REPORT MANAGEMENT PROCEDURE COMPLIANT WITH THE PROVISIONS OF LEGISLATIVE DECREE No. 24 OF 10 March 2023 (WHISTLEBLOWING)

Revision n. 00	Approved by the Board of Directors	on 15.06.2023
Revision no. 01	Approved by the Board of Directors	on 08.08.2023

TABLE OF CONTENTS

1. DEFINITIONS AND ACRONYMS

"**ANAC**": Italian National Anti-Corruption Authority.

"**MISSONI**" and/or the "**Company**": Missoni S.p.A.;

"**Code of Ethics**": the Code of Ethics of the Missoni Group;

"**Work context**": the work or professional activities, present or past, carried out within the framework of the relationships referred to in articles 4 and 7.2, letter c) of the Policy, through which, regardless of the nature of such activities, a person acquires information on violations and within which he/she could risk retaliation in the event of making a report or public disclosure or complaint to the judicial or accounting authority;

"**Decree 231**": Legislative Decree no. 231 of 8 June 2001 and subsequent amendments and additions;

"**Whistleblowing Law**": Legislative Decree no. 24 of 10 March 2023;

"**Model 231**": the organisation, management and control model provided for by Decree 231 and adopted by Missoni S.p.A.;

"Privacy Policy": Regulation (EU) 2016/679 and Legislative Decree no. 196 of 30 June 2003.

"**Supervisory Body or SB**": the Supervisory Body established pursuant to Decree 231/2001, the individual members;

"**Person involved**": the natural or legal person mentioned in the internal or external report or in the public disclosure as the person to whom the violation is attributed or as a person involved in the violation reported or publicly disclosed;

"**Procedure**": this procedure;

"**Retaliation**": any behaviour, act or omission, even if only attempted or threatened, carried out as a result of the report, complaint to the judicial or accounting authority, or public disclosure, and that causes or may cause, both directly and indirectly, unjust damage to the reporting person or the person who filed the complaint;

"**Report (s)**": communication of violations according to the definitions and through the use of the channels referred to in the Whistleblowing Law;

"**Report (s) 231**": communication of violations referred to in article 5, no. 1) of the Procedure;

"**Reporting (s) of violations of European Union provisions**": communication of the violations referred to in article 5, no. 2), 3) and 4) of the Procedure;

"**Reporting party**" and/or "**Whistleblower**": the natural person, among those indicated in Article 4 of this Procedure, who makes the report;

"**Follow-up**": the action taken by the person entrusted with management of the reporting channel to verify the existence of the reported facts, the outcome of the investigations and any measures adopted;

"**Violation (s)**": conduct, acts and omissions concerning the matters indicated in article 5 of this Procedure.

2. DESCRIPTION OF THE PROCEDURE

The purpose of the Procedure is to regulate and discipline the methods of communication and management of reports concerning violations of national regulatory provisions and violations of EU regulatory provisions, which harm the public interest or the integrity of MISSONI, of which the subjects identified below have become aware within the Company's work context, in order to ensure that all appropriate actions are taken and all measures implemented to address the violations reported and, consequently, to avoid their recurrence. In particular, the Procedure transposes the provisions of Legislative Decree no. 24 of 10 March 2023, containing "*Implementation of 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 Union law and containing provisions concerning the protection of persons who report violations of national regulatory provisions*".

This tool is aimed at preventing the emergence of irregularities within the organisation by promptly intercepting divergent behaviour in order to remedy it, but also to involve senior management, employees and anyone in a relationship based on interest with MISSONI, in an effort to combat *non-compliance* through active and responsible participation.

To this end, the Procedure sets out, in accordance with the Whistleblowing Law, to define the following operational aspects:

- Identification of individuals/entities who can make the reports;
- Identification of the subject of the reports and their basic content;
- Identification of the different forms of reporting and related channels;
- Identification of the recipient of internal reports;

- Indication of the methods used to make the reports;
- Indication of management methods for internal reports;
- Indication of forms of protection for the whistleblower.

3. REGULATORY FRAMEWORK

The term *"whistleblowing"* refers to the legal provision aimed, on one hand, at defining the methods of reporting illegal conduct in a given context (such as work) and, on the other, at protecting the reporting party from possible retaliation.

The Whistleblowing Law has transposed into the Italian legal system Directive (EU) 2019/1937 of the European Parliament and of the Council, of 23 October 2019, concerning the protection of persons who report breaches of Union law and containing provisions concerning the protection of persons who report violations of national regulatory provisions, introducing a "generalised" institution for reporting violations of national and European Union regulations that harm the public interest or the integrity of the public administration or private body, of which the persons referred to in article 3 of the Whistleblowing Law have become aware in a public or private work context.

