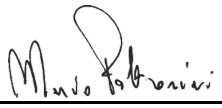
# WHISTLEBLOWING POLICY

| RESPONSIBILITY | FUNCTION | DATE | SIGNATURE |
|---|---|---|---|
| **Drawn up by:** | CCO<br>(Dania Pizzolato) | 11/07/2023 |  |
| **Approved by:** | President of the Company | 13/07/2023 |  |

## CONTENTS


1. PURPOSE ..... 3
2. DEFINITIONS ..... 3
3. SCOPE ..... 4
3.1. Scope of persons ..... 4
3.2. Scope of the reporting ..... 5
3.2.1. Relevant information ..... 5
3.2.2. Relevant breaches ..... 5
4. CHARACTERISTICS OF THE REPORTS ..... 8
5. ANONYMOUS REPORTS ..... 9
6. INTERNAL REPORTING CHANNEL ..... 9
7. RECIPIENTS OF THE REPORTS ..... 10
7.1. Conflict of interest situations ..... 10
7.2. Report sent to a non-authorised person ..... 10
8. MANAGEMENT AND ASSESSMENT OF THE REPORTS ..... 10
9. ARCHIVING AND STORAGE OF THE DOCUMENTATION ..... 12
10. PROTECTION OF THE WHISTLEBLOWER AND OTHER PERSONS ..... 12
10.1. Protection of confidentiality ..... 12
10.2. Protection from retaliation ..... 13
10.3. Notification of retaliations ..... 14
11. PROTECTION OF THE REPORTED PERSON ..... 14
12. DATA PROCESSING ..... 14
13. EXTERNAL REPORTING CHANNEL AT THE ANAC ..... 14
14. APPROVAL, MODIFICATION AND PUBLICATION OF THE POLICY ..... 16
15. OTHER USEFUL DOCUMENTATION ..... 16

## 1. PURPOSE

This Whistleblowing Policy (below, the "**Policy**") sets out the procedures for reporting information relating to various types of misconduct that may contribute to the emergence of risks and/or potentially adverse situations (so-called whistleblowing) for Mitsubishi Electric Europe B.V. Italian Branch (below, the "**Company**"). Specifically, this Policy, also by means of operational instructions, governs the process of sending, receiving, analysing, processing and managing the reports, the forms of protection of the confidentiality of the Whistleblowers, Facilitators and persons mentioned in the report, as well as the roles, activities and responsibilities of the persons involved.

This Policy implements the provisions of Legislative Decree 24 of 10 March 2023 (below, the "**Whistleblowing Decree**") implementing Directive (EU) 2019/1937 (the "**EU Directive**"), and Article 6, paragraph 2-bis of Legislative Decree 231 of 8 June 2001 (below, the "**231 Decree**"), as amended by the Whistleblowing Decree.

In order to promote lawfulness and transparency within its organization, the Company intends to accomplish the following through this Policy:

- removing any factor that may hinder or otherwise discourage the reporting of crimes, offences or breaches;
- promoting a virtuous working environment, by providing full protection and confidentiality for whistleblowers.

## 2. DEFINITIONS

The definitions of the terms used in this Policy are provided below. All terms beginning with a capital letter, unless defined in the body of this Policy, have the meaning given to them in this section.

- *CCO (Chief Compliance Officer)*: person responsible for the continuous assessment and verification of the effective and proper implementation of the management system for the prevention of corruption and the compliance programme adopted by the Company;
- *Code of Conduct*: document adopted by the Mitsubishi Electric Group as a uniform code of conduct that consolidates and summarises the main laws and regulations and social norms to be observed and respected by each and every employee of Mitsubishi Electric Group in the execution of business in order to achieve and pursue our Mission, Values, and Commitment;
- *231 Decree*: Legislative Decree 231 of 8 June 2001, as amended, concerning the regulation of the administrative liability of legal persons, companies and associations, including those without legal personality;
- *Whistleblowing Decree*: Legislative Decree 24 of 10 March 2023 concerning the protection of persons who report breaches of European Union law and containing provisions concerning the protection of persons who report breaches of national regulatory provisions;
- *EU Directive:* Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons who report breaches of European Union law;

- *Facilitators*: persons who aid the Whistleblower in the reporting process and who work in the same work-related context as the latter;
- *231 Model*: organisation, management and control model adopted by the Company in accordance with the 231 Decree;
- *Whistleblower*: the individual who makes the (internal or external) report or publicly discloses information on breaches acquired within his or her work-related context;
- *Reported Person*: the individual or legal person mentioned in the report or public disclosure as a person to whom the breach is attributed or as a person otherwise involved in the breach reported;
- *Supervisory Board or SB*: internal body responsible for supervising the functioning, proper implementation and the observance, management and control of the 231 Model and for ensuring its updating.

