ORGANIZATION, MANAGEMENT AND CONTROL MODEL

(Legislative Decree no. 231 of 2001 and subsequent modifications and integrations)

MEMC ELECTRONIC MATERIALS S.P.A.

GENERAL SECTION

Approved by resolution of the Board of Directors on 26/11/2024

TABLE OF CONTENTS

Definitions

The following definitions refer to all parts of the Model, without prejudice to any further definitions contained in the Special Section.

GlobalWafers Co. Ltd: is the parent company, with registered office in Taiwan, listed on the local stock exchange.

GlobalWafers BV: is the company with registered office in The Netherlands, belonging to the GlobalWafers group and sole shareholder of Memc Electronic Materials S.p.A.

Risk Areas: the areas of the Company's activities in the context of which there is a risk of commission of the Crimes pursuant to Legislative Decree 231/2001 that may entail administrative liability for the Company, as identified in the individual parts of the Special Section of this Model, and better detailed in the matrix of Processes and Sensitive Activities, attached to the document.

CCNL: the National Collective Labour Agreements applied by the Company.

Code of Ethics: the code of ethics adopted by the Company in December 2023.

External Collaborators: the Consultants, Business Partners and Suppliers.

Supervisory Board (SB): the internal control body in charge of supervising the operation of and compliance with the Model, as well as its updating.

Consultants: the subjects acting in the name and/or on behalf of the Company by virtue of a mandate or other contractual relationship of professional collaboration.

Addressees: directors, auditors, managers and Employees of the Company and External Collaborators.

Employees: persons having a subordinate working relationship with the Company, including managers.

Legislative Decree 231/2001 or the Decree: Legislative Decree no. 231 of 8 June 2001 and subsequent amendments and additions.

Entity or Company: the company Memc Electronic Materials S.p.A. or one of its organizational units.

Suppliers: the Company's suppliers of goods and services.

Guidelines: the Guidelines adopted by Confindustria (Italian Industry's Association) on 7 March 2002 and subsequent updates and additions, for the preparation of organization, management and control models pursuant to Article 6, paragraph 3, of Legislative Decree 231/2001.

Model: the organization, management and control model provided for by Legislative Decree 231/2001.

Corporate Bodies: the Board of Directors, the Board of Statutory Auditors and their members.

P.A.: the Public Administration and, with reference to offences against the public administration, public officials and persons in charge of a public service.

Partners: the contractual counterparties with whom the Company enters into some form of contractually regulated collaboration (temporary business association, joint venture, consortium, licence, agency, collaboration in general), where intended to cooperate with the Company within the scope of the Sensitive Activities.

Offences: the types of offences to which the provisions of Legislative Decree 231/2001 on the administrative liability of entities apply.

Foreword

This document, adopted by resolution of the Board of Directors on __/__/2024, contains the guidelines and general principles describing the Model and consists of a 'General Section' and a 'Special Section'.

The General Section contains a concise illustration of the Decree and its contents, as well as the rules and general principles of the Model, the identification of the Supervisory Board and the definition of its tasks, powers and functions, the description of the reporting, sanctioning and disciplinary systems; the definition of a system of communication, information and training on the Model, as well as the provision for periodical checks and updating of the Model.

The Special Section contains the identification of the areas and activities considered relevant to the Company, as well as the description of the preventive control protocols adopted for each category of offence considered relevant to the Company pursuant to Legislative Decree 231/2001. It also includes the 'Matrix of Sensitive Processes and Activities', i.e. the risk analysis concerning the Offences.

1. PURPOSE OF LEGISLATIVE DECREE NO. 231/2001 AND ITS APPLICATION

Legislative Decree No. 231/2001, titled "Regulations on the Administrative Liability of Legal Persons, Companies, and Associations, Including Those Without Legal Status," introduced for the first time in Italy, the "criminal" liability of entities for certain offenses committed in their interest or for their benefit. The provisions contained therein, identify as active subjects of the offense individuals who hold positions of representation, administration, or direction within the Entity or one of its organizational units endowed with financial and functional autonomy, as well as individuals who exercise, even *de facto*, management and control over the entity or one of its organizational units. Additionally, it includes individuals who are subject to the direction or supervision of any of the aforementioned persons. This liability is in addition to that of the individual who physically committed the act.

The Offences, the commission of which gives rise to the Entity's administrative liability, are those expressly and strictly referred to by the Decree and subsequent amendments and additions. As for the Offences to which the rules in question apply, these are currently the following types: (a) offences committed against the Public Administration and against the assets of the State or other Public Entity, (b) offences relating to counterfeiting money, public credit cards, revenue stamps and identification instruments or signs, (c) corporate offences (including offences of corruption between private individuals and incitement to corruption between private individuals) (d) offences with the purpose of terrorism and subversion of the democratic order, (e) offences against the individual, (f) offences of insider trading and market manipulation, (g) offences committed in violation of the rules on accident prevention and protection of hygiene and health at work, (h) handling stolen goods, money laundering, use of money, goods or benefits of unlawful origin as well as self-laundering, (i) transnational offences, (j) computer crimes and unlawful processing of data, (k) offences relating to violation of copyright, (l) offences against industry and trade, (m) organised crime offences (n) offences against the administration of justice, (o) environmental offences, (p) offences concerning immigration and the condition of foreigners, (q) racism and xenophobia offences, (r) fraud in sporting competitions, unlawful gaming or betting and gambling by means of prohibited devices, (s) tax offences, (t) smuggling offences.

An essential prerequisite for the application of the Decree is that the offences are committed in the interest or to the advantage of the companies or entities to which the regulations apply:

a) by individuals who hold positions of representation, administration, or direction within the Entities or one of its organizational units endowed with financial and functional autonomy, as well as individuals who exercise, even *de facto*, management and control over the abovementioned entities; and

b) by individuals subject to the management or supervision of one of the aforementioned individuals.

It is important to note that, for the purposes of the offences provided for in this Decree, it is not necessary for the Company to be aware of the acts committed by the above-mentioned individuals or for the Company to have gained a pecuniary advantage. It is sufficient that the offence is committed simply to the advantage or in the interest of the entity; obviously, the interest or advantage of the entity must be assessed *ex ante*.

The sanctions provided for, in the event that one of the offences indicated in the Decree is committed, are: pecuniary sanctions, interdiction measures, confiscation and official notification of the sentence. Among the sanctions provided for, the most serious are the interdiction measures such as the prohibition from exercising the activity, the suspension or revocation of authorisations, licences or concessions functional to the commission of the offence, the prohibition from contracting with the Public Administration, the exclusion from incentives, financing, contributions or subsidies and the possible revocation of those already granted, the prohibition from advertising goods or services.

However, the company is not liable if it proves:

- that it has adopted and implemented a suitable organization, management and control models before the offence was committed,
- that it has entrusted the task of supervising the functioning and observance of the models to a body endowed with autonomous powers of initiative and control,
- that the persons have committed the offence by fraudulently circumventing the organization and management models,
- that there has been no failure to supervise on the part of the appointed body.

2. IMPLEMENTATION OF ARTICLE 6 OF LEGISLATIVE DECREE NO. 231/2001

With the adoption of this document, we intend to fulfil, also on a formal level, the express requirements of Article 6 of the Decree in relation to the planned 'adoption' of organization, management and control models.

In drafting the document, inspiration and guidance was partly drawn from the Confindustria Guidelines.

In any case, it is necessary to point out that the Model adopted by the Company refers, in many cases, to a multiplicity of sources and internal company references (e.g. procedures, Code of Ethics, schemes and workflows, etc.), the text of which will not be reproduced here for the sake of synthesis and clarity. These sources and references are, however, made available to the addressees and can be attained if necessary.

The task of taking care, where necessary, of updating the Model as well as of supervising its operation and observance falls upon the Supervisory Board ('SB').

With particular reference to the activity of updating the Model, in order to ensure its perfect adherence to any corporate or regulatory changes that may entail an extension of the Risk Areas, the Supervisory Board, also with the help of external consultants, must ensure the utmost timeliness in the integration and revision of the Model.