This legislation replaces and repeals the previous discipline provided for in Article 54-bis of Legislative Decree no. 165 of 30 March 2001, Article 3 of Law no. 179 of 30 November 2017 and Article 6, paragraphs 2-ter and 2-quater, of Legislative Decree no. 231 of 8 June 2001, which, respectively in the public and private spheres, limited the subject of the reports to irregularities in the management or organisation of the activity of an institution, to the extent that such irregularities constituted episodes of so-called *Maladministration* (especially in the public sector) or violations of the organisational model and/or the code of ethics, as well as circumscribing the categories of whistleblowers and the reporting channels.

The Whistleblowing Law expands the subject of reports, and extends the category of whistleblowers to whom the protections provided for therein apply; identifies three reporting channels; specifies the methods to be used for handling reports; regulates the identification of the recipient of reports; and provides for a specific sanctioning regime, which punishes, *inter alia*, entities that do not have a "*compliant*" reporting system with the relative regulation.

4. PERSONS WHO MAY MAKE REPORTS

Reports can be made by the following persons:

- employees of MISSONI S.p.A., also during the probationary period;

- self-employed workers, individual entrepreneurs, collaborators with whom MISSONI S.p.A. has relationships for the provision of services, the execution of works, the supply of goods;
- the holders of an agency agreement, commercial representation agreement and other relationships of continuous and coordinated collaboration, according to the *pro tempore* laws in force, who carry out their work at MISSONI S.p.A.;
- workers or collaborators, who carry out their work at legal entities, who provide goods or services or carry out works for MISSONI S.p.A.;
- freelancers and consultants who provide services for MISSONI S.p.A.;
- volunteers and trainees, both paid and unpaid, who work at MISSONI S.p.A.;
- the shareholders of MISSONI S.p.A.;
- the directors and statutory auditors, and the auditing company of MISSONI S.p.A., or any person who *de facto* exercises functions of administration, direction, control and supervision at MISSONI S.P.A.

In addition, the report can also be made:

a) when the legal relationship with the Company has not yet started, if the information on the violations was acquired during the selection process or at other pre-contractual stages;
b) after the termination of the employment relationship with MISSONI, if the information on the violations was acquired during the course of the work relationship.

5. SUBJECT OF THE REPORTS

Reports may concern violations of national or European Union regulatory provisions that harm the public interest or the integrity of MISSONI S.p.A., of which the whistleblower has become aware within the Company's work context.

Specifically, violations are behaviours, acts or omissions, which consist of:

1) relevant unlawful conduct pursuant to Decree 231, or non-compliance with Model 231, the Code of Ethics, and policies and procedures adopted by the Company;
2) offences falling within the scope of the acts of the European Union, in violation of national and European provisions, relating to the following sectors: public procurement; 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; protection of privacy and protection of personal data and

security of networks and information systems; acts or behaviours that compromise the interests protected by the European Union in these sectors are also included;

3) acts or omissions that damage or, in any case, compromise the financial interests of the European Union;
4) acts or omissions concerning the internal market of the European Union, including breaches of European Union competition and state aid rules, as well as breaches concerning the internal market of the European Union related to acts that violate corporate tax rules or mechanisms whose purpose is to obtain a tax advantage that defeats the object or purpose of the applicable corporate tax legislation (and therefore, the use of avoidance mechanisms).

The whistleblowing reports relating to the matters indicated above may also concern well-founded suspicions concerning violations committed or that, on the basis of concrete elements, could be committed at MISSONI, as well as information concerning conduct aimed at concealing such violations.

The following reports **are not subject** to this Procedure and are not addressed by the provisions of the Whistleblowing Act:

- disputes, claims or requests related to a personal interest of the whistleblower, or inherent to their employment relationships with hierarchically superior figures (such as, for example, complaints of a personal nature by the whistleblower, a disagreement between two employees or relationships with the hierarchical superior or with colleagues, or a situation of doubt regarding their job growth prospects and, more generally, claims/requests that fall within the discipline of the employment relationship, etc.).

The topics referred to in the previous point must not be reported through the channels described below. These situations can of course be discussed and addressed through the other available channels (for example, interviews with the line manager).

It should be noted that any reports that do not concern aspects falling into any of the categories indicated above will not be considered.

5.1 Basic content of the report

In order to carry out an adequate investigation in this regard, it is essential that the report contains at least the following elements:

- a clear and complete description of the facts being reported, expressly stating that the report refers to MISSONI S.p.A.;
- reference to any documents that may substantiate these facts;

- if known, the time and place in which the reported facts took place;
- if known, general information or other elements (such as the qualification and service in which the activity is carried out) that allow identification of the person involved;
- any other information that may usefully substantiate the reported facts.

Reports made by using the methods provided below (in particular internal reporting), but without any element that allows their author to be identified (*i.e.* anonymous reports), will be taken into consideration provided that they are adequately substantiated, detailed and based on precise and concordant factual elements (without generic or confusing content), so as to allow evaluation and assessment of the case (for example, the mention of specific company areas, procedures or particular events, etc.).