## 3. SCOPE

### 3.1. Scope of persons

The reports subject to this Policy may only be made by the following persons, connected to the Company by a legal relationship:

| Whistleblowers | Whistleblowing Decree |
|---|---|
| Employees | – Article 3, paragraph 3, letter c) |
| Self-employed workers, contractors and agents | – Article 3, paragraph 3, letters d) and e) |
| Freelancers and consultants | – Article 3, paragraph 3, letter f) |
| Volunteers and trainees | – Article 3, paragraph 3, letter g) |
| Shareholders/members and persons with administrative, management, supervisory or representation functions | – Article 3, paragraph 3, letter h) |

The protection afforded to Whistleblowers also applies if the report is made in the following cases:

a) pre-contractual stage, if information on the breaches was acquired during the recruitment process or at another stage prior to the establishment of the relationships described above;
b) during the probationary period;
c) after the termination of the legal relationship, if the information on the breaches was acquired in the course of that relationship.

Pursuant to the Whistleblowing Decree, the following persons will benefit from some of the protections afforded to Whistleblowers (see section 10 below):

| Additional protected persons (other than the Whistleblower) | Whistleblowing Decree |
|---|---|
| Facilitators | – Article 3, paragraph 5, letter a) |
| Persons in the same work-related context as the Whistleblower and who are linked to him or her by a stable emotional attachment or family relationship up to the fourth degree | – Article 3, paragraph 5, letter b) |
| Work colleagues of the Whistleblower who work in the same work-related context and have a regular and current relationship with the Whistleblower | – Article 3, paragraph 5, letter c) |
| Entities owned by the Whistleblower or entities that the Whistleblower works for | – Article 3, paragraph 5, letter d) |
| Entities operating in the same work-related context as the Whistleblower | – Article 3, paragraph 5, letter d) |

For a detailed description of the categories falling within the scope of persons covered by this Policy, see also the above-mentioned provisions of the Whistleblowing Decree and the guidelines issued by the ANAC in accordance with Article 10 of the Whistleblowing Decree (the "**ANAC Guidelines**").

### 3.2. Scope of the reporting

The scope of the reporting is the information on breaches of national or EU regulatory provisions that harm the public interest or the integrity of the Company as detailed below.

#### 3.2.1. Relevant information

The information to be reported must relate exclusively to breaches committed or, on the basis of concrete evidence, that may be committed within the Company, which the Whistleblower has become aware of within the work-related context.

| Relevant information | Irrelevant information |
|---|---|
| Well-founded suspicions that a breach has been or will be committed | Clearly unsubstantiated information |
| Information concerning conduct aimed at concealing breaches | Information that is already fully in the public domain |
| | Information obtained solely on the basis of unreliable gossip or rumours (so-called hearsay) |

#### 3.2.2. Relevant breaches

Below are the breaches that may be subject to reporting under this Policy.

| Breaches of national law | Breaches of European Union law |
|---|---|

| Cases | Example | Cases | Example |
|---|---|---|---|
| Relevant unlawful conduct pursuant to the 231 Decree (so-called predicate offences) and breaches of the 231 Model and the Code of Conduct not related to breaches of European Union law | – Undue receipt of payments<br>– Fraud against the State, a public entity or the EU in order to obtain public funds<br>– Computer fraud against the State or a public entity and fraud in public procurements<br>– Embezzlement<br>– Extortion<br>– Undue inducement to give or promise benefits<br>– Bribery and abuse of office<br>(see Article 24 et seq., 231 Decree) | Offences committed in breach of the EU regulations set out in Annex 1 to the Whistleblowing Decree and all the related national implementing provisions (Article 2, paragraph 1, letter a), no. 3), which therefore concern the following areas: public contracts; financial services, products and markets and prevention of money laundering and terrorist financing; product safety and compliance; transport safety; environmental protection; radiation protection and nuclear safety; food and feed safety and animal health and welfare; public health; consumer protection; privacy and personal data protection; and security of networks and information systems | – Environmental offences such as the discharge, emission or other release of hazardous materials into the air, soil or water or the unlawful collection, transport, recovery or disposal of hazardous waste. |
| | | Acts or omissions affecting the EU's financial interests (Article 325 TFEU | – Fraud<br>– Corruption or any other illegal activity related |