3. FUNCTION OF THE MODEL

The adoption of the Model by companies is not mandatory, but optional.

Below are the procedures for the drafting of the Model and its objectives:

- identify areas of activity at risk of criminal offenses,
- verify and provide documentary evidence of operations at risk,
- identify a body to perform the control and supervisory functions required by the Decree,
- implement the control and supervisory systems already existing within the Company and, if necessary, address any omissions therein,
- develop new control procedures for those risks not covered by the existing control and supervisory systems, in accordance with the principles dictated by the Decree,
- publicize and raise awareness at all company levels of the established rules of conduct and procedures,
- reiterate that all unlawful behaviours are condemned by the Company as they violate legal provisions and the requirements of the Code of Ethics adopted by MEMC,
- enable the Company and consequently the Supervisory Board (OdV) to intervene promptly to prevent and counteract the commission of the offences specified by the Decree.

The Company aims to adopt and update the Model provided for in the Decree, to enhance awareness among all individuals acting in the name and on behalf of the Company. This initiative is intended to ensure that they adhere to appropriate conduct in their activities and duties, thereby minimizing the risk of committing offenses as defined by legislation.

The elements characterising this Model are its effectiveness, specificity and topicality.

Effectiveness

The effectiveness of an organizational model depends on its practical ability to establish decision-making and control mechanisms that can contain, or at the very least, significantly reduce, the potential area of risk of liability. This effectiveness is ensured by the presence of both preventive and subsequent control mechanisms that can identify sensitive activities at risk of offenses and report any unlawful behaviour. In fact, the effectiveness of an organizational model also depends on the efficiency of the tools designed to identify and prevent the commission of offenses under Legislative Decree 231/2001.

Specificity

The specificity of an organizational model is one of the elements that characterise its effectiveness.

- Specificity is needed in relation to the areas at risk, as referred to in Article 6 paragraph (2) letter (a) of Legislative Decree No. 231/2001, which requires a census of the activities within the scope of which, offences may be committed.
- A specificity of the entity's decision-making and implementation processes in 'sensitive' areas is also necessary, as provided for in Article 6 paragraph (2) letter (b) of Legislative Decree No. 231/2001.

The Model must take into account the specific characteristics, the size of the Company and the type of activities performed, as well as the Company's history.

Topicality

It is important to highlight that, to maintain the effectiveness of the Organization, Management, and Control Model adopted by the Company, continuous monitoring of its implementation and regular updates are essential. This is necessary to account for changes in the corporate structure and to assess its actual effectiveness in preventing the offenses outlined in Legislative Decree No. 231/2001. In this context, Article 6 of Legislative Decree No. 231/2001 stipulates that the supervisory board, which possesses independent powers of initiative and control, is responsible for updating the Model.

4. ADDRESSEES OF THE MODEL

The rules contained in the Model apply:

- to those who hold, within the Company, formal positions, such as those of legal representative, director, member of the board of auditors,
- to those who perform, even *de facto*, management, administration, direction or control functions in the Company or in one of its autonomous organizational units,
- to those who, though not formally appointed, actually perform management and control activities in the Company or in one of its organizational units,
- to employees of the Company, including Employees of any rank and under any type of contractual relationship,
- to all those individuals who collaborate with the Company by virtue of a para-subordinate employment relationship, such as project collaborators, temporary workers, interim workers, etc.,
- to those individuals who, although not belonging to the Company, work on behalf or in its interest,
- to those individuals who act in the interest of the Company, insofar as they are linked to the same by contractual legal relations or by agreements of another nature, such as, for example, joint-venture partnerships or association for the realisation or acquisition of a project,
- all Group subjects whose activities/decisions have an impact on the Company.

The Model constitutes an indispensable reference for all those who contribute to the development of the various activities with whom MEMC operates, such as suppliers of materials, services and works, consultants and partners.

5. ETHICS AND COMPLIANCE

MEMC has established strict adherence to current regulations and ethical principles as the foundation of its activity. This commitment is clearly reflected in all standards and procedures issued by MEMC and/or the Parent Company over time, to which all Group companies, including MEMC, are required to comply.

Operating in an international context, MEMC recognizes the critical importance of complying fully with the relevant local or national regulatory frameworks. As a result, it implements policies, standards, and codes of conduct that are often more stringent than those required by various legislations. Furthermore, MEMC adopts uniform procedures, criteria, and working methods internationally, that are deemed effective for preventing or detecting any unlawful activities committed by its employees or representatives.

The policies adopted by the Company concern: customs compliance, purchasing, production, research and development, commercial, IT, communication and marketing, personnel, occupational safety and the environment.

They are contained in the organization's DMS system, accessible only to Employees granted with a username and password, with the exception of the Code of Ethics, which can be found on the intranet system.

Each Employee can access the common policies and those specific to his/her job description.

6. POLICIES, STANDARDS, PROCEDURES AND REFERENCES OF TAIWANESE DERIVATION

GlobalWafers Co. Ltd operates on the Italian territory through MEMC, whose shares are entirely owned by GlobalWafers B.V., based in the Netherlands.

MEMC is the direct addressee and responsible for the application of all policies, standards and procedures (hereinafter jointly referred to as ‘policies’) issued over time by the Parent Company.
MEMC also drafts its own policies. The adoption of policies must comply with the Functional Procedure entitled DMS System Administration.

The purpose of this procedure, which is also contained in the DMS System, is to bring together information for the control of online documentation, which is managed through the DMS application.

The cogency of these documents and the disciplinary consequences of their violation are clearly explained to all employees.

As far as the archiving of policies is concerned, these are contained in MEMC's DMS. The Functional Procedure entitled DMS System Administration, provides for automated information methods to predefined recipients.

AREAS OF RISK WITHIN THE ACTIVITIES OF MEMC ELECTRONIC MATERIALS S.P.A.

The Company has a particularly structured corporate purpose and organization. This entails the need to carefully monitor the exposure to the potential risks of committing offenses relevant under the Decree across all its activities. Certain areas, however, require particularly diligent oversight.

Specifically, the Company primarily conducts its operations with customers in the private sector. In the public sector, MEMC enters into agreements with universities concerning training (scholarships) and research and

development, and it collaborates with public authorities on strategic projects aimed at securing funding. Additionally, the Company interacts with the PA as a user or beneficiary of their services.

The fact of having to interact with representatives of public Entities, Authorities or public Bodies, presents a distinct risk factor, particularly concerning the potential for corruption practices. The new legislative framework has, in any case, mandated a more comprehensive and detailed examination of the areas of activity and business processes that could theoretically give rise to offenses outlined in the Decree.

Given the complex structure of the Company's activities and processes, a "Matrix of Sensitive Processes and Activities" has been developed, categorizing types of offenses through a thorough analysis of the corporate context where the risk of committing various offenses outlined in the decree, exist.
This detailed assessment, conducted through careful examination of the Company's activities, corporate policies, procedures, and relevant documentation, involved input from Company Representatives holding key functions within the organization. It inevitably concentrated on the risks of offenses that are particularly significant within MEMC's specific context. The findings of this analysis are reflected in the parts of the Special Section, which provide detailed treatment for each type of offense, as well as in the "Matrix of Sensitive Processes and Activities" attached to the Model.
Within the framework of this Matrix, areas of activity deemed "sensitive" to the commission of offenses have been identified—specifically, activities where opportunities for committing the offenses specified in the Decree may hypothetically arise.