In all cases, it **is forbidden to**:

- use insulting language;
- submit reports for purely defamatory or slanderous purposes;
- submit reports relating exclusively to aspects of private life, and having no direct or indirect association with business activities. Such reports will be considered even more serious when they involve sexual, religious, political and philosophical habits and beliefs.

6. TYPES OF REPORTING

Depending on the means of communication used, in accordance with the provisions indicated below, the whistleblower may rely on:

- **internal reporting**: written or oral communication of information on violations through the use of the channels referred to in paragraph 6.1;
- **external reporting**: written or oral communication of information on violations through the use of the channel referred to in paragraph 6.2;
- **public disclosure**, providing information about violations in the public domain through the public press or electronic means, or in any case through communication methods allowing to reach a large number of people.

In any case, the whistleblower may always report violations to the judicial or accounting authority.

6.1 Internal reporting

a) Recipient of the report

The Recipient of the report is the Supervisory Body of MISSONI S.p.A. (hereinafter the "Channel Manager").

b) Reporting channels

The channels for making reports are as follows:

i) Written communication

- **Online portal:**
  https://areariservata.mygovernance.it/#!/WB/missoni
  The portal is managed in full respect of confidentiality rules by a third party independent of the Company. The Whistleblower must indicate that this is a report relating to the Company.

- **Regular mail** to be sent to the following address: Mario Ippolito c/o Carnelutti Law Firm – Via Principe Amedeo 3, Milan, 20121. In view of the confidentiality protocol of the report as handled by the Channel Manager, it is necessary that the report be sent in two closed envelopes: the first with the identification data of the reporter together with a photocopy of an identification document; the second with the report, in order to keep separate the identification data of the reporter from the report itself. Both must then be placed in a third closed envelope bearing the words "Strictly confidential. Reserved to the Channel Manager - whistleblowing", in order to guarantee maximum confidentiality; in the event of use of this channel, the Whistleblower must indicate in the communication an address / email to which the Channel Manager can send proof of receipt of the Report and provide all relative feedback pursuant to article 5 of the Whistleblowing Law, as indicated below.
  If no address / email is indicated, the Channel Manager will examine the Report in compliance with the conditions referred to in Article 5 of the Procedure, without any obligation to send proof the receipt or to give feedback as provided for by the Whistleblowing Law.

ii) Oral communication

- **Direct meeting**: the whistleblower, using the above channels, may request a direct meeting with the Channel Manager, to make the report orally, provided that he/she indicates in the request a telephone number at which he/she can be contacted. The meeting will be scheduled within 15 (fifteen) days of receipt of the request.

  With the consent of the whistleblower, oral communication of the report is documented by the Channel Manager, by recording on a device suitable for storage and listening or by

keeping written minutes. In the event of a written report, the whistleblower may verify, correct and confirm the meeting report by signing it.

c) Subject of the report

Model 231 reports and reports of violations of European Union provisions may be communicated through internal reporting.

d) Management of the report and outcome of the investigation phase

Following the report, the Channel Manager:

- issues a notice of receipt of the report to the whistleblower within seven days of the date of receipt, where possible in accordance with the indications provided above;
- issues the Policy on the processing of personal data (according to the Attached document) to the whistleblower;
- holds discussions/maintains communication with the whistleblower and may request additional information from the latter, if necessary; the discussions/communication and integrations can take place, at the request of the whistleblower, through the acquisition of written observations and documents;
- duly follows up on the reports received;
- provides information relating to all follow-up activities carried out or intended to be carried out regarding the report ("feedback") within three months from the date of the notice of receipt or, in the absence of such notice, within three months from the expiry of the seven-day period from submission of the report.

It is understood that proof of receipt and feedback will not be provided in the event of an anonymous report or failure to indicate an address by the whistleblower.

For the purposes of the investigation phase, the Channel Manager may also rely on the support and collaboration of the competent bodies. In the event that specialist support is necessary (technical, legal, etc.), this activity may also be carried out with the involvement of an external consultant selected by the Channel Manager. In this case, subject to a commitment to professional confidentiality, all the documentation necessary to carry out the investigation may be sent to the consultant.

The report will be considered well-founded where it is inherently plausible, supported by documentary evidence or other evidence (such as, for example, precise reference to other persons who can confirm it).

The validity of the circumstances represented in the report must, in any case, be assessed, in compliance with the principles of impartiality and confidentiality, by the Channel Manager, who carries out any activity deemed appropriate, including the hearing of any other persons eligible to provide information on the reported facts.