| | | | |
|---|---|---|---|
| | | countering fraud and illegal activities affecting the EU's financial interests) as identified in EU regulations, directives, decisions, recommendations and opinions (Article 2(1)(a)(4)) | to expenditure of the European Union |
| | | Acts or omissions relating to the internal market that jeopardise the free movement of goods, persons, services and capital (Article 26(2) TFEU). This includes breaches of EU competition and state aid rules or corporate tax rules or arrangements whose purpose is to obtain a tax advantage that defeats the object or purpose of the applicable corporate tax law (Article 2(1)(a)(5)). | |
| | | Acts or conduct that defeat the object or purpose of European Union provisions in the areas mentioned in the points above | Abusive practices (adoption of predatory pricing, target discounts, tying) in breach of the protection of free competition |

On the other hand, reports concerning the following content do not fall within the scope of this Policy and will therefore be considered irrelevant:

| Exclusions | Examples |
|---|---|
| Challenges, claims or demands linked to a personal interest of the Whistleblower or the person lodging a complaint with the judicial or accounting authorities that relate exclusively to his or her individual employment relations, or pertain to his or her relations with hierarchical superiors | Reports concerning labour disputes, discrimination between colleagues, and interpersonal conflicts between the Whistleblower and another worker |
| Reports of breaches where already mandatorily regulated by the European Union or national acts mentioned in Part II of the Annex to the Whistleblowing Decree or by national acts implementing the European Union acts mentioned in Part II of the Annex to the EU Directive, also when not mentioned in Part II of the Annex to the Whistleblowing Decree | Reports of breaches regulated in European Union directives and regulations and in the implementing provisions into Italian law that already ensure specific reporting procedures |
| Reports of breaches of national security, as well as procurement relating to defence or national security aspects, unless these aspects are covered by the relevant secondary legislation of the European Union | Procurement contracts envisaged in Articles 15 and 24 of Directives (EU) 2435 and 2536 of 2014 and Article 13 of Directive (EU) 2009/81 |

## 4. CHARACTERISTICS OF THE REPORTS

The report must be as detailed as possible and provide all the information necessary to enable the CCO to understand the subject matter of the report and conduct a proper examination, in order to assess the admissibility and merits of the report.

The report should therefore contain at least the following:

- personal details of the Whistleblower stating the function/activity carried out within the Company, except for the anonymous reports described in section 5;
- a clear and complete description of the precise and corroborating facts subject of the report and relating to the breaches identified in section 3.2;
- if known, details of the time and place in which the reported acts were committed;
- if known, the personal details or other information enabling identification of the person and/or persons to whom the reported acts are to be ascribed (e.g. position held and/or function/activity performed within the Company);
- details of any other persons who may provide information on the acts reported;
- details of any documents that may confirm the validity of the acts reported;
- any other information that may provide confirmation of the existence of the acts reported and, in general, any other information or document that may be useful in understanding the acts reported.

You are reminded that the report should not include personal data that are not clearly needed for the processing of the report. Where they are accidentally included, such personal data that are not clearly necessary will be deleted immediately by the Company.

Please also note that the encouragement to report any wrongdoing or breaches that someone has become aware of does not mean, nor does it in any way imply, that the Whistleblower is tacitly or implicitly authorised to carry out "investigations", particularly when improper or unlawful, in order to gather evidence of wrongdoing in the workplace.

## 5. ANONYMOUS REPORTS

Anonymous reports (i.e. reports lacking any reference enabling the identification of the Whistleblower), although not governed by this Policy, will be taken into account by the Company only if they are duly substantiated in accordance with the provisions of section 4 above and provided they are received by the Company in the manner set out in this Policy (see section 6 below)

In any event, Whistleblowers who are subsequently identified and retaliated against will be afforded the same protection recognised by the Whistleblowing Decree in the case of retaliatory measures taken by the Company.

## 6. INTERNAL REPORTING CHANNEL

Reports must be made directly to the CCO, by sending the report through the whistleblowing IT platform adopted by the Company as an internal reporting channel.