The analysis concerned:

- the offences referred to in Articles 24 and 25 of the Decree (offences against the public administration and against property committed to the detriment of the State or another public body),
- the offences referred to in Article 25-ter of the Decree (so-called corporate offences), including the offence of 'corruption between private individuals' and 'incitement to corruption between private individuals' referred to in letter *s- bis* of the same article,
- the offences of unintentional murder and grievous or very grievous body injuries, committed in violation of the rules on accident prevention and on the protection of hygiene and health at work referred to in Article 25-*septies* of the Decree,
- computer crimes and unlawful processing of data under Article 24-*bis* of the Decree,
- organised crime offences under Article 24-*ter* of the Decree,
- the counterfeiting of money in public credit cards, revenue stamps and identification instruments or signs referred to in Article 25-*bis* of the Decree,
- offences against industry and trade referred to in Article 25-*bis*.1 of the Decree,
- offences relating to the violation of copyright, as referred to in Article 25-*nonies o*f the Decree,
- offences against the administration of justice referred to in Article 25-*decies* of the Decree,
- environmental offences under Article 25-*undecies* of the Decree,
- offences relating to immigration and the condition of foreigners referred to in Article 25- *duodecies* of the Decree,
- offences against the individual as set out in Article 25- *quinquies* of the Decree,
- the offences of receiving stolen goods, money laundering, use of money, goods or benefits of unlawful origin, and self-laundering set out in Article 25-*octies* of the Decree,
- the offences relating to racism and xenophobia set out in Article 25-*terdecies* of the Decree,
- tax offences referred to in Article 25 - *quinquiesdecies* of the Decree,
- the offences of smuggling referred to in Article 25 - *sexiesdecies* of the Decree.

After a preliminary assessment, terrorism offences under Article 25-*quater* of the Decree, as well as offences of insider trading and market manipulation under Article 25-*sexies* and transnational offences were excluded from the detailed analysis, since, although their abstract verifiability cannot be completely ruled out, their concrete realisation is unlikely, both in view of the Company's operational reality and in view of the elements necessary for the realisation of the offences in question (with particular reference for some of them to the psychological element of the offence).

Concerning the offense of criminal conspiracy as defined in Article 416 of the Italian Criminal Code, the analysis concentrated on the traceability of this offense to those considered in the mapping of processes and sensitive activities. While it is not possible to entirely rule out the applicability of criminal conspiracy to offenses beyond those mapped, the analysis conducted comply to the principles outlined in Articles 2 and 3 of Legislative Decree No. 231/2001, focusing specifically on the characteristics of the Company's operational activities.

Regarding the offense of "self-money laundering," the analysis was conducted in strict accordance with the principles outlined in Articles 2 and 3 of Legislative Decree No. 231/2001, particularly emphasizing the mandatory nature of the offense. The examination was approached from two perspectives:

- self-money laundering is considered as a means by which funds, goods, or other benefits derived from non-negligent offenses—already classified as predicate offenses under Legislative Decree No. 231/2001 and included in the risk analysis—could be utilized, substituted, or transferred within the context of the Company's economic and entrepreneurial activities. In this regard, self-money laundering can be viewed as a potentially "consequential" offense stemming from previously identified predicate offenses of a non-culpable nature. Accordingly, the control protocols for the "source" offense of self-money laundering, specifically concerning the categories of offenses listed as predicate offenses under Legislative Decree No. 231/2001, are those established in the special section of the Model for each macro-category of offense,
- the analysis also considers self-money laundering with a focus on the moment of commission of the offense itself. This perspective highlights the regulatory requirement that for self-money laundering to occur, there must be conduct aimed at deliberately obstructing the identification of the criminal origin of funds, goods, or other benefits resulting from any non-culpable offense (including those not covered by the mapping). In this context, the analysis concentrated on tracing financial and treasury flows, as these processes are where actions to impede the identification of criminal origins can be hypothesized. This is particularly relevant, but not exclusive to transactions of an extraordinary nature, such as capital increases through contributions or shareholder financing etc.

With regard to the tax crimes referred to in art. 25-*quinquiesdecies* of the Decree, it should be noted that all the crimes indicated by the law have been deemed potentially relevant:

- fraudulent tax declaration through invoices for non-existent transactions, provided for by art. 2 of Italian Legislative Decree 74/2000,
- fraudulent tax declaration through other means, provided for by art. 3 of Italian Legislative Decree 74/2000,
- issuing invoices or other documents for non-existent transactions, provided for by art. 8 of Italian Legislative Decree 74/2000,
- concealment or destruction of accounting documents, provided for by art. 10 of Italian Legislative Decree 74/2000,
- fraudulent evasion of tax payment, provided for by art. 11 of Italian Legislative Decree 74/2000.

Furthermore, in the implementation of the so-called “PIF Directive”, the following crimes have also been introduced:

- unfaithful declaration, a crime provided for by art. 4 of Italian Legislative Decree no. 74/2000,
- failure to declare, a crime provided for by art. 5 of Italian Legislative Decree no. 74/2000,
- undue compensation provided for by art. 10-*quater* of Italian Legislative Decree no. 74/2000,

which fall within the scope of application of Legislative Decree 231/2001 only when the false or unfaithful declaration concerns VAT (the equivalent crime provided for income taxes is therefore excluded) and the criminal conduct jointly meets all the conditions provided for by Legislative Decree no. 75/2020, regarding the thresholds (evaded VAT exceeding 10 million Euros) and the commission in the context of cross-border fraudulent systems.

7. CODE OF ETHICS

As previously mentioned, MEMC has adopted a Code of Ethics that is well-known among all employees. This Code is accessible through the MEMC intranet for employees and is also available on the GlobalWafer Co. website.

In order to facilitate its dissemination and understanding, the Code of Ethics has also been translated into English and is sent to Consultants and Suppliers.

The Code of Ethics clearly defines prohibited behaviours and emphasizes the binding nature of the internal ethical rules, along with the potential for disciplinary sanctions to be imposed by the Company, which will be proportional to the severity of any violations identified.

Particular emphasis has been placed on preventing the illicit acts specified in the Decree, with significant attention given in the manual, to issues of corruption and, more generally to the overall necessity of adopting ethical conduct in business practices.

The topics addressed in the Code of Ethics include: 1) Management System; 2) Ethics; 3) Where to Get Help; and 4) Whistleblowing – Management of Reports Concerning Violations of Law, the Code of Ethics, and MEMC Electronic Materials S.p.A.'s Policies.

For the analysis of each individual topic, please refer to the Code itself.

The contents of the Code of Ethics are constantly at the centre of training and awareness initiatives; all employees have undertaken to know and apply the rules with a specific declaration (in electronic version).

The Supervisory Board has the specific responsibility of ensuring the updating of the Code of Ethics.

The Code of Ethics is recognized as the primary regulatory source in all new operating procedures issued by the Company as part of its quality system. Consequently, the provisions outlined in the Code of Ethics, must be regarded as an integral and essential component of the rules and procedures applicable to every operational sector of the Company. Thus, the Code of Ethics is considered an essential part of this Model.

The Code of Ethics is also explained and delivered to all newly hired individuals upon joining the company. A specific record of this activity is kept.

8. THE PROCEDURES

The company procedures, which are found in the DMS System of the Entity, are identified, described and recalled in the documentation produced and stored by the company, for the purposes of quality certification by safety and environmental bodies. In fact, for several years MEMC has voluntarily undergone the controls and has complied with the most advanced standards required by national and international quality regulations, and, for this purpose, it issues and periodically updates, a series of procedures and operating regulations, concerning the main processes and workflows.

The procedures are accessible from the DMS System with a username and password. In any case, only employees can access the DMS System, and the first access must be previously authorized by the Function Manager.

The procedures that more specifically pertain to the finance area are also subject to control by the auditors and also by the Internal Audit department.

The procedures cover all areas of business operations and, therefore, also include those transactional or administrative processes where, if not properly regulated or governed, they may facilitate the commission of the offenses indicated by the Decree.

Each procedure is verified from a regulatory standpoint, must be officially approved by Management or its delegates, and clearly indicates a corporate function responsible for its implementation. For each procedure, the purpose is clarified along with references related to quality, environmental protection, workplace safety, and regulations.

The content of the procedures is made easily accessible through a dedicated portal, which can be immediately accessed via the intranet page, from which users can access the DMS system; all employees are required to become familiar with and apply the procedures relevant to their specific operational area.

These procedures, like those issued by the Taiwanese Parent Company, are perceived by most employees as binding tools for regulating workflow and identifying roles and responsibilities at the corporate level.