At the end of the investigation phase, the Channel Manager, in addition to providing feedback to the whistleblower, also communicates the outcome to those corporate subjects appointed to take the appropriate measures in this regard, namely:

- the Chief Executive Officer, the HR Manager, the Manager of the structure to which the person responsible for the established violation belongs (if the person responsible is an employee or collaborator of MISSONI);
- the Managing Director, the Manager of the structure with which the person responsible for the established violation interacts, if the person responsible is a supplier/consultant of MISSONI;
- the Chief Executive Officer, in all other cases, or the Chairman/other director, if the report concerns the Chief Executive Officer.

In addition to the above, the outcome of the investigation phase of the report may be communicated to the Board of Directors of the Company and to the competent bodies so that they adopt any further measures and/or actions that may be necessary to protect MISSONI in the specific case.

If, for the purposes of the investigation, it is necessary to reveal the identity of the whistleblower, the provisions of Article 7.1 below shall apply.

6.2 External reporting

a) Conditions for making an external report

The whistleblower may make an external report (relying on the protection provided by the Whistleblowing Act) if, at the time of its submission, one of the following conditions is met:

- the whistleblower has already made an internal report pursuant to Article 6.1 of the Procedure, which has not been followed up;
- the whistleblower has reasonable grounds to believe that, if he/she made an internal report, it would not be effectively followed up or that said report may result in a risk of retaliation;
- the whistleblower has reasonable grounds to believe that the breach may constitute an imminent or obvious danger to the public interest.

b) Recipient

The recipient of the external report is ANAC. The external report submitted to a subject other than ANAC is transmitted to the latter within seven days from the date of receipt, providing a notice of its submission to the whistleblower at the same time.

c) Reporting channels and related implementation methods

The whistleblower can acquire information on implementation methods at www.anticorruzione.it in order to submit an external report.

d) Subject of the report

Reports of violations of European Union provisions may be communicated through external reporting.

e) Management of the report by ANAC

Following receipt of the report, ANAC carries out the following activities:

- gives notice to the whistleblower of receipt of the external report within seven days from the date of its receipt, unless explicitly requested otherwise by the whistleblower or unless ANAC believes that the notice would compromise confidentiality measures adopted to protect the identity of the whistleblower;
- holds discussions with the whistleblower and requests additional information from the latter, if necessary;
- duly follows up on the reports received;
- carries out the necessary investigations to follow up on the report, including hearings and acquisition of documents;
- replies to the whistleblower within three months or, in the presence of justified and well-founded reasons, within six months from the date of notice of receipt of the external report or, in the absence of such notice, from the expiration date of seven days from receipt;
- informs the whistleblower of the final outcome, which may also consist in archiving of the report or its submission to the competent authorities (administrative, judicial, institutions and bodies of the European Union), or in a recommendation or administrative sanction.

6.3 Public disclosure

a) Conditions for making a public disclosure

The whistleblower may make a public disclosure (relying on the protection provided by the Whistleblowing Act) if, at the time of submission, one of the following conditions is met:

- the whistleblower has previously made an internal and external report or has directly made an external report, in the manner provided for by articles 6.1 and 6.2, and no response has been given within the terms provided therein regarding the measures envisaged or adopted to follow up on the reports;
- the whistleblower has reasonable grounds to believe that the breach may constitute an imminent or obvious danger to the public interest;
- the whistleblower has reasonable grounds to believe that the external report may involve the risk of retaliation or may not be effectively followed up due to the specific circumstances of the case, such as those in which evidence may be concealed or destroyed or in which there is a well-founded fear that the person who received the report may be in collusion with the person responsible for the violation or involved in the violation itself.

b) Channels of public disclosure

The channels for making reports are the public press or electronic means, or in any case communication methods allowing to reach a large number of people.

c) Subject of the report

Reports of breaches of European Union provisions may be the subject of public disclosure.

7. FORMS OF PROTECTION FOR THE WHISTLEBLOWER

The whistleblowing system adopted by MISSONI ensures the confidentiality and protection of personal data pertaining to the reporting party.

MISSONI also adopts all necessary measures to guarantee full protection of the whistleblower against possible retaliatory, discriminatory or otherwise unfair conduct resulting from the report.

7.1 Confidentiality of the whistleblower's identity

Access to the internal reporting channel is allowed exclusively to the Channel Manager; if the whistleblower uses his/her MISSONI email account, identified with the subject indicated in article 6.1 of this Procedure, for the purpose of sending the report, no one (including managers of the IT systems) is authorised to view it.

Violation by any person of the provisions referred to in the previous paragraph is a source of disciplinary, contractual, and, where applicable, criminal liability.

The identity of the whistleblower and any other information from which such identity may be inferred, directly or indirectly, may not be disclosed without the express consent of the same whistleblower to persons other than the Channel Manager team, which is expressly authorised to process such data pursuant to Privacy legislation.

In the case of external reporting, the confidentiality of the identity of the whistleblower is guaranteed by ANAC.