The procedure for submitting reports is detailed below.

| **Procedure for submitting reports** |
|---|
| 1) Go to the webpage page https://mee.parrotwb.app/ |
| 2) Select the language preference of Italian or English |
| 3) Click on "*Access*" |
| 4) Select the box "*Send a report*" or "*Send an anonymous report*" |
| 5) Fill in the report questionnaire, following the instructions provided in the questionnaire, as well as the instructions in section 4 |
| 6) Once you have checked the correctness of the data entered and successfully uploaded the documents you wish to attach to the report, make the submission by selecting the "*Send report*" box<br><br>N.B. Only if the report concerns the CCO or a member of the CCO's department/work team, the report may be sent to external members of the SB, by selecting the related option |

The reporting channel described above enables the protection, also through the use of encryption tools, of the confidentiality of the Whistleblower, the Reported Person and/or the person mentioned in the report, as well as the content of the report and the related documentation, regardless of whether or not the report is anonymous. All Whistleblowers are therefore invited to make non-anonymous reports.

The Company guarantees the possibility of making reports, also orally, at the request of the Whistleblower, by arranging an in-person meeting, set within a reasonable period of time, with the CCO, or in the event of a conflict of interest, with the persons mentioned in section 7.1.

## 7. RECIPIENTS OF THE REPORTS

The reports are received by the CCO, identified by the Chairman of the Company as the person responsible for implementing this Policy and managing and assessing the reports.

### 7.1. Conflict of interest situations

If the report concerns the CCO or a member of the CCO's department/work team, the Whistleblower may send the report to the external members of the SB (as indicated in section 6 above). These external members will handle the management and assessment of the reports, as set out in section 8, in lieu of the CCO, while ensuring the utmost confidentiality of the Whistleblower's identity (if known).

The CCO and members of the SB are required to immediately disclose any conflicts of interest, even if they arise at a later stage, and ensure that they are documented in the related report file. In such cases, where a conflict of interest is identified, the individuals involved will be replaced in their respective roles.

### 7.2. Report sent to a non-authorised person

If the internal report is submitted to a person other than the person identified and authorised by the Company, that person must immediately (or in any event within 7 days of receipt) send the report to the authorised person (CCO/external members of the SB), while also notifying the Whistleblower of this.

## 8. MANAGEMENT AND ASSESSMENT OF THE REPORTS

In managing and assessing the reports, the CCO (or, in the event of a conflict of interest, the SB) shall adopt the following procedure:

| Procedure for the Management and Assessment of the Reports | Timeframes (where applicable)/Notes |
|---|---|
| 1) The CCO provides the Whistleblower an acknowledgement of receipt of the report. | Within 7 days from the date of receipt of the report. |
| 2) While respecting the confidentiality of the Whistleblower and the data concerning the report, the CCO assesses the presence of the essential requirements of the report to verify its admissibility and validity in accordance with this Policy. | By way of non-limiting example, the CCO will consider reports inadmissible that:<br>a) are clearly unfounded due to the absence of facts capable of justifying the claims;<br>b) have generic content that does not enable an understanding of the facts; |

| | |
|---|---|
| | c) are accompanied by inappropriate or completely irrelevant documentation;<br>d) only contain attached documentation, without any description of the subject of the report;<br>e) clearly do not come under the responsibility of the CCO (in his or her role as the person responsible for the whistleblowing regulations under this Policy). |
| 3) The CCO maintains the communications with the Whistleblower and, where necessary, asks the Whistleblower for any additional information needed. | |
| 4) If the report is admissible, the CCO initiates the internal examination[1] of the reported acts or conduct in order to investigate their existence. | In examining the, the CCO may, where considered necessary or even only useful, use the support and assistance of other functions/offices (e.g. HR Department; SB, (...), (...)) and/or the Company's external consultants (e.g. lawyers, (...)), expressly authorised to process the data concerning the identity of the Whistleblower and any other information that may directly or indirectly reveal his or her identity, pursuant to Articles 29 and 32(4) of Regulation (EU) 2016/679 ("**GDPR**") and Article 2-quaterdecies of the Personal Data Protection Code set out in Legislative Decree 196 of 30 June 2003.<br><br>The persons involved in this phase will, in any case, be required to ensure the utmost |

[1] For example, the CCO, in compliance with the applicable regulations (including Articles 4 and 8 of the Workers' Statute, the GDPR, etc.), may carry out any activity considered appropriate for the purpose of:

- assessing the seriousness of the reported offences and breaches and considering their potential adverse consequences;
- identifying the activities to be carried out to ascertain whether the reported offences or breaches have actually been committed;
- conducting checks to determine whether the offence and/or breach has actually been committed, assessing whether it would be appropriate to interview the Whistleblower in order to obtain further clarifications, interviewing persons mentioned in the report who may have relevant information, gathering useful documentation or taking steps to locate and obtain it, interviewing (where deemed appropriate) the person indicated in the report as the perpetrator of the offence or breach (the Reported Person), etc;
- identifying, where necessary, the steps to be taken immediately to reduce the risk of the occurrence of adverse events or events similar to those reported.