Although the company's higher-risk activities are already governed by specific procedures, the Company—under the supervision of the Supervisory Board (OdV), as outlined in the "Information Flow Procedure" mentioned below—believes it is important to continuously monitor the situation and, where necessary, formalize new, more comprehensive, and clearer procedures in certain areas of activity considered to be at potential risk, as specifically indicated in the Special Part.

This is all aimed at more effectively preventing the commission of certain offenses outlined in the regulations and promoting better awareness and consistent application of internal rules by all employees.

9. TRAINING

MEMC's Employees undergo intense and periodic training activities that often deal with issues of ethics and compliance.

Training initiatives are organised and managed by internal specialist functions, also following the Supervisory Board’s indications. External consultants and experts in the various sectors are frequently involved. The Company generally promotes the participation of Employees in both internal and external training initiatives.

Records on the attendance are kept and updated on electronic files by the Human Resources Department and the entire process of training activities is subject to a specific and analytical procedure according to quality standards.

At the end of the sessions, employees undergo final tests, which are properly recorded and stored.

The Human Resources function provides training courses at all levels of the company organization, focusing on ethical issues and the understanding and application of regulations. These courses highlight the importance of adhering to the standards established by Global Wafers and MEMC at an international level. Specifically, regarding the administrative responsibility of companies arising from unlawful acts, there is a strong emphasis on strictly complying with internal rules and procedures designed to prevent the offenses outlined in Decree No. 231/2001.

The courses are tailored in terms of content and delivery methods based on the participants' qualifications, the risk level of their operational areas, and whether they hold representation roles on behalf of the Company. During these sessions, employees are informed about the key aspects of the regulations—particularly concerning the types of offenses currently specified by the Decree—and the potential consequences, both individual and corporate, that may result from any criminal conduct.

Special emphasis is placed on the necessity to avoid any involvement in corrupt practices or actions, as well as on maintaining proper (also from a formal standpoint) relationships and interactions with the Public Administration and, more generally, with public officials.

A specific and targeted training program is also provided for new recruits. Upon joining the company, they receive an individual reiteration of the principles and values adopted by MEMC regarding business ethics, along with an overview of the main contents of the Code of Ethics. New recruits formally declare their personal commitment through a special declaration that is maintained in the Human Resources files.

Regarding administration and financial statements, training initiatives have been organized (also managed by internal specialists) to enhance understanding of regulatory requirements and corporate procedures among those working in these areas. This aims to further mitigate the risks associated with offenses outlined in the regulations. These courses are conducted periodically to include new employees and ensure continuous updates on regulatory matters.

In terms of occupational safety, training is governed by the Manual for Safety, Health, Environmental Protection, and Energy Management, which is part of the DMS System. This manual specifies that training must be appropriate to the tasks, roles, and responsibilities of all personnel.

The training criteria (content, delivery method, frequency) in the areas of safety, health, environmental protection, and energy management (referred to as ‘ESH’) are established by the ESH Service based on the tasks performed by individuals and their associated ESH impacts. The training includes formalized instruction according to well-defined MEMC S.p.A. procedures at the workstation, with proper evaluation tools used to assess learning outcomes.

The Company has appropriate training tracking systems referred to individual employees.

More generally, in each field, MEMC verifies the effective implementation of training activities. With particular reference to ethic topics, training activities are subject to a periodic audit conducted by the internal auditing function, the results of which, are then shared with company management.

10. COMPANY ORGANIZATION

MEMC's organizational structure may vary over time, depending on various requirements, including local ones. Nevertheless, it basically tends to reflect, at least in its main features, the organizational criteria and choices adopted by the parent company.

As far as MEMC is concerned, it is the task of the Human Resources Department to ensure - at a general level - that company organization charts are updated and shared, clarifying the roles and responsibilities of the various organizational structures operating within the company.

Each supervisor, as indicated in the Company's Organizational Chart available on the Entity's Intranet System, is required to be knowledgeable about and to communicate to their employees the organizational structure of the Company, the tasks and responsibilities of their respective organizational units, as well as the specific duties associated with those tasks. Furthermore, each employee is obligated to understand their job description, duties, powers, and responsibilities pertinent to their role.

Additionally, MEMC's voluntary participation in the certification processes for the Company's quality system ensures that there is adequate documentation and assurance regarding the specific organizational structures adopted by the Company. This participation also facilitates the identification of the primary decision-making and control processes, along with the responsibilities assigned to each organizational unit.

11. ATTRIBUTION OF POWERS

The general criterion adopted by the Company stipulates that executives may be granted powers of representation through the issuance of specific powers of attorney. These powers define precise guidelines for their proper exercise and include an assessment of the necessity for such delegation. In all instances, the Chairman of the Board of Directors and personnel granted special powers of attorney are subject to the limitations outlined in the regulations of the Parent Company.

Special powers of attorney and related sub-delegations are granted based on Board resolutions, with ordinary activities managed in accordance with the Delegation of Authority (DOA) of the Global Wafer Group. The Company also oversees the updating and revocation of powers, ensuring uniform application of internal regulations.

The nature of these powers aligns with the operational needs of the Company. Management personnel are required to undergo appropriate training and awareness programs regarding this matter, particularly concerning issues related to potential abuse or improper use of the powers conferred upon the Company's representatives, especially in the public sector.

12. EXTERNAL AND INTERNAL AUDIT

The Company entrusts audits to leading companies that certify its financial statements, and the information contained therein. The assignment is approved by MEMC's Shareholders' Meeting.

The personnel involved in such audits are called upon to cooperate openly and actively in order to allow the auditing company to fulfil its mandate.

The external audit process ensures an additional qualified and thorough level of control with respect to the need for accuracy, truthfulness and transparency of the financial data and information communicated or published by the Company.

At the internal level, audits are conducted periodically during the fiscal year by the Parent Company's Internal Audit, either remotely or in person, which then presents its findings to the CEO.

13. CONTRACTUAL REFERENCES

The practice employed by MEMC to formalize its relationships with suppliers, customers, consultants, agents, and other third parties—whether in the private or public sector—entails the signing of specific contracts that govern all aspects of the business relationship. These contracts explicitly make reference to precise commitments regarding ethics and compliance with applicable regulations.

The standard contractual templates utilized by the Company contain clauses that may vary in content based on the specific circumstances, outlining detailed and clear commitments made by the parties engaged with the Company concerning principles of ethics and fairness, as well as the necessity to comply with regulatory requirements.

Some contractual texts also reference MEMC's Code of Ethics, thereby obliging counterparties to familiarize themselves with and apply its provisions within their contractual relationship with the Company.

Particular emphasis is placed on the issue of ethics and regulations in contractual relations that have an effect or in any case concern the Public Administration, in which it is unambiguously reiterated - also through reference to separate texts, documents or references - that the Company is opposed to any practice that does not comply with the regulations.

Particular emphasis is placed on ethical considerations and regulatory compliance in contractual relationships involving the Public Administration. In such contexts, it is unequivocally reiterated—often through mention to separate texts, documents, or references—that the Company opposes any practices that contravene applicable regulations.

With respect to consultants specifically, they are additionally required to declare and guarantee the following:

- that they do not operate in a situation of conflict of interest, nor utilize interpersonal or contractual relationships that may place the consultant or third parties in a conflict of interest.
- that they have not undertaken assignments or engaged in activities that are incompatible, even on a formal, contractual, or legal basis, with the consultancy relationship with the Company. This includes any current or prior activities and assignments within the Public Administration, as well as with public or private entities or businesses that compete with the Company.
- that they have not been convicted for any offense or subjected to legal proceedings for acts or conduct contrary to ethical standards and professional integrity
- that they will not use, in the performance of the consultancy relationship, any confidential information unlawfully obtained in connection with prior activities or assignments.

All individuals with whom the Company enters into contractual relationships are subject to prior verification by the responsible functions regarding their integrity, correctness, honourableness, and reliability. Any violations of rules or principles of professional ethics are considered serious breaches of contractual

commitments and may consequently result in the termination of agreements and potential claims for damages by the Company.

For procedural principles applicable to contractual relationships involving specific risk areas, please refer to the Special Part of the Model.