In addition, to protect the whistleblower, it should be noted that:

- in the context of criminal proceedings, the identity of the whistleblower is kept confidential in the manner and within the limits provided for by article 329 of the Code of Criminal Procedure "Obligation of secrecy";
- as part of the procedure before the Court of Auditors, the identity of the whistleblower cannot be revealed until the end of the investigation phase;
- within the framework of the disciplinary procedure, the identity of the whistleblower cannot be revealed where a dispute on the disciplinary charge is based on separate and additional findings with respect to the report, even if consequent to the same. If the dispute is based on the report, in whole or in part, and the disclosure of the identity of the whistleblower is essential for the defence of the accused party, the report may be used for the purposes of the disciplinary procedure only with the express consent of the whistleblower to disclose his/her identity.

7.2 Prohibition of "retaliation"

a) Prohibited acts of retaliation

MISSONI provides for absolute prohibition of any discriminatory measures against the whistleblower; specifically, whistleblowing **retaliation includes**:

- dismissal, suspension or other equivalent measures;
- demotion or non-promotion;
- a change of position or workplace, reduction in salary, change to working hours;
- the suspension of training activities or any restriction in access to training;
- negative assessment reports or references;
- the adoption of disciplinary measures or other sanctions, including financial penalties;
- coercion, intimidation, harassment or ostracism;
- discrimination or any unfavourable treatment;

- failure to convert a fixed-term employment contract into a permanent employment contract, where the worker had legitimate expectations of such a contractual conversion;
- the non-renewal or early termination of a fixed-term employment contract;
- damage, including to the person's reputation, in particular on social media, or economic or financial prejudice, including loss of economic opportunities and loss of income;
- placing on erroneous lists based on a formal or informal sectoral or industrial agreement, which may make it impossible for the person to find employment in the sector or industry in the future;
- the early conclusion or cancellation of the contract for the supply of goods or services;
- the revocation of a licence or permit;
- a request to complete a psychiatric or medical assessment.

Any retaliatory actions are null and void. Persons who have been dismissed due to whistleblowing (internal and/or external), public disclosure or reporting to the judicial or accounting authority, are entitled to reinstatement in the workplace.

Any retaliation suffered can be communicated to ANAC, using the tools provided on the website www.anticorruzione.it; in this case, ANAC informs the Italian National Labour Inspectorate regarding the measures within its remit.

b) Conditions for the protection of the whistleblower

The protection against acts of retaliation referred to in the previous point applies in the presence of the following conditions:

- at the time of the report (internal and/or external), of the complaint to the judicial or accounting authority or of the public disclosure, the whistleblower had reasonable grounds to believe that the information included in the whistleblowing report, publicly disclosed or reported, was true and fell within the objective scope of application of this legislation;
- the report (internal and/or external) or public disclosure was made in compliance with the steps provided for by article 6 of this Procedure.

Protection is also guaranteed in the event of reports or complaints made to the judicial or accounting authority, or anonymous public disclosure, if the whistleblower has subsequently been identified and suffered retaliation, as well as in cases of whistleblowing reports submitted to the institutions, bodies, offices and competent bodies of the European Union, in accordance with the provisions of this legislation.

Protection is not guaranteed and a disciplinary sanction is imposed on the whistleblower, when (i) the criminal liability of the whistleblower for the crimes of defamation or slander or, in any case, for the same crimes committed with the complaint to the judicial or accounting authority, or (ii) his civil liability, for the same title, in cases of wilful misconduct or gross negligence is ascertained, even with a first instance ruling.

c) Other subjects to whom the protection applies

The protection referred to in the previous letters also applies to the following subjects:

- any natural person who assists the whistleblower in the reporting process, operating within the same work context, and whose assistance must be kept confidential (the so-called "facilitators");
- persons operating in the same work context as the whistleblower, as the person who has filed a complaint with the judicial or accounting authority or as the person who has made a public disclosure, and who are linked to them by a stable emotional or kinship bond within the fourth degree;
- work colleagues of the whistleblower or of the person who has filed a complaint with the judicial or accounting authority or made a public disclosure, who are operating in the same work context and who have a current habitual relationship with said person;
- owned entities of the whistleblower, or of the person who has filed a complaint with the judicial or accounting authority, or who has made a public disclosure, or entities where said persons work, as well as entities operating in the same work context as the aforementioned persons.

8. SANCTION SYSTEM

Violation of the provisions contained in the above paragraphs may trigger the sanctioning procedure: in particular, the following are subject to sanction:

(i) a whistleblower who has made reports with intent or gross negligence or that prove to be false, unfounded, with defamatory content or in any case made for the sole purpose of damaging the Company, the reported party or other persons affected by the report;
(ii) any person who has violated the confidentiality of the whistleblower;
(iii) a person responsible for acts of retaliation;
(iv) any person who has obstructed or attempted to obstruct the report.

