WHISTLEBLOWING
Reporting Policy

1. PREMISE

1.1 - Why this Policy?

Legislative Decree 10 March 2023 no. 24 implementing Directive (EU) 2019/1937 (hereinafter "**Decree**"), the texts of which are attached, concerning "the protection of persons reporting violations of Union law and containing provisions concerning the protection of persons reporting violations of national legislative provisions", introduced the new whistleblowing regulation in Italy by gathering in a single legislative text the entire regulation of reporting channels and protections recognized to whistleblowers, both in the public and private sectors.
Whistleblowing is a tool of Anglo-Saxon origin through which employees of an organization, whether public or private, report to specific individuals or bodies a possible violation, a crime, an illicit act or any irregular conduct committed by other individuals belonging to the organization.
The purpose of *whistleblowing* is to allow organizations to address the reported problem as soon as possible, making known situations of risk or damage and contributing to the prevention and fight against any illicit activities.
This procedure (hereinafter "**Policy**") is intended to protect those who report crimes or irregularities of which they have become aware for work-related reasons and to spread the culture of ethics and legality in the workplace, as well as to create a climate of transparency and a sense of participation and belonging, generated by overcoming the fear of employees of suffering retaliation by corporate bodies or colleagues, or by the risk of seeing their report go unheard.
Our Policy plays a critical role in detecting and preventing various violations, as defined below. It also enables us to take appropriate action with stakeholders and protect employees who raise good faith concerns about legal or ethical violations. It also seeks to preserve our reputation and assets.
Accordingly, this Policy has the following objectives:

- ✓ encourage employees and third parties with whom we work to report internally and as promptly as possible any violations of the law or ethics, as defined in Article 2.3, with the knowledge that their concerns or suspicions will be taken seriously and, if necessary, investigated internally;
- ✓ inform employees and other stakeholders about how to report such concerns internally and how their reporting will be handled;
- ✓ create a safe space where employees and other interested parties can report misconduct in good faith, confidentially and without fear of retribution, even if their suspicions prove unfounded.

In order to ensure the effectiveness of our Policy, we implement reporting channels, as defined below.
This Policy is not part of the employment contract of employees and we can modify it at any time, in compliance with the procedures for informing and consulting workers' representatives, where applicable.
The implementation of this Policy, where required by law, is subject to information or consultation of workers' representatives.

1.2 – Glossary

Informant	Means the person who made the report (and, where required by law, the natural persons and/or, subject to applicable local laws, legal persons, who "facilitated" such reporting pursuant to Article 5 of EU Directive 2019/1937, hereinafter "**Facilitators**") through the reporting channels in accordance with this Policy.
Other interested parties	A person who is not an employee, but who, in accordance with applicable laws, has the ability to forward, to the next level, information on violations, acquired in the course of his professional activities.
Reporting channels	The reporting tools, modified from time to time if necessary: - letter written and sent as better described in section 3.1.1; - reporting of a person subject to compliance with the requirements set out in section 3.1.2 of the Policy.
Directive	Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons reporting breaches of Union law.

Personal data	Information relating to a natural person that allows that person to be identified, directly or indirectly.
Investigation	Fact checking, research, analysis and conclusions in relation to a report.
Dielle S.p.a.	The company Dielle S.p.a. with registered office in Via Montegrappa, 142 – 31010 Moriago delle Battaglia (TV) - VAT number 00761830264 – REA number TV-120840.
Whistleblowing Manager or Manager	It means a person authorized by the Sole Administrator, trained and enabled to receive and process all or part of the reports through the reporting channels. The Manager is subject to strict confidentiality obligations and must be independent and impartial. If necessary, it uses an Inspector (internal or external) to conduct targeted investigations.
Confidential information	They include, within the scope of applicable laws, all confidential information, including all data of a private nature, which is communicated, identified or which arises from the implementation of the reporting channels, in particular information on the identity of the Whistleblower, the identity of the persons concerned by the report and all information relating to a report and disclosed or collected in the course of the investigation of that report, regardless of their format (written, oral, electronic or any other form).
Inspector	The term "**Internal Inspector**" refers to an employee of Dielle S.p.a. specifically designated, trained and authorized to conduct investigations following a report. The Inspector is subject to strict confidentiality obligations and must be independent and impartial. "**External Inspector**" means a third party specifically designated by Dielle S.p.a., trained and authorized to conduct investigations following a report. An External Inspector is subject to strict confidentiality obligations and must be independent and impartial.
GDPR	Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data.
DPIA	The Data Protection Impact Assessment (or DPIA) is a particular procedure, provided for by Article 35 and recitals 90 and 93 of the GDPR, aimed at identifying, evaluating and managing the risks associated with a specific type of processing.
Employee	A person who has an employment contract with Dielle S.p.a., even if the contract has not yet started.
Violation	It is defined in art. 2.3.
Policy	This document and the obligations and rights contained herein means
Report	Reporting violations of laws, regulations or internal policies (as defined in art. 2.3) by an employee or other interested parties of Dielle S.p.a. or, if applicable, by a third party, through the available reporting channels.
Attached	A document referred to by the Policy.