14. DECISION-MAKING PROCESSES

All decision-making processes within MEMC are conducted through established methods of communication and evaluation, which often involve multiple functions and, in all cases, the hierarchical chain. This is particularly pertinent to decision-making processes related to investments, disbursements, financing, expenses, contributions or donations, transfers of goods, or the provision of services (including those provided free of charge) to third parties. It is understood that such processes cannot be managed independently and at the discretion of individual employees—even those in senior management positions—but require collaborative assessments and clearly defined levels of prior approval within the organizational structure. Furthermore, there must always be the possibility for checks or verifications, at any time, by the competent functions.

In this context, reference should be made to the comprehensive structure of procedures pertaining to procurement processes, their approval, acceptance of charges, and expense settlement.

The principle of collaboration and joint assessment is similarly applied by MEMC in activities and evaluations that contribute to the formation of the budget and the preparation of the individual documents that comprise it.

In this regard, it should be noted that MEMC prepares monthly financial statements, which are consistently submitted to the Parent Company for control, scrutiny, and examination, as well as quarterly to the auditor. Additionally, an annual audit of the financial statements is conducted, resulting in the issuance of a certification report.

The contents of corporate communications are also subject to prior review by department heads, particularly by the Company's Finance Department and the Parent Company. Furthermore, as mandated by law, these communications undergo prior assessment and verification by the Company's administrative and control bodies. The entire process is supported by the Company's consultants.

Moreover, the reports accompanying the financial statements from the responsible entities, the semi-annual report pursuant to Article 2381 of the Italian Civil Code, and the quarterly report submitted to the Board of Statutory Auditors constitute an integral part of the Entity's information flow.

Concerning the processing of applications for funds, financing, and contributions provided by National Authorities or European Bodies (Organismi Comunitari), thorough controls are conducted by the functions responsible for managing such applications. These controls ensure compliance with legal requirements and verify that allocated funds align with the objectives established by the Legislator.

In all cases, financing contracts and the establishment of credit lines must receive prior authorization from the Parent Company and approval from the Board of Directors.

15. THE ROLE OF THE BODY REFERRED TO IN ARTICLE 6 OF THE DECREE

Legislative Decree No. 231/2001 specifies that the body responsible for overseeing the operation and compliance of the Model, as well as ensuring its ongoing updates, must be a designated entity within the company (Article 6.1, letter B) endowed with autonomous powers of initiative and control.

The Confindustria Guidelines recommend that this body should be distinct from the Board of Directors, characterized by autonomy, independence, professionalism, continuity of action, integrity, and an absence of conflicts of interest. This body may also coincide with the Board of Statutory Auditors.

Such autonomy implies that the Supervisory Board is accountable solely to the highest hierarchical level (i.e., the Board of Directors). If the Supervisory Board overlaps with the Board of Statutory Auditors, it will report to the Board of Directors exclusively in its capacity as Supervisory Board, thereby maintaining the independence of the controls exercised by the Board of Statutory Auditors.

To effectively perform its verification and control functions or to update the Model, the Supervisory Board may engage external consultants with proven expertise when necessary.

The Supervisory Board has a fixed term that coincides with that of the Board of Statutory Auditors.

Specifically, the Supervisory Board is a permanent collegial body with a multidisciplinary composition, tasked with the responsibilities outlined by regulations, particularly the oversight of the functioning and compliance of the organizational and management models, as well as ensuring their ongoing updates. Consequently, this body is entrusted with performing the supervisory and control functions mandated by the Model.

It has been determined to establish a collective body composed of individuals with specific expertise, in accordance with Italian Legislative Decree 24/2023, the Confindustria Guidelines, and established case law:

- Autonomy and Independence: The requirements for autonomy and independence are fundamental, assuming that the Supervisory Board is not directly involved in the management activities subject to its control,
- Respectability: The members of the Supervisory Board must not have received any criminal convictions, even if not final, or engaged in plea bargaining for offenses that would result in disqualification from public offices or are listed in the Decree,
- Proven Professionalism: The Supervisory Board must possess the technical and professional skills necessary for fulfilling its designated functions. These attributes, combined with independence, ensure impartiality in judgment,
- Continuity of Action: The Supervisory Board must continuously undertake activities necessary for supervising the Model with adequate commitment and suitable investigative powers. It is structured to ensure continuity in supervisory activities, focusing on implementing and regularly updating the Model without engaging in operational tasks that could compromise its overall perspective on the Company's activities,
- Specific Skills in Inspection and Advisory Activities,
- Availability of Organizational and Financial Resources to effectively perform its functions.

The Supervisory Board is vested with autonomous powers of initiative, control, and expenditure.

It has been expressly tasked with updating the Code of Ethics adopted by the Company, ensuring that all employees are fully informed of its contents and comply with it. This is achieved through the promotion of appropriate training activities and the facilitation of necessary corrective measures, including disciplinary

actions. The Supervisory Board may carry out these activities in collaboration with the most suitable corporate functions.

The Supervisory Board operates in accordance with established regulations. It meets periodically, and the matters discussed, along with the decisions made, are documented in a dedicated register maintained in the prescribed format for corporate records.

The Supervisory Board may be convened at any time by any Director and may also submit a written request to convene a meeting of the Board of Directors to report on the functioning of the Model, identify areas at risk for offenses, and address specific situations concerning the recipients of the Decree.

Additionally, the Supervisory Board is required to prepare a special report every six months to inform the Board of Directors about its activities and the implementation status of the Model.

In general, the Supervisory Board (SB) of MEMC is tasked with:

- monitoring compliance with the provisions of the Model by all recipients,
- proposing additions, amendments, or updates to the Model as deemed appropriate in response to changes in company conditions or new legislative guidance. To this end, the Supervisory Board collaborates continuously with other relevant organizational units, recommending necessary corrections and adjustments to the competent bodies, such as the Board of Directors.

On a strictly operational level, the SB is responsible for:

- identifying and implementing appropriate control procedures, while acknowledging the primary responsibility of individuals in senior positions within MEMC (i.e., top management, executives, directors),
- identifying activities that are at risk of criminal conduct,
- promoting initiatives to share the Model and raise awareness among all individuals involved in areas susceptible to offenses,
- collecting and documenting all information related to compliance with this Model,
- coordinating with heads of corporate functions through meetings to better identify risk areas and prevent the occurrence of offenses,
- receiving information regarding control activities conducted within MEMC by external parties (e.g., Independent Authorities, Labour Inspectorate) and by designated company functions responsible for control (e.g., internal audit),
- accepting reports from any individual (e.g., employees, consultants) who, while performing their activities, become aware of violations or alleged violations, or any relevant ordinary or extraordinary facts concerning the implementation and effectiveness of the Model,
- ensuring that individuals reporting violations (as per the point above) are protected against any form of retaliation, discrimination, or penalization—whether direct or indirect—while maintaining the confidentiality of their identity,
- initiating internal investigations to ascertain alleged violations of the provisions of the Model,
- when deemed appropriate, informing external parties (e.g., representatives, agents, consultants, partners) about specific policies and procedures adopted by MEMC based on this Model.

The role of prevention, supervision, and control exercised by the Supervisory Board, along with the powers and responsibilities assigned to it, is communicated to all employees.

The Supervisory Board serves as a permanent control entity on matters of ethics and legal compliance, with the objective of prevention and control, and reports its activities to the Company's administrative bodies.

The following circumstances constitute causes for ineligibility and incompatibility with membership on the Supervisory Board, thereby ensuring the requirement of honourability:

- being a member of the Board of Directors of MEMC or any controlled and/or affiliated companies, or of parent and/or affiliate companies, with operational powers,
- serving as an auditor for MEMC or any controlled and/or affiliated companies, or for parent and/or affiliate companies,
- having familial relationships (by marriage, kinship, or affinity) up to the fourth degree with individuals mentioned in the preceding points,
- having held administrative, managerial, or control positions in companies subject to bankruptcy, compulsory administrative liquidation, or equivalent procedures within the last three years,
- having had employment or self-employment relationships within the last three years with entities against which crimes specified by Legislative Decree 231/2001 may potentially be committed,
- having been convicted, even if not final, of:
    - a custodial sentence resulting in disqualification from public office or temporary disqualification from management positions in ordinary legal entities,
    - a custodial sentence for committing any offense outlined in Legislative Decree 231/2001,
- having received a plea bargain sentence for committing any offenses specified by Legislative Decree 231/2001.