For the relative sanctioning treatment, please refer to the provisions in chapter 7 of Model 231.

The above behaviours can also be ascertained by ANAC, which imposes the following administrative fines:

- for the conduct referred to in point (i), fines ranging from € 500.00 to € 2,500.00, unless the reporting person has been convicted in criminal proceedings, including in the first instance, for the crimes of defamation or slander, or convicted for the same crimes through a complaint to the judicial or accounting authority;
- for the conduct referred to in points (ii), (iii), (iv), fines ranging from € 10,000.00 to € 50,000.00.

9. RECORD KEEPING

Internal reports and all related documentation are retained for the time necessary to process the report, and in any case no longer than five years from the date of communication of the final outcome of the reporting procedure, in compliance with the confidentiality obligations referred to in article 7.1 above.

For these purposes, the Channel Manager has established a computerised and paper archive, insofar as may be necessary.

The storage of external reports is the responsibility of ANAC.

Any personal data contained in the report, including those related to the identity of the whistleblower or other individuals, will be processed in compliance with the rules for protection of personal data.

10. AVAILABILITY OF THE PROCEDURE DOCUMENTATION

This policy procedure documentation, in electronic or paper format, is available in the following physical and electronic locations:

- Website at https://www.missoni.com/it/ in the Corporate section;
- Company intranet at: https://hrportal.missoni.it/;
- Company bulletin board;
- At the entrance to all sites;
- HR Office.

11. UPDATING THE PROCEDURE

This procedure has been approved by the Board of Directors and is subject to periodic updating.

INFORMATION ON THE PROCESSING OF PERSONAL DATA PURSUANT TO ARTICLES 13 AND 14 OF REGULATION (EU) 2016/679 IN RELATION TO "WHISTLEBLOWING" REPORTS

This policy information is provided by Missoni S.p.A. with respect to the processing of personal data of the interested parties (meaning the whistleblower, the reported party or other natural persons involved in the report) in the context of the management of reports made in the public interest or to protect the integrity of Missoni S.p.A. in case of alleged illegal conduct of which it has become aware due to its employment relationship with, or due to service or supply/consultancy activities carried out for the Data Controller (so-called *whistleblowing* reports, hereinafter only "**Reports**"), and received through the channels provided for by the *Whistleblowing* Procedure adopted by the Company ("**Procedure**"). If the report comes from a person that has an employment or collaboration relationship with the Company, this policy information must be understood as supplementary and not a substitute for the information provided to staff regarding management of the employment relationship.

1. Data Controller and Data Protection Officer

Missoni S.p.A., with registered office in Via Luigi Rossi 52, 21040, Sumirago (VA) (the **"Data Controller"** or the **"Company"**), which can be reached at the email address privacy@missoni.com, protects the confidentiality of your personal data and protects said data from any event that may put them at risk of violation.

The Data Controller has appointed a Data Protection Officer (hereinafter, "**DPO**"), who is at your disposal for any information on matters relating to the processing of your personal data and the exercise of your rights as a data subject.
The DPO can be contacted both at the physical address of the Company's registered office indicated above and at the email address dpo@missoni.com.

2. Type of data processed

The personal data collected and processed by the Data Controller in the context of the reception and management of Reports received through the channels provided for by the Whistleblowing Policy adopted by the Company – including the MY Whistleblowing reporting platform - are those contained in the Report, as well as those acquired during related investigative activities, including any hearing. These data may belong to the following categories:

- general personal data (e.g. the personal details of the person making the report, with indication of his/her qualification or professional position; a clear and complete description of the facts pertaining to the report and the methods with which these became known; the date and place where the event occurred; the name and role - qualification, professional position or service in which the activity is carried out - that allow identification of the subject(s) of the report; indication of the names and roles of any other subjects who may hold information on the events mentioned in the report; information relating to any documents that may verify the reported facts; the status of your report and any other information contained in the reports or provided through the use of the messaging *tool* embedded in the Platform that may be referred to the whistleblower, the reported parties and/or any other third parties involved, according to the company policy (hereinafter, collectively, "**interested parties**").
- personal data belonging to the so-called "special" categories pursuant to article 9, paragraph 1 of the Regulation *("racial and ethnic origin, religious, philosophical or other beliefs, political opinions, membership of parties, trade unions, associations or organisations of a religious, philosophical, political or , as well as personal data which may reveal health status or sexual preferences*") that may be referred to any interested parties who may be indicated by the whistleblower;
- data relating to criminal convictions and crimes or related security measures that are contained in and/or that emerge from the report pursuant to article 10 of the Regulation;

All personal data indicated above will be hereinafter collectively defined as "personal data".
It should also be noted that, in compliance with applicable laws, the Data Controller may process personal data, including data relating to third parties, which are already available to the Data Controller.
Personal data that are manifestly not useful for the processing of a specific Report are not collected or, if accidentally collected, are promptly deleted.