2. SCOPE OF APPLICATION OF THE POLICY

2.1 - Who does the policy apply to?

This Policy applies to Dielle S.p.a., the Administrator and the Managers of the company functions must ensure the implementation of this Policy.
All employees or other interested parties of Dielle S.p.a. undertake to comply with this Policy.
Customers are excluded from the scope of this Policy and any reports should be made directly to the relevant sales representative.

2.2 - Who can report?

Our reporting channels are available to those who have a contractual relationship with Dielle S.p.a., in particular:

- Dielle S.p.a. employees;
- Volunteers or interns (paid or unpaid);
- Members of the administrative, management and control/supervisory bodies of Dielle S.p.a.;

- Self-employed workers, collaborators, consultants, workers with collaborations organised by the client;
- Collaborative relationships pursuant to art. 409 of the Italian Code of Civil Procedure, i.e. agency relationships, commercial representation relationships and other collaborative relationships which materialize in a continuous and coordinated provision of work, predominantly personal, even if not of a subordinate nature;
- Workers or collaborators who carry out their work activities at public or private sector entities that supply goods or services or carry out works for third parties.

Furthermore, the report can be sent by:

- Subjects who are in the selection or pre-contractual phase;
- During the trial period;
- After termination of the relationship (only if the information was acquired during the relationship).

Reports must concern facts acquired in a professional context and be made in good faith. In compliance with applicable laws, reports must have been initiated without any direct financial compensation.

2.3 - What are the violations to report?

Whistleblowers may report or disclose violations or attempts to conceal violations that have occurred or are suspected to have occurred in relation to the provisions of art. 2, paragraph 1 of the Decree, and in particular to the following ("Violations"):

a. Crimes and offences relating, among others, to the following behaviours:
   - Corruption;
   - Money laundering, financial, tax and accounting crimes;
   - Conflicts of interest;
   - Privacy and data protection;
   - Anti-competitive practices;
   - Trade sanctions;
   - Safety and compliance of products and services;
   - Public health;
   - Security of networks and information systems;
   - Environmental protection;
   - Corporate tax evasion;
   - Fraud.

b. Threat or harm to the public interest;
c. Illicit conduct and relevant pursuant to Legislative Decree 231/2001
d. Violation of applicable laws regarding moral or sexual harassment, discrimination and violence in the workplace;
e. Failure to respect human rights;
f. Violation of the principle of non-retaliation.

Whistleblowers may report violations that have already occurred or when they have a reasonable suspicion that violations are highly likely to occur.
Except where provided for by applicable national legislation, the Informant must have become aware of such violations in the course of his/her professional activity and, in any case, must have had personal knowledge of them.

2.4 - What is excluded from this policy

In accordance with the Directive, the following information is completely excluded from the scope of this Policy and cannot be reported or investigated:

- Violations that do not harm the public interest;
- Any information protected by professional secrecy or medical confidentiality;
- Any information covered by the secrecy of judicial deliberations or by the secrecy of investigations and inquiries.

They are also excluded:

- reports of violations governed by the directives and regulations of the European Union and by the implementing provisions of the Italian legal system which already guarantee specific reporting procedures;
- reports of breaches relating to national security, as well as procurement relating to defence or national security aspects, unless such aspects fall within the relevant secondary legislation of the European Union.

This Policy should not be used in the event of complaints relating to your personal situation or decisions affecting you (e.g., challenging a job evaluation, individual complaint against your employer), except in cases of discrimination or harassment. It may not be used for customer complaints either.