Furthermore, the independence of the Supervisory Board is ensured by the availability of financial resources, which the Supervisory Board may utilize for any need deemed appropriate for the proper execution of its duties (e.g., specialist consultancy, business travel, etc.).

To effectively carry out its responsibilities, the Supervisory Board must coordinate with the relevant functions within the Company for various specific matters, particularly but not exclusively:

- With the Heads of the Financial Department regarding corporate obligations that may be pertinent to the commission of corporate crimes.
- With the Head of Human Resources concerning the sharing of information, staff training, and disciplinary procedures.
- With the Safety Manager (RSPP) to ensure compliance with all legal requirements and internal company procedures related to health, safety, and hygiene in the workplace.
- With the Environmental Manager to ensure adherence to all legal requirements and internal company procedures concerning environmental matters.
- With any other function deemed relevant on a case-by-case basis for the purposes of its activities.

16. PERIODIC CONTROL OF THE MODEL

The supervisory activities conducted continuously by the Supervisory Board aim to: 1) verify the effectiveness of the Model (i.e., the alignment between the actual behaviours of the recipients and the Model itself), 2) perform periodic assessments of the adequacy of codified procedures in relation to the prevention of crimes specified in Legislative Decree 231/2001, and 3) implement necessary updates to the Model. These activities are primarily outlined in the "Control Activity Work Plan" of the Supervisory Board.

The control system is designed to:

- ensure that operating methods comply with applicable laws,

- identify areas requiring corrective actions and/or improvements and assess the effectiveness of such corrective measures,
- foster a culture of control to effectively support any inspections conducted by other entities appointed to carry out verification activities.

Internal audits are managed by the Supervisory Board. To execute the planned audit activities, the Supervisory Board may engage personnel from other functions who are not involved in the audited activities and that possess specific expertise in internal control, as well as an adequate level of autonomy, or may utilize external consultants.

To facilitate its supervisory activities regarding the effectiveness and functioning of the Model, the Supervisory Board receives:

- information that is useful and necessary for fulfilling its supervisory responsibilities,
- reports concerning violations, whether alleged or actual, of the Model and/or unlawful conduct relevant under Legislative Decree 231/2001, which have occurred or are ongoing.

Information

In the corporate context, the following information must be communicated to the Supervisory Board in accordance with the "information flow procedure" outlined in the DMS:

- on a regular basis, the information, data, or updates identified by the Supervisory Board and/or requested from individual functions must be transmitted. Such information should be provided within the timelines and formats specified by the Supervisory Board,
- on an occasional basis, any other relevant information, regardless of its source—including that from third parties—pertaining to compliance with and implementation of the Model in "critical" areas of activity and adherence to the provisions of the Decree, must also be communicated. In particular, but not limited to, the following information must be transmitted to the Supervisory Board in a timely and mandatory manner:
    - measures and/or information from judicial or tax police authorities or any other relevant authority indicating that investigations are being conducted for offenses specified in the Decree, even against unidentified individuals,
    - requests for legal assistance submitted by managers and/or employees in the event of legal proceedings initiated against them for offenses covered by the Decree,
    - reports prepared by heads of company functions as part of their control activities, which may reveal facts, actions, events, or omissions that present critical issues concerning compliance with the Decree,
    - iInformation regarding organizational changes that may affect "critical" areas,

- information regarding the effective implementation of the Model at all levels of the Company must also be provided, including documentation of disciplinary proceedings undertaken and any sanctions imposed, or reasoned decisions regarding the archiving of disciplinary proceedings that fall within the scope of Legislative Decree 231/2001.

17. WHISTLEBLOWING REPORTS

Information

Law No. 179/2017, Legislative Decree No. 231/2001, and Legislative Decree No. 24/2023 mandate the adoption of specific tools supported by an IT platform within Public and Private Organizations for the implementation of Legislative Decree 231/2001. These tools enable employees, collaborators, and all individuals identified by the legislation as potential Whistleblowers to report possible fraud, criminal activity, unlawful acts, or any irregular conduct committed by other individuals within the organization to designated persons or bodies (including law enforcement agencies and public authorities).

This framework is underpinned by European Directive 2019/1937, which seeks to establish common minimum standards to ensure a high level of protection for individuals reporting violations of Union law. It creates secure communication channels for reporting both within and outside organizations. In certain circumstances, public disclosure through the media is also permitted.

The new regulation applies to violations of national and European laws that adversely affect the interests or integrity of the entity and of which whistleblowers have become aware in a work context.

This section further aims to regulate the process for receiving, analysing, and handling reports submitted by any individual, including those made anonymously, and outlines the established communication channels through which reports may be made.

Whistleblowing is regarded as a vital tool for opposing potential unlawful activities, promoting a culture of ethics and legality among employees within organizations, and fostering an environment of transparency along with a sense of participation and belonging.

Reports

The obligation to report lies with:

- the company's top management and members of corporate bodies,
- Shareholders,
- employees and collaborators of the company (including interns, trainees, temporary workers, etc.), even if they are in a trial period or have been terminated,
- commercial partners, customers, suppliers, consultants, members, and generally anyone with a vested interest in the Company, (hereinafter collectively referred to as "Recipients") who acquire information regarding the commission of crimes or behaviours that do not align with established rules of conduct.

Reports must be detailed and based on precise and consistent factual elements.

The channels designated for submitting reports ensure the confidentiality of the whistleblower's identity during the management of the report, in compliance with Article 6 of Legislative Decree 231/2001.

Furthermore:

- in the event of a report or complaint made in accordance with the forms and limits specified in Article 6 of Legislative Decree 231/2001, the pursuit of interests related to the integrity of the entity, as well as the prevention and repression of embezzlement, constitutes just cause for disclosing information subject to confidentiality obligations as outlined in Articles 326 (Disclosure and Use of Official Secrets), 622 (Disclosure of Professional Secrecy), and 623 (Disclosure of Scientific or Industrial Secrets) of the Italian Criminal Code, as well as Article 2105 (Obligation of Loyalty) of the Italian Civil Code,
- the aforementioned provision does not apply if the obligation of professional secrecy is imposed on those who become aware of the information through a professional consultancy or assistance relationship with the entity, company, or individual concerned,

- when information and documents communicated to the body responsible for receiving them are subject to business, professional, or official secrecy, any disclosure that exceeds the purpose of eliminating unlawful acts—particularly disclosure outside the communication channel specifically established for this purpose—constitutes a violation of the relevant confidentiality obligation.

Procedure

All Recipients of this Procedure are required to report any potential illegal activities that may violate the law, the Code of Ethics, or MEMC's policies.

Reporting possible violations is encouraged to enable the Company to investigate the matter and implement necessary corrective measures. Such measures help MEMC mitigate any risks or damages to individual employees, colleagues, and the Company itself.

To facilitate this process, individuals wishing to make a report may choose to use the communication channel accessible via the GRC CORA WHISTLEBLOWING portal, which allows for anonymous or named submissions.

Additionally, reporters may utilize other external reporting channels, provided that such reporting is done in compliance with applicable laws.

Forms of Protection

MEMC has assigned the management of reports to the members of the Supervisory Board, who act as investigators and are authorized to process personal data and have received the necessary training.

During the verification process, other internal Company personnel (such as structure managers) may be involved to request information or opinions; however, they will not have access to the details of the report or any information that could lead to the identification of the whistleblower.