3. Purpose of the processing, legal basis and provision of the data

The personal data provided to report, in the public interest or to protect the integrity of Missoni S.p.A., alleged unlawful conduct of which it has become aware due to an employment relationship with, or due to service or supply/consultancy activities carried out for the Data Controller, in accordance with the provisions of the Policy adopted by the Data Controller and to which reference is here made, will be collected and processed by the Data Controller himself to allow the Supervisory Body ("SB") of the Company to carry out its functions in accordance with the Policy and to carry out the necessary investigative and instrumental activities to substantiate the fact/event that is the subject of the Report and, where appropriate, to adopt any appropriate corrective measures and take any appropriate disciplinary and/or judicial actions against those responsible for **the unlawful conduct ("Purposes of the Whistleblowing Policy**").
The legal basis for the processing of the above data is to be identified:
- for general personal data, processing for the aforementioned purposes is legitimate as it is necessary to comply with a legal obligation to which the Data Controller is subject, pursuant to article 6, paragraph 1, letter c) of the Regulation, taking into account Legislative Decree no. 24 of 10 March 2023, containing "*Implementation of 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 Union law and containing provisions concerning the protection of persons who report violations of national regulatory provisions*;
- for personal data belonging to the so-called ""“special"" categories, this processing is legitimate pursuant to article 9, paragraph 2, letter b) of the Regulation. In any case, the whistleblower should not provide personal data belonging to the so-called "special" categories, pursuant to article 9, paragraph 1 of the Regulation, unless strictly necessary.

Any processing of personal data relating to potential crimes or convictions subject to reporting is carried out according to the provisions of article 10 of the GDPR, as authorised by specific regulations on whistleblowing, as well as for the protection or defence of rights in court [see article 2-octies, paragraph 3, letter e) of Legislative Decree no. 196/2003 – so-called "*Privacy Code*"].

The provision of personal data for the indicated purpose is optional for the whistleblower, as it is possible to make the report anonymously; in the event of failure to provide the data, it may not be possible to undertake and manage the Report according to the provisions of the Company Policy. In the event that the whistleblower still wishes to submit an anonymous report, said report will be processed and managed only if it is adequately substantiated, detailed and based on precise and concordant factual elements (without generic or confusing content), so as to allow evaluation and assessment of the case.
With regard to the whistleblower, it is in any case guaranteed that no form of retaliation or discriminatory measure, both direct and indirect, and affecting working conditions for reasons directly or indirectly related to the report will be allowed.

Once provided, your personal data may also be processed in order to:
- fulfil any obligations established by laws, regulations and European legislation, as well as by provisions issued by the courts in the performance of their functions, based on article 6, paragraph 1, letter c) of the Regulation and, with regard to personal data belonging to special categories, article 9, paragraph 2, letter g) of the Regulation ("**Compliance Purposes**");

to safeguard rights and freedoms, based on article 6, paragraph 1, letter f, and article 9, paragraph 2, letter f) of the Regulation ("**Defensive Purposes**").

4. Recipients of personal data

The personal data contained in the Reports received by the Data Controller will not be disclosed to third parties or disseminated, except within the limits of the provisions of national and European Union law and in accordance with the procedure adopted by the Data Controller; in particular, your data may be shared, in compliance with the provisions of the legislation on the processing of personal data, with the following subjects:
- specifically identified personnel, who are authorised to process personal data and duly instructed pursuant to article 29 of the Regulation and article *2-quaterdecies* of Legislative Decree 196/2003 ("**Personal Data Protection Code**”), as well as the Code and/or operating procedures making up the Organisation, Management and Control Model (specifically the Data Controller's Supervisory Body as the figure in charge of receiving and assessing reports);
- only where strictly essential for the achievement of the purposes pursued, subjects external to the company of the Data Controller and that may provide services to the SB, where appropriate, in compliance with relevant legislation pertaining to the sector and with legislation on the protection of personal data, who typically act as data processors pursuant to article 28 of the Regulation (the provider of the IT platform for the management of violations);

- for the aforementioned purposes, personal data may also be disclosed to public and/or private bodies and authorities, as autonomous owners entitled to receive them by virtue of current legislation and/or to whom it is mandatory to communicate personal data pursuant to legal provisions or orders of the authorities, in particular in order to investigate activities relating to reported facts/events on which the existence of ongoing investigations by public authorities is known.

The complete and updated list of recipients of the data may be requested from the Data Controller and/or the DPO, at the addresses indicated above.