| | |
|---|---|
| | confidentiality concerning the Whistleblower, the Reported Person, the Facilitator and any persons mentioned in the report and all the data relating to the report that come into their possession. |
| 5) The CCO maintains the communications with the Whistleblower and, where necessary, asks the Whistleblower for any additional information needed, while diligently following up on the reports. | If what has been reported is not adequately substantiated, the CCO may request additional information from the Whistleblower through the internal channel (box: "*Have you already made a report?*" - *Access the report*). |
| 6) The CCO sends an acknowledgement to the Whistleblower, detailing the measures taken (e.g. termination of the procedure due to lack of sufficient evidence) or to be taken to act upon the report (e.g. initiation of an internal investigation) and the reasons for the choice made, when this information does not prejudice the internal investigation. | Within 3 months from the date of acknowledgement of receipt or, in the absence of such acknowledgement, within 3 months from the expiry of the 7-day period from the submission of the report. |

## 9. ARCHIVING AND STORAGE OF THE DOCUMENTATION

In order to ensure the proper management and traceability of reports and the related investigative activity, the CCO archives the documentation relating to the report.

Specifically, the internal and external whistleblowing reports and related documentation are kept for as long as necessary for the processing of the report and in any case no longer than five years from the date of the notification of the final outcome of the whistleblowing procedure, in compliance with the confidentiality obligations set out in Article 12 of the Whistleblowing Decree and the principle set out in Article 5(1)(e) of Regulation (EU) 2016/679 and Article 3, paragraph 1, letter e), of Legislative Decree 51 of 2018.

## 10. PROTECTION OF THE WHISTLEBLOWER AND OTHER PERSONS

### 10.1. Protection of confidentiality

The Company ensures the confidentiality of the Whistleblower's identity as well as any other information or details in the report that could potentially disclose their identity, whether directly or indirectly, unless the Whistleblower gives his or her consent to the disclosure of such information (see Article 12, paragraph 2, of the Whistleblowing Decree).

In the event of disciplinary proceedings, if the report forms the basis of the claim, either in whole or in part, and the Whistleblower's identity is essential for the defence of the person involved in the disciplinary proceedings, the Company may use the report solely for those proceedings, provided the Whistleblower has explicitly consented to the disclosure of their

identity. In such case, the Company will send a request for consent to the Whistleblower (see Article 12, paragraph 5 of the Whistleblowing Decree).

Where the report is made by the Whistleblower by means other than the internal reporting channel described in section 6, but still meets the requirements for the reports governed by this Policy, the CCO and the other responsible persons will ensure the protection of the Whistleblower's confidentiality.

The Company also ensures the confidentiality of the identity of the Facilitators or of other persons implicated because they are mentioned in the report, until the conclusion of the proceedings initiated as a result of the report and in accordance with the same protections envisaged for the Whistleblower.

### 10.2. Protection from retaliation

The Company shall not engage in or threaten any retaliation against the Whistleblower as a result of the report.

By way of non-limiting example, the following are some of the conduct that are to be considered retaliatory (see Article 17, paragraph 4, of the Whistleblowing Decree):

- dismissal, suspension or equivalent measures;
- change of duties, transfer of place of work, reduction of salary, change of working hours;
- suspension of training or any restriction of access to training;
- negative performance assessments or employment references;
- adoption of disciplinary measures or other sanctions, including fines;
- coercion, intimidation, harassment or ostracism;
- discrimination or unfair treatment;
- early termination or cancellation of a contract for the supply of goods or services.

The Whistleblower will have access to the protections provided for by the Whistleblowing Decree (Articles 16 et seq.) in the event of a breach of the above-mentioned prohibition of retaliation, where the following conditions are met:

a) there must be a consequential relationship between the report and the unfair conduct/act/omission suffered by the Whistleblower, in order for these to be considered retaliation pursuant to the Whistleblowing Decree;
b) at the time of the report, the Whistleblower had reasonable grounds to believe that the information on the reported breaches fell within the scope of section 3.2. As stated above, mere suppositions or hearsay are not sufficient;
c) the reports must be made on the basis of the procedure set out in the sections above (see section 6 in particular).

In the absence of any of the above conditions, the report will not fall within the scope of this Policy and the Whistleblowing Decree.