The portal facilitates the following:

- separation of identifying information from the content of the report by adopting codes that replace identifying data, thereby allowing for anonymous processing of reports while enabling reconstruction of the whistleblower's identity only in permitted cases,
- transparent management of reports through a defined process communicated externally, including specific timelines for initiating and concluding investigations,
- confidentiality of report content throughout the entire management phase,
- implementation of secure protocols for data transport over the networks and use of encryption tools for report contents and any attached documentation,
- adequate methods for data and documentation storage (physical, logical, hybrid),
- confidentiality protection policies utilizing IT tools (decoupling whistleblower data from report information, encryption of data and attached documents),
- data access policies specifying authorized personnel (e.g., authorized officials, IT system administrators),
- provision for whistleblowers to monitor the progress of investigations through specific IT tools.
- assurance of anonymity by preventing tracing of the whistleblower's identity, except in cases involving disciplinary proceedings against the reported individual. The identity of the whistleblower cannot be disclosed without their consent unless their knowledge is essential for defending the accused, as provided by Article 54-bis, paragraph 2, of Legislative Decree 165/2001.
- implementation of auditing methods for system access, ensuring that consultations are reserved exclusively for authorized individuals,

- compliance with ANAC software model functions,
- allowance for entry of personal data even after submission of a report,
- HTTP Link Referrer Privacy measures to protect user privacy by implementing countermeasures for accessing external resources from within the platform, including obscuring Referrer application behaviours.
- advanced security Headers for all requests processed using advanced Headers such as Strict-Transport-Security and X-Content-Security-Policy.

The GRC CORA Whistleblowing platform is a web-based application accessible from any PC or mobile device (tablet, smartphone). The platform facilitates the submission, transmission, and receipt of reports, as well as allows for anonymous communication with the investigator.

MEMC ensures the confidentiality of the whistleblower's identity through appropriate procedures and prohibits any form of retaliation or discrimination against individuals who make reports, as well as against third parties associated with the whistleblower. Measures are also implemented to protect the rights of the individuals being reported.

All parties involved in the management of reports are required, within the limits established by law, to maintain confidentiality regarding the existence and content of the report and any activities conducted in this regard. They must also ensure the confidentiality of the identities of the whistleblower, the reported individual, and other involved parties, in accordance with current legislation.

Platform Security

Regarding cybersecurity aspects, the GRC CORA Whistleblowing platform undergoes periodic Application Security Assessments (ISO 27001, OWASP) in both pre-operational and operational environments.

The key security features of the platform are outlined below:

- Data Retention Policy: Each report stored in the database increases its attractiveness to potential hackers. Reports have a validity period that can be extended by the recipient; once expired, the report and all associated data are removed,

- Server Resiliency: The server is configured to mitigate D/DOS attacks. Any excessive requests from a single IP address that may indicate an attack are automatically blocked,

- Web Content Security: Communication between the front end and back end adheres to internationally recognized best practices, including the use of security headers and TLS 1.3 for communication encryption,

- File Encryption: Recipients may utilize their own PGP keys if available. Each file is stored using a randomly generated symmetric AES key, which is retained in RAM,

- GDPR Compliance: The Whistleblowing Platform complies with the General Data Protection Regulation (GDPR – EU Regulation 2016/679).

Subject of the Report

The reports pertain to facts (of any nature, including mere omissions) that have already occurred or are likely to occur, attributable to individuals associated with MEMC or to Third Parties, which may constitute illicit acts, irregularities, or conduct carried out in violation of:

- administrative, accounting, civil, or criminal offenses,
- violations of the organizational and management models established therein,
- Illicit acts that fall within the scope of European Union or national legislation relating to the following sectors: public procurement; financial services, products, and markets; prevention of money laundering and terrorist financing; product safety and compliance; transport safety; environmental protection; radiation protection and nuclear safety; food safety; public health; occupational health and safety; privacy protection; personal data protection; and the security of networks and information systems,
- acts or omissions that harm the financial interests of the Union,
- acts or omissions concerning the internal market,
- acts or behaviours that undermine the objectives or purposes of Union legislation,
- violations of Company Policies and the Company Code of Ethics.

Reports must concern facts of which the reporting individual has direct knowledge and must be based on well-founded reasons to believe that the information reported is true at the time of communication.

Reports should be made promptly upon gaining knowledge of the relevant facts to facilitate a factual verification. Communications, complaints, claims, or requests concerning matters outside the scope of these reports are excluded. Reports must not address personal grievances.

If it is necessary to send a communication unrelated to whistleblowing matters, such communication should be directed to the HR department of the Entity.

If the Supervisory Board receives a report not related to whistleblowing issues, it will forward it without delay, or in any case within seven (7) days, to the HR department. The HR department will respond within the same timeframe if a similar situation arises.

Reasons for Reporting

Reports made in good faith and in the interest of the common good, can facilitate the timely identification and rectification of irregular or illicit behaviours that may harm the Company and/or individuals.

Content of the Report

The reporting individual must provide all necessary information to enable the appropriate checks and investigations to verify the validity of the reported facts. In this respect, the report should preferably include the following elements:

a) identification of the person making the report (except in cases of anonymous reporting),
b) a detailed description of the reported facts, including, if known, the time and place in which they occurred,
c) personal details or other information that enables the identification of the individuals involved in the reported facts,
d) identification of any other individuals who may provide information regarding the reported facts,
e) names of any persons who are aware of the facts,
f) submission of any documents or multimedia files relevant to the reported facts,

g) any additional information that may serve as useful evidence regarding the existence of the reported facts.

Transmission of the Report

To enable the whistleblower to submit a report in a timely manner, MEMC has created a dedicated GRC CORA Whistleblowing portal, accessible via its website at the following web address: https://memc.openblow.it.

Upon accessing the portal, the whistleblower will be guided through a questionnaire consisting of both open and closed questions, which will facilitate the provision of essential details related to the report (such as facts, temporal context, economic significance, etc.).

The whistleblower may choose to disclose their identity or remain anonymous. In any case, they have the option to provide their personal details at a later time through the portal.

To protect the identity of the whistleblower, access to the portal operates under a "no-log" policy. This means that the Company's IT systems are unable to identify the access point to the portal (IP address), even if accessed from a computer connected to the company network.

Upon submission of the report, the portal will generate a unique 16-digit identification code (KEY CODE) for the reporting individual. This code, known only to the whistleblower, cannot be recovered if lost. The KEY CODE will be used by the whistleblower to access their report through the portal for purposes including:

- monitoring its progress,
- requesting further information via chat,
- providing their personal details,
- responding to any inquiries for additional information.

It is imperative that this KEY CODE is not lost under any circumstance.

Additionally, reports can be submitted through the following channels, although these are not preferred:

- by calling 800237555; in this case, the report will be recorded in writing by the investigator,
- by arranging a direct meeting with an investigator; such meetings will be recorded and signed.

Report Management

Reports submitted via the portal are received by the Supervisory Board, which is responsible for managing the reports and conducting follow-up checks in accordance with the principles of impartiality and confidentiality. The Supervisory Board will undertake any activities deemed appropriate in this regard. Specifically, reports are subject to the following investigation process:

- notify the reporting individual of receipt of the report within seven (7) days from the date of receipt,
- engage in discussions with the reporting individual and request additional information, if necessary,
- diligently follow up on the reports received,
- conduct any necessary investigations related to the report, including hearings and document acquisition,
- provide feedback to the reporting individual within three (3) months or, if justified and warranted, within six (6) months from the date of notification of receipt of the external report or, in the absence of such notification, from the expiration of the seven (7) days following receipt,
- communicate to the reporting individual the final outcome of the report.

If a report concerns one or more members of the Supervisory Board, it must be forwarded to the HR Managers/Directors.

Retention of the Report and Privacy

Internal and external reports, along with related documentation, are retained for as long as necessary to process the report and, in any case, for no longer than five (5) years from the date of communication of the final outcome of the reporting procedure. This retention is conducted in compliance with confidentiality obligations established by European and national legislation regarding personal data protection.

18. DISCIPLINARY SYSTEM

Function of the Disciplinary System

The function of a sanctions system (commensurate with the violation and possessing adequate deterrent efficacy) applicable in the event of violations of the rules set forth in this Model is to enhance the supervisory action of the Supervisory Board and to ensure the effective implementation of the Model itself.

The establishment of this disciplinary system constitutes, pursuant to Article 6, paragraph 2, letter e) of the Decree, an essential requirement of the Model for the purpose of exempting MEMC from liability.