In all cases, the utmost confidentiality of your identity will be guaranteed in accordance with company procedures. In particular, in the event of submission of the report to other structures/bodies/third parties for the performance of investigative activities, the forwarding of the content of the report alone will be preferred, excluding all references that may allow to trace, even indirectly, the identity of the whistleblower. If it is necessary to reveal the identity of the whistleblower to subjects other than the manager of the internal reporting channel, for investigative purposes, the consent of the whistleblower to the disclosure of his/her identity will be expressly requested.
In the event of disciplinary proceedings, the identity of the whistleblower will not be revealed in all cases where the dispute on the disciplinary charge is based on separate and additional findings with respect to the report, even if consequent to the same, while it may be revealed where three conditions concur, namely (a) that the dispute is based, in whole or in part, on the report, (b) that knowledge of the identity of the whistleblower is essential for the defence of the accused party and (c) that the whistleblower has expressed a specific consent to the disclosure of his/her identity.

5. Processing methods

The data will be processed with mainly computerised tools, with organisation and processing methods that are strictly related to the purposes indicated above and so as to guarantee the security, integrity and confidentiality of the data, in compliance with the organisational, physical and logical measures provided for by the provisions in force. The dedicated channels that are used to send the Reports, in accordance with the internal procedure adopted by the Data Controller, offer a high guarantee of confidentiality of the information through the use of data encryption technologies on the servers. The Data Controller implements appropriate measures to ensure that the data provided are suitably processed in accordance with the purposes for which they are managed; the Data Controller adopts appropriate security, organisational, technical and physical measures to protect the information from alteration, destruction, loss, theft or improper or illegitimate use.

6. Retention period for personal data

Personal data will be retained only for the time strictly necessary for the purposes for which they are collected, respecting the data minimisation and retention limitation principles referred to in article 5, paragraph 1, letters c) and e) of the Regulation.
Specifically, the personal data contained in the Report and any accompanying documentation are retained in a form that allows identification of the data subjects for the time necessary to process the specific Report and, in any case, no longer than five (5) years from the date of communication of the final outcome of the reporting procedure. However, the Data Controller reserves the right to retain the aforementioned personal data for as long as necessary to comply with regulatory obligations and to safeguard rights and freedoms. It is understood that in the event that a judgment is established, the terms indicated above may be extended until the conclusion of the judgment itself and the consequent limitation periods of the rights. After the times indicated above, the reports and any accompanying documentation will be deleted and/or anonymised.
More information is available from the Data Controller and the DPO at the addresses indicated above.

7. Non-EU transfer of personal data

We also inform you that your personal data will be processed by the Data Controller within the territory of the European Union. If, for technical and/or operational reasons, it is necessary to rely on subjects located outside the European Union or it is necessary to transfer some of the data collected to cloud-managed technical systems and services located outside the territory of the European Union, the processing will be regulated in accordance with the provisions of Chapter V of the Regulation and will be authorised according to specific decisions of the European Union. The Data Controller ensures that the processing of your personal data by these recipients will take place in compliance with the GDPR. In particular, data transfers

will be based on an adequacy decision of the European Commission, or on the Standard Contractual Clauses approved by the European Commission, or on another suitable legal basis, in compliance with the 01/2020 recommendations adopted on 10 November 2020 by the European Data Protection Board.
Further information can be obtained, upon request, from the Data Controller and/or the DPO at the contacts indicated above.

8. Your privacy rights

You have the right to access data concerning you at any time, pursuant to Articles 15-22 of the Regulation. In particular, you may request the rectification, cancellation, or limitation of data processing in the cases provided for by article 18 of the Regulation, the withdrawal of consent given pursuant to article 7 of the Regulation, and also to obtain data portability in the cases provided for by article 20 of the Regulation.

You can make a request to restrict processing of your data pursuant to article 21 of the Regulation, in which you give evidence of the reasons justifying the objection: the Data Controller reserves the right to assess your request, which will not be accepted in the event of the existence of compelling legitimate reasons to proceed with processing that prevail over your interests, rights and freedoms.

You also have the right to file a complaint with the competent supervisory authority pursuant to article 77 of the Regulation (Guarantor for the protection of personal data) or to refer the matter to the appropriate courts pursuant to article 79 of the Regulation.

Requests must be addressed in writing to the Data Controller or to the DPO at the addresses indicated above.

Please consider that, in order to protect the confidentiality of the identity of the reporting party, you may be precluded from exercising the rights provided for in articles 15 to 22 of the Regulation, if the exercise of these rights may result in effective and concrete prejudice to the confidentiality of the identity of the reporting party, pursuant to article 23, paragraph 1, letter i) of the Regulation and article 2-undecies, paragraph 1, letter f) of the Privacy Code.
We also inform you that you may exercise your rights under articles 15 to 22 of the Regulation through the Guarantor Authority, in the manner set out in article 160 of the Privacy Code. In this case, the Guarantor Authority will inform the interested party that it has carried out all the necessary checks or a review, and will also inform the interested party of the right to file a judicial appeal.