3. REPORT A VIOLATION

3.1 - Reporting method

In many cases, simply addressing a human resources issue (for example, a personal dissatisfaction with a decision involving the Whistleblower) is outside the scope of reporting. Even if you see or suspect a violation that could be reported, we hope you can escalate it to your manager. You can discuss it in person. They will likely find a way to resolve the issue quickly and efficiently, or they may even contact another relevant department.

However, if you believe that your manager has not responded to the violation, or if you prefer not to report it to him/her for any reason, you may use the reporting channels currently available, set out below.

3.1.1 - Written report

The informant sends a written report by registered mail to Dielle S.p.a - Via Montegrappa, 142 – 31010 Moriago delle Battaglia (TV) using the methods specified below.

The letter must be prepared as follows:

Envelope 1: The following must be included inside an envelope:

- name, surname;
- telephone number – which will be used by the Manager to contact the reporter;
- email address (non-business) - which will be used by the Manager to contact the reporter;
- indication of the type of relationship you have with the company (employee, ex-employee, supplier, etc.)
- copy of identity document.

The envelope must be closed.

Envelope 2: It must contain envelope 1 and the text of the report with any other supporting documentation – the envelope must be closed;

Envelope 3: It must contain envelope 2 - it will be closed and in addition to the company address it must bear the words “Reserved for the WB Manager”.

3.1.2 - Reporting of person

The Informant can make the report in person during a video conference or a physical meeting with the Manager. The meeting can be arranged by writing an email to: gestoreWB@dielle.it

In the event of an in-person meeting, the Report, with the prior consent of the reporting party, may be documented by the Manager by recording it on a device suitable for storage and listening or by full transcription (as provided for by art. 14, 2 and 4 paragraphs of Legislative Decree 24/2023.

3.1.3 - Other means of reporting

This Policy is intended to provide an effective, reliable and trusted internal mechanism for reporting, investigating and correcting workplace misconduct. In most cases, there will be no need to inform anyone externally, as this Policy ensures that any reports will be taken seriously and appropriately addressed.

However if you are sure that:

- the report has not had any follow-up;
- or has not been taken into account within the expected period;
- or you believe you have suffered retaliation;
- or there is a reasonable ground to believe that the violation may constitute an imminent or obvious danger to the public interest, the report can be forwarded to the National Anti-Corruption Authority (ANAC) via the IT platform https://www.anticorruzione.it/-/whistleblowing following the instructions provided therein.

This platform guarantees all the rights of the Informant as specified in the following art. 4 of this Policy.

3.2 – Content of the report

Reports must describe the facts objectively, be directly linked to the scope of the Policy and be limited to the elements strictly necessary to verify the reported facts.

In particular, the report must contain at least the following elements:

- general information about the Informant, indicating the position or type of relationship with the company;
- a clear and complete description of the facts being reported;
- if known, the circumstances of time and place in which the reported facts were committed;
- the indication of any other subjects who can report on the facts which are the subject of the report;
- the indication of any documents that can confirm the validity of such facts;
- any other information that may provide useful feedback on the existence of the reported facts.

The letter may also include any supporting documents.
It is recommended to be as specific as possible to allow for better understanding and faster management of the problem by the Manager.
The reporting channels must be used in good faith.

3.3 - Receiving the report

3.3.1 - Receipt of the report by letter

The received letter is delivered to the Manager who opens a new reporting case.
The Manager must guarantee the protection of the Informant and any Facilitators as provided for in the following art. 4.

3.3.2 - Receiving the report in person

The Reporter may request to be received by the Report Manager by sending an email to: gestoreWB@dielle.it.
The Manager organizes the physical meeting no later than twenty (20) business days after the meeting request.
The Manager opens a new reporting case.
The Manager must ensure the protection of the Informant and any Facilitators as provided for in the following art. 4.