The application of the disciplinary system and related sanctions is independent of the conduct and outcome of any criminal proceedings that may be initiated by judicial authorities, if the conduct in question also constitutes a relevant crime under Legislative Decree No. 231/2001.

This section also outlines the disciplinary measures that MEMC intends to adopt in cases of violations of the Model by directors, as well as representatives of other corporate bodies and employees, in coordination with the disciplinary system established by the National Collective Labor Agreement (CCNL) applicable to MEMC and in compliance with the procedures set out in Article 7 of Law No. 300 of 30 May 1970 (Workers' Statute).

Sanctions Against Employees Subject to the CCNL

Violations of the rules of conduct outlined in this Model by employees subject to the CCNL constitute a disciplinary offense.

The disciplinary measures that may be imposed on such employees—consistent with the procedures established in Article 7 of Law No. 300 of 30 May 1970 and any applicable special regulations—are those provided for by the disciplinary system of the relevant CCNL, specifically including:

- verbal warning,
- fine up to an amount equivalent to three (3) hours' pay and contingency allowance,
- written warning,
- suspension from work for up to three (3) days,
- dismissal with notice,
- dismissal without notice.

All provisions within the aforementioned CCNL relating to procedures and obligations for applying sanctions, remain valid and are hereby referenced.

Without prejudice to the obligations imposed on MEMC by the Workers' Statute, the following behaviours are subject to sanctions:

1. violation by the employee of internal procedures, including those explicitly outlined or referenced in this Model (e.g., failure to comply with prescribed procedures, failure to communicate required information to the Supervisory Board, failure to conduct necessary checks, etc.), or engaging in activities related to Sensitive Processes that do not conform to the provisions of the Model,

2. violation of internal procedures established in this Model or engaging in activities related to Sensitive Processes that do not comply with the Model and expose MEMC to an objective risk of committing one or more offenses,

3. engaging in activities related to Sensitive Processes that clearly contravene the provisions of this Model and are intentionally aimed at committing one or more crimes, even if such crimes are not ultimately committed,

4. engaging in activities related to Sensitive Processes that constitute clear violations of this Model, which could result in the application of sanctions against MEMC under Legislative Decree 231/2001,

5. making reports under whistleblowing regulations fraudulently or with gross negligence that are subsequently determined to be unfounded, following a finding of civil liability against the whistleblower or a conviction for defamation or slander, even if at first instance,

6. committing any act of retaliation that causes or may cause unjust harm, directly or indirectly, to the reporting individual and/or other individuals protected by law,

7. violating confidentiality obligations.

In cases involving employees, sanctions will be proportionate to the level of responsibility and autonomy of the individual, any prior disciplinary actions taken against them, the intentionality of their behaviour, and the severity of the conduct, particularly regarding the level of risk to which MEMC may reasonably be considered exposed under the Decree as a result of the censured behaviour.

Human Resources is responsible for:

- conducting disciplinary proceedings; and
- imposing sanctions.

Employees will receive immediate and comprehensive notification regarding any new provisions through an internal communication that clarifies the reasons for these changes and summarizes their content.

Measures Against Managers

In the event that Employees holding managerial positions violate the procedures outlined in this Model or engage in behaviours that do not comply with the provisions of the Model in connection with Sensitive Processes, MEMC reserves the right to implement appropriate measures against those directly responsible, in accordance with the provisions of the applicable National Collective Labor Agreement (CCNL) for Managers.

The Manager may also have any powers of attorney granted to them, revoked. In all cases, the Manager is obligated to compensate MEMC for any damages resulting from behaviours contrary to the provisions of the Model.

The authority to impose sanctions on Managers lies with the Board of Directors.

Measures Against Directors

In instances where one or more members of the Board of Directors violate the Model, the Supervisory Board will notify both the Board of Auditors and the entire Board of Directors. These bodies are required to take appropriate measures based on the severity of the violation, which may include convening a General Assembly to adopt suitable actions as provided by law, including revocation for just cause in serious cases.

Measures Against Auditors

If one or more Auditors violate this Model, the Supervisory Board will inform both the Board of Auditors and the Board of Directors, who will then take appropriate measures.

If the Board of Auditors also serves as the Supervisory Board, reports concerning one or more members will be directed to HR Managers/Directors, who will promptly inform the Board of Directors to ensure appropriate actions are taken.

Measures Against the Supervisory Board

In the event of a violation of the Model by one or more members of the Supervisory Board, the Board of Directors shall take appropriate action based on the severity of the incident.

In cases of serious violations, and without prejudice to the measures stipulated in existing contracts, the assignment may be revoked. This includes violations of measures designed to protect whistleblowers pursuant to the Whistleblowing Law.

Measures Against Consultants and Partners

Any violation by Consultants or Partners of the rules of the Model applicable to them, will be sanctioned in accordance with the specific contractual clauses included in their respective agreements.

The right to seek compensation remains unaffected if such behaviour results in damage to MEMC, particularly in cases where judicial authorities impose measures as provided for by the Decree.

Sanctions for Whistleblowing

MEMC is obliged to sanction the following behaviours:

1. making reports under whistleblowing regulations fraudulently or with gross negligence that are subsequently recognized to be unfounded, following an assessment that may include a first-instance judgment regarding the civil liability of the whistleblower, or a conviction for defamation or slander, even at first instance,

2. committing any act of retaliation that causes or may cause unjust harm, directly or indirectly, to the whistleblower and/or other individuals protected by law,

3. failing to establish reporting channels, failing to adopt whistleblowing procedures compliant with applicable legislation, and failing to conduct verification and analysis of reports,

4. engaging in behaviours that hinder or could hinder reporting,

5. violating confidentiality obligations.

Sanctions Against the Reporting Party

If internal investigations reveal that a report concerning unlawful conduct or a violation of the Model is unfounded, an inquiry will be conducted to determine if there is evidence of serious guilt or fraud regarding the improper reporting. If such evidence is found, the Board of Directors and/or the responsible corporate function will impose disciplinary actions as provided for by the applicable CCNL, existing contracts, and relevant laws. Additionally, if conditions warrant, criminal charges may be brought against the reporting party unless they present further evidence to support their report.

Any liability of the reporting party for slander, defamation, conceptual forgery, moral damage, or other civil or criminally relevant damage, remains unaffected.

Reporting Employee

In accordance with the principle of proportionality in disciplinary sanctions, the following measures may be imposed on Employees:

- a verbal or written warning issued if the reporting individual violates the whistleblowing procedures fraudulently or with gross negligence by submitting false reports,

- a fine, not exceeding three hours of hourly pay, applicable if the reporting individual repeatedly violates the whistleblowing procedures fraudulently or with gross negligence within a period of less than one year from the previous violation by submitting false reports,

- suspension from work and pay for a maximum of three days, applicable if the reporting individual violates the whistleblowing procedures fraudulently or with gross negligence by submitting false reports that also cause damage to the entity,

- dismissal without notice may be applicable if the reporting individual repeatedly violates the whistleblowing procedures fraudulently or with gross negligence within a period of less than one year from the previous violation by submitting false reports that also cause damage to the entity.

Reporting Manager

If managers are found to be responsible for violations of the whistleblowing procedures fraudulently or with gross negligence, measures deemed appropriate by the Board of Directors will be applied in accordance with the provisions of the applicable National Collective Labor Agreement (CCNL).

Reporting Director

If individual directors of MEMC are found responsible for violations of the whistleblowing procedures, the Supervisory Board will promptly inform both the Board of Directors and the Board of Auditors, enabling them to adopt any measures deemed appropriate and compliant with current legislation.

Third-Party Whistleblower

Third parties—such as members of the Supervisory Board and external collaborators—who violate whistleblowing procedures may face consequences as stipulated in their contractual clauses, which may include termination, withdrawal, and compensation for damages.

Sanctions Against Those Who Violate Whistleblower Protections

Violations of a whistleblower's confidentiality obligations or acts of retaliation or discrimination against a whistleblower will result in disciplinary liability pursuant to the applicable CCNL, current contracts, and relevant laws, without prejudice to any other forms of liability provided by law.