outlined above, must adopt an internal system of procedures to regulate the main company processes in accordance with the requirements of Legislative Decree 231/2001.

This set of company procedures serves the dual purpose of preventing and impeding the commission of the crimes foreseen by the Decree and ensuring the highest level of reliability of financial reporting.

### **3.9 Disciplinary System**

The effectiveness of this Model is guaranteed by an adequate Disciplinary System that sanctions non-compliance with the Model's provisions and its constituent elements. Such violations must be disciplined, regardless of the potential initiation of a criminal trial, as they constitute violations of the employee's duties of diligence and loyalty and, in more severe cases, breach the trust established with the employee.

The Disciplinary System is independent of criminal offenses and is not a substitute for the regulations governing the employment relationship, the Workers' Statute (Law No. 300/1970), and the applicable Company and National Collective Labor Agreement for the company's employees. The Disciplinary System aims to sanction non-compliant behaviors by employees – both managerial and non-managerial – the sole administrator and auditors, as well as consultants, OdV members, collaborators, and third parties. The Disciplinary System is an integral part of this Model (Attachment no. 7 of this Model).

### **3.10 Training Plan**

Internal training is an essential tool for the effective implementation of the Model and for disseminating the behavior and control principles adopted by Zilio Industries S.p.A., aiming to reasonably prevent crimes under Legislative Decree 231/2001.

For this purpose, the HR manager, when appointed, or the Sole Administrator in collaboration with the OdV, promotes the creation of a specific training plan for those subject to this Model, covering the contents of this document and the Decree.

The training program must meet the following requirements:

- Be suitable for the position held within the organization (new hire, employee, executive, director, etc.);
- Content must vary according to the subject's activities within the company (high-risk activities, control activities, non-risk activities, etc.);
- Training frequency must be based on the level of change the subject is exposed to;
- Consider the external environment in which the company operates, as well as the capacity for learning of personnel and the commitment of management to make the training authoritative;
- The instructor should be competent and authoritative to ensure the quality of the content and emphasize the importance of the training for Zilio Industries S.p.A. and its strategies;
- Participation in the training program must be mandatory, and specific control mechanisms should be in place to verify the presence and learning outcomes of each participant.

Training can be classified as general or specific.



In particular, general training must involve all levels of the organization, to ensure everyone:

- Understands the principles established by Legislative Decree 231/2001 and is aware that Zilio Industries S.p.A. intends to incorporate them into its corporate culture;
- Knows the objectives the Company aims to achieve through the Model's implementation and how each individual's duties contribute to this goal;
- Understands their role and responsibilities within the company's internal control system;
- Knows the behaviors that are expected or acceptable and those that are not acceptable;
- Understands the reporting channels available and how to report any anomalies in company activities;
- Is aware of the disciplinary actions applicable in the case of violations of the Model's rules;
- Knows the powers and duties of the OdV.

Specific training is intended for individuals who, due to their activities, require specific expertise to manage the particularities of their tasks, such as personnel working in areas identified as potentially "at risk of criminal activity." These individuals must receive both general and specific training. In particular, specific training must enable individuals to:

- Be aware of the potential risks associated with their activity, as well as the specific control mechanisms to implement in order to monitor their work.
- Understand the risk assessment techniques related to their activity and the precise procedures regulating the same, in order to acquire the ability to detect potential anomalies and report them in a timely manner for corrective actions.

Additionally, individuals responsible for internal control, tasked with monitoring activities deemed potentially risky, will receive specific training to make them aware of their responsibilities and their role in the internal control system, as well as the penalties they face if they fail to meet these responsibilities.

In the event of relevant changes or updates to the Model, targeted refresher modules will be organized to address the updates.

Finally, specific modules will be provided for new hires working in high-risk areas.

### **3.11 Communication of the Model**

In line with the provisions of the Decree and the Guidelines, the Company will ensure full publicity of this Model to ensure that all personnel are aware of its contents.