The protections provided for in Article 17, paragraphs 2 and 3 of the Whistleblowing Decree also apply to persons other than the Whistleblower identified in section 3.1 of this Policy (e.g. Facilitators, colleagues of the Whistleblower, etc.).

### 10.3. Notification of retaliations

Alleged retaliations as defined in section 10.2 must be notified by the Whistleblower to the ANAC (National Anti-Corruption Authority), which is tasked with establishing whether they are actually consequential to the report.

For information on the procedure to be followed for the purposes of the aforementioned communication, see the ANAC Guidelines available at the following link: *https://www.anticorruzione.it/-/schema.linee.guida.whistleblowing*

## 11. PROTECTION OF THE REPORTED PERSON

The Company also ensures the confidentiality of the identity of the Reported Person, the Facilitators or other persons implicated because they are mentioned in the report, until the conclusion of the proceedings initiated as a result of the report and in accordance with the same protections envisaged for the Whistleblower.

## 12. DATA PROCESSING

The processing of the personal data of the Whistleblower, the Reported Person, the Facilitators and any other person involved and/or mentioned in the reports is carried out by the Company – as controller – in accordance with the prevailing law and the privacy policy available at the following link: https://mee.parrotwb.app/

The rights awarded by Articles 15-22 of the GDPR (i.e. the right of access to personal data, the right to rectification, the right to erasure or so-called right to be forgotten, the right to restriction of processing, the right to data portability, the right to object to the processing, and the right not to be subject to automated decision-making) cannot be exercised by the Reported Person or by any persons mentioned in the report – by request to the controller or by complaint to the competent supervisory authority pursuant to Article 77 of the GDPR – if the exercise of those rights could result in an actual and concrete prejudice to the confidentiality of the identity of the Whistleblower.

## 13. EXTERNAL REPORTING CHANNEL AT THE ANAC

Subject to the preference for the internal channel indicated in section 6, the Whistleblowing Decree provides for the possibility, solely upon the occurrence of certain circumstances precisely identified and categorised by the Whistleblowing Decree, of making a report through an external channel managed directly by the ANAC (https://servizi.anticorruzione.it/segnalazioni/#!/#%2F).

The Whistleblower may only make an external report if the report relates to a breach of EU law (as identified in section 3.2.2)[2] and if the following conditions are met at the time of its submission:

[2] The external reporting channel cannot therefore be used in the event of a report concerning unlawful conduct relevant for the purposes of the 231 Decree (so-called predicate offence) or a breach of the 231 Model and/or the Code of Conduct.

| Scope of the external reports to the ANAC | Alternative conditions for using the ANAC external reporting channel | Examples |
|---|---|---|
| Breaches of European Union law | 1. The internal channel described in section 6, even though mandatory, is not active or, even if activated, does not comply with the provisions of the Whistleblowing Decree (with reference to the persons and the procedures for submitting internal reports, which must be able to guarantee the confidentiality of the identity of the Whistleblower and the other protected persons). | |
| | 2. The Whistleblower has already made an internal report and it has not been acted upon by the designated person or office. | The report has not been processed within a reasonable time. |
| | 3. The Whistleblower has reasonable grounds to believe, on the basis of the specific circumstances attached and verifiable information and, therefore, not mere conjecture, that if he or she made an internal report:<br>– it would not be effectively acted upon;<br>– or it could lead to the risk of retaliation. | – The ANAC is better placed to address the specific breach, particularly in matters falling within its remit.<br>– Breach of the obligation to maintain the confidentiality of the Whistleblower's identity. |
| | 4. The Whistleblower has good reason to believe that the breach may constitute an imminent or obvious danger to the public interest. | The breach requires urgent action to safeguard the health and safety of persons or to protect the environment. |

Therefore, unlawful conduct relevant for the purposes of the 231 Decree (so-called predicate offences) and breaches of the 231 Model that are not attributable to breaches of EU law can only be reported through the Company's internal channel described in section 6.

Following the report, the ANAC must:

- give notice to the Whistleblower of receipt of the report within 7 days from the date of its receipt, unless the Whistleblower explicitly requests otherwise or unless the ANAC considers that such notice would compromise the protection of the confidentiality of the Whistleblower's identity;
- maintain the communication with the Whistleblower and, where necessary, request additional information from the Whistleblower;
- diligently act upon the reports received;
- carry out the necessary preliminary examination to follow up on the report, also by conducting interviews and obtaining documents;
- provide a response to the Whistleblower within 3 months or, if there are justified and substantiated reasons, within 6 months from the date of acknowledgement of receipt of the external report or, in the absence of such notice, within 7 days of receipt;
- notify the Whistleblower of the final outcome of the report.