The communication must be widespread, effective, clear, and detailed, with periodic updates related to changes in the Model.

For the communication to be effective, it must:

- Be sufficiently detailed according to the hierarchical level of the intended recipients.
- Use the most appropriate and easily accessible communication channels to ensure timely delivery of information, allowing recipients to access it effectively and efficiently.
- Be of high quality in terms of content (including all necessary information), timeliness, updates (containing the most current information), and accessibility.



Therefore, the actual communication plan for the essential components of this Model must be developed, in line with the principles defined above, using the company's communication tools, such as email distribution or publication on the company's intranet.

### **3.12 Information for Collaborators and Partners**

Zilio Industries S.p.A. promotes the knowledge of the principles and conduct rules set out in the Code of Ethics and this Model among consultants, partners, collaborators, customers, and suppliers. These individuals will be provided with specific information and mechanisms for the inclusion and acceptance of contractual clauses that the Company, after consulting the relevant department, may include in the applicable contracts.

## **4. INTRODUCTION TO THE SPECIAL PART**

The purpose of the Special Part is to ensure that all recipients of the Model (such as employees, managers, directors, liquidators, consultants, suppliers, external collaborators, company partners, etc., and generally all those required to comply with the Model, hereinafter referred to as the "Recipients") adopt conduct rules in line with what is prescribed in order to prevent the occurrence of crimes considered in the Model.

In particular, the Special Part has the following functions:

- To describe the procedural principles – both general and specific – that Recipients of the Model must observe to ensure the correct application of the Model.
- To provide the Supervisory Body with the tools necessary to carry out the control and verification activities required by the Model.

The following outlines the general control principles that must be observed within all company activities:

### Formalization of Behavioral Norms

It must be ensured that:

- There is a clear, formal, and accessible description and identification of activities, tasks, and powers assigned to each department and professional role.
- There is a precise description of the control activities and their traceability.

### Definition of Roles and Responsibilities

Internal regulations must outline the roles and responsibilities of organizational units at all levels, providing a homogeneous description of the activities of each structure. This regulation must be made available and known within the organization.

If employees, collaborators, consultants, or partners engage with public entities on behalf of the Company, formal power must be granted (through appropriate delegation for employees or specific clauses for others). Where necessary, a written power of attorney will be issued to these individuals, complying with all defined criteria.

### Segregation of Duties

Within each relevant business process, the functions or individuals responsible for decision-making and implementation must be separated from those responsible for recording and controlling the process.



**ORGANIZATION, MANAGEMENT AND CONTROL  
MODEL – EX D.LGS 231/2001**

There should be no overlap between individuals making or implementing decisions, those recording financial transactions, and those tasked with performing the required checks in line with the law and the internal control system procedures.

The compliance with authorizations, delegations, and powers of attorney must be adequately monitored by the company's control bodies through random checks of signed documentation.

**Control Activities and Traceability**

Operational controls and their characteristics (responsibility, evidence, periodicity) must be formalized within procedures or other internal regulations.

Documents relevant to sensitive activities must be adequately formalized, including dates, acknowledgments, and recognizable signatures of the person responsible or supervisor. These documents must be stored in appropriate places to protect data confidentiality and prevent damage, deterioration, or loss.

The formation of documents and their corresponding authorization levels, the development of operations (both material and recording), must be traceable, showing the reasoning and rationale behind decisions to ensure transparency in choices made.

The responsible party for the activity must produce and maintain adequate monitoring reports, which provide evidence of checks performed and any anomalies.

Where possible, IT systems should be adopted to ensure the correct and truthful assignment of each operation (or its segment) to the responsible individuals, and those involved should be identified. The system should prevent modifications to records.

Documents related to the Company's activities, especially digital documents concerning sensitive activities, should be archived and stored by the relevant department in such a way that they cannot be modified, except with proper evidence.

Access to archived documents must always be justified and allowed only to authorized persons or those delegated by other control bodies, such as the Supervisory Body.