## 14. APPROVAL, MODIFICATION AND PUBLICATION OF THE POLICY

This Policy was approved by the President of the Company on 13 July 2023 and is reproduced in the 231 Model by reference to the link where it is published.

This Policy becomes effective on 15 July 2023.

The Company reserves the right to amend this Policy at any time.

This Policy will be published on the Company's website and on the page of the online platform of the internal reporting channel, in addition to being available on the company intranet and on display in a visible and easily accessible place within the Company's premises (company notice board).

## 15. OTHER USEFUL DOCUMENTATION

For any further information on the whistleblowing rules, please consult the following documentation:

EU Directive

Whistleblowing Decree

231 Decree

ANAC Guidelines

* * *

Vimercate (MB), 13 July 2023

## PRIVACY POLICY - WHISTLEBLOWING

**Privacy Notice pursuant to Articles 13 and 14 of Regulation (EU) 2016/679 (GDPR)**

### 1. CONTROLLER

The controller, pursuant to Articles 4 and 24 of the GDPR, is **Mitsubishi Electric Europe B.V. Italian Branch,** with branch office in Vimercate (MB), Via Energy Park no. 14, in the person of its legal representative, who can be contacted by e-mail at privacy@it.mee.com (below, the **Company**).

The Company has also appointed a **Data Protection Officer (DPO)**, pursuant to Articles 37 - 39 of the GDPR who can be contacted at the email address: MEU.DMO@mecc.mee.com

### 2. TYPE OF PROCESSED DATA

**"Personal Data":** any information regarding an identified or identifiable natural person (**Data Subject**); a natural person is considered identifiable where they may be directly or indirectly identified, with particular reference to identifiers such as a name, an identification number, location data, an on-line identifier or one or more characteristic elements of the individual's physical, physiological, genetic, psychological, economic, cultural or social identity.

"**Processing**": means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

As concerns the processing under this Privacy Policy, the data processed will be those relating to the reports made by reporters (so-called whistleblowers), including the content of the reports, which may include personal data relating to third parties.

As applicable, the personal data are and will be collected by the Company directly from the Data Subject or from the reporting person (the **Whistleblower**) who submits a report through the whistleblowing procedure.

The personal data relating to the Whistleblower may include:

- Name, surname, function/activity within the Company, gender

- Contact details: e.g. telephone number (cell phone), e-mail address, work address

- Employment details (e.g. type of contract and workplace)

- Method and time of the report (including the place of origin)

- Other information provided by the Data Subject.

The personal data relating to the reported person (the **Reported Person**) may include:

- Name, Surname, job title and/or function/activity performed within the Company, gender

- Employment details (e.g. type of contract and workplace)

- Any disciplinary measure imposed on him or her or previous alleged breaches or incidents

- Description and circumstances of the alleged breaches or incidents

- Other information and personal data in the report

- Other personal data required for compliance with a provision of a relevant authority, a collective employment agreement or a legal obligation.

The personal data of individuals assisting the Whistleblower in the reporting process and working in the same work-related context as the Whistleblower (the **Facilitators**), may include:

- Name, Surname, job title and/or function/activity performed within the Company, gender.

The personal data of any other persons mentioned in the report may include:

- Name, Surname, job title and/or function/activity performed within the Company, gender

- Employment details (e.g. type of contract and workplace)

- Any disciplinary measure imposed on him or her or previous alleged breaches or incidents

- Other information and personal data in the report

- Other personal data required for compliance with a provision of a relevant authority, a collective employment agreement or a legal obligation.

The Whistleblower is requested not to include any sensitive data in the report (e.g. relating to state of health, religious beliefs and political opinions) that are not clearly necessary for the purposes of the report, and if such data are provided and are not strictly necessary, they will be deleted immediately.

If the report is made anonymously, no personal data of the Whistleblower will be processed (unless the Whistleblower is subsequently identified), but the data of the Reported Person and of other persons involved and/or mentioned in the report may be processed.

## 3. PURPOSE AND LEGAL BASIS OF THE PROCESSING, STORAGE PERIOD, NATURE OF THE DATA PROVISION

**PURPOSE OF THE PROCESSING**: The personal data will be processed in compliance with the conditions of lawfulness, pursuant to Article 6 of the GDPR, for the following purpose:

A) Receipt and management of whistleblowing reports, in accordance with Article 8 of the Company's Whistleblowing Policy.

**LEGAL BASIS**: The processing is necessary to comply with a legal obligation of the controller in accordance with Legislative Decree 24/2023. The processing is therefore lawful in accordance with Article 6(1)(c) of the GDPR.

**DATA STORAGE PERIOD**: The personal data are kept for the time necessary to process the report and, in any case, no longer than 5 years from the date of the communication of the final outcome of the reporting procedure.

In the event of a court case, the above-mentioned time limit may be extended in accordance with the limitation period established by law for enforcing or defending a legal claim against the Data Subject and/or third parties.

Personal data which are clearly not relevant for the management of a specific report shall not be collected or, if accidentally collected, shall be erased immediately.

**NATURE OF THE PROVISION**: The provision of personal data of the Reported Person and/or of any persons mentioned and/or involved in the report is necessary for the proper management of the report. A refusal may therefore result in the report not being managed in accordance with the Company's Whistleblowing Policy.

The provision of the Facilitator's personal data is optional. Therefore, any refusal to provide such data does not result in any consequences.

The provision of the Whistleblower's personal data is optional. If the report is made anonymously, no personal data of the Whistleblower shall be processed, unless the Whistleblower is subsequently identified.

## 4. RECIPIENTS OR CATEGORIES OF RECIPIENTS OF DATA

The personal data will not be publicly disclosed. However, the personal data may be communicated to:

- the CCO, identified by the Chairman of the Company as the person responsible for implementing the Company's Whistleblowing Policy and managing and assessing the reports. The CCO will act as the processor's representative duly appointed by the Company;

- the members of the Supervisory Board (SB), if the report concerns the CCO or a member of the CCO's department/work team. As applicable, the members of the SB may act as the processor's representatives or processors duly appointed by the Company;

- employees or collaborators of the Company that may be engaged by the CCO or the SB in the internal investigations, who will act as the processors' representatives duly appointed by the Company;

- the Company's external consultants that may be engaged by the CCO or the SB in the internal investigations, who will act as controllers duly appointed by the Company.

Finally, the Company may disclose personal data to the competent legal authorities in response to summonses, to comply with orders issued by courts or other legitimate requests from competent authorities, and to enforce or exercise its rights or defend itself in legal proceedings.

In accordance with Article 7.2 of the Company's Whistleblowing Policy, if the internal report is submitted to a person other than the person identified and authorised by the Company, that person will immediately forward the report to the competent person (CCO/external members of the SB), while also notifying the Whistleblower of this.

## 5. DATA TRANSFER TO A THIRD COUNTRY AND/OR AN INTERNATIONAL ORGANISATION AND GUARANTEES

The personal data collected and processed in the management of whistleblowing reports will under no circumstances be transferred outside the EEA countries.

## 6. WILL AUTOMATED DECISION-MAKING PROCESSES BE USED?

The collection and processing of personal data will be carried out by manual, computerised and electronic means, using procedures strictly related to the purposes of the processing and, in any case, in a way that guarantees the confidentiality and security of the data, including the confidentiality of the Whistleblower, the Reported Person, the Facilitator and any other persons mentioned in the report.

No fully automated decision-making processes are used.

## 7. RIGHTS OF THE DATA SUBJECTS

The Data Subject may assert his or her rights in accordance with Articles 15-22 of the GDPR by contacting the Controller by e-mail to privacy@it.mee.com or by writing to the contacts listed in section 1 of this Privacy Notice.

The Data Subject has the right, at any time, to request any of the following rights from the Controller: right of access (Article 15), right to rectification (Article 16), right to erasure (Article 17), or right to restriction of processing (Article 18). The controller shall communicate (Article 19) any rectification or erasure of personal data or restriction of processing to each recipient to whom the personal data have been disclosed. The controller shall inform the Data Subject about those recipients if the Data Subject requests this. If the Data Subject believes that the processing of their personal data by the Controller breaches the provisions of the GDPR, the Data Subject has the right to lodge a complaint with the Supervisory Authority, in particular in the Member State where they habitually work or reside or the place where the alleged breach of the regulation took place (the contact details of the Data Protection Authority are available at the following link: https://www.garanteprivacy.it/home/footer/contatti), or to take appropriate legal actions.

Please note, however, that the rights awarded by Articles 15-22 of the GDPR cannot be exercised by the Reported Person or by any persons mentioned in the report – by request to the controller or a complaint to the competent supervisory authority pursuant to Article 77 of the GDPR – if the exercise of those rights could result in actual and concrete prejudice to the confidentiality of the Whistleblower's identity.

Date of update: 13 July 2023