3.3.3 - Reporting Management

Within seven days from the date of the report, the Informant will receive a confirmation of receipt of the same.
Once the report is received, the Manager will proceed with the initial analysis of the same which can lead to four results:

1 **Request for further information**	If the details of the report are not sufficient to determine its admissibility (for example, facts that may be of a certain seriousness but are described inaccurately or without specific details, or whose description may suggest that the person was not directly aware of them, etc.), the Manager sends a message to the Informant who originated the report (if he or she has revealed his or her identity) and asks to be contacted again. In this message, the Manager asks the Informant to provide further information. If the Informant does not respond, the report is closed.
2 **Inadmissibility of the report**	Reports may also be deemed inadmissible under this Policy (e.g., facts that do not constitute a violation, unverifiable, vague or unfounded allegations, etc.). All reports that fall outside the scope of the Policy will be destroyed or archived in accordance with the applicable retention period.
3 **Management of the report by the Manager**	The report will be considered admissible if i) the situation described corresponds to facts and behaviors that fall within the scope of this Policy, ii) its description appears sufficiently precise, iii) from a preliminary analysis the informant appears to be in good faith. If all three of these requirements are met, the Manager will proceed with the management and, if able to do so, will provide for its resolution.
4 **Appointment of an inspector**	If the Manager is unable to resolve the situation, he may forward the case to an internal and/or external Inspector selected based on the importance of the case, the people involved in the report, the seriousness of the report, the type of report and the place where the events took place.

The decision to close the report may also be taken at one of the following stages. Regardless of the date of adoption of this decision, the Whistleblower will be informed, if he has revealed his identity, that the report has been closed and the general reasons for this decision.

3.4 - Follow up of the report

The Manager and any internal Inspector must carry out their work in a confidential and impartial manner in all phases of the investigation and in the drafting of the investigation report. They must evaluate their ability to conduct the investigation according to the principle of impartiality.
The Manager reserves the right, where it deems appropriate, to appoint an external Inspector.
The Inspector will contact the Informant and inform him of the means by which he can be contacted and of the follow-up actions envisaged.
Follow-up may include, for example:

- the initiation of an internal investigation and, if appropriate, the actions taken to resolve the issue raised;
- referral to a competent service or authority for further investigation, to the extent that such information does not prejudice the investigation or the rights of the data subject;

closure of the proceedings due to lack of sufficient evidence or for other reasons.
As part of the Manager's supervisory and planning responsibilities, the Inspector is responsible for the following actions:

- Carry out checks or investigations into reports;
- Interview people, including the Informant if necessary. At the request of the person being interviewed, the interview may be conducted in the presence of a witness;
- Collect documents and evidence, where appropriate, from individual interviewees and open source databases;
- Maintain communication with the Informant;
- Prepare an investigation report detailing the facts, checks carried out and reasons for the violation (where possible), concluding on the facts and recommending actions;
- Protect the rights of the persons affected by the report or during the investigations resulting from it;
- Establish an action plan and propose recommendations;
- Propose disciplinary sanctions where appropriate and/or legal action;
- Close unjustified cases.

In all cases, the Inspector shall take all reasonable steps to ensure that the investigation can be completed expeditiously. Without prejudice to applicable legislation, the internal and/or external Inspector shall provide feedback to the Whistleblower on the proposed action within 3 (three) months of receipt of the report, unless:

- such communication is not prohibited by applicable legislation; or
- the Informant did not wish to reveal his identity; or
- in the case of a complex investigation: the content of this feedback may be limited by the fact that further investigation is necessary, in which case the Inspector must also communicate to the Informant the expected timescales for completing the investigation.

The investigation of reports is not in any way disciplinary in nature. Unless otherwise provided by law, “interviews” or discussions with the Whistleblower, persons named in the minutes and, if applicable, witnesses are intended solely for the purpose of verifying the facts in the context of an internal investigation.

3.5 - Survey results

The Manager or Inspector, if appointed, must communicate the outcome of the report to the Informant. The Informant may request to be kept informed of the progress and outcome of the report. The Informant may provide additional information during the investigation.
The investigation concludes with a report drawn up by the Manager or the Inspector (if appointed). The investigation report is sent to the Sole Administrator and/or the competent company office to implement any recommended measures.
If the Human Resources function or the Sole Administrator decides not to follow the recommended measures, they must document in writing the reasons why they did not follow the recommendations and transmit them in writing to the Manager.

4. PROTECTION OF THE INFORMANT AND FACILITATORS

4.1 - Confidentiality of reports

The identity of the Informant and the person(s) concerned by the report and the information collected are considered confidential and will not be disclosed. This obligation of confidentiality also applies to the Informant, in order to guarantee the serenity of the investigation and the protection of the people involved (Informant, witnesses, facilitators and accused).
During the investigation, information relating to the report, including the identity of the Whistleblower, may be shared only for the purposes of enforcing this Policy and only with the following persons:

- Manager;
- Inspector.

These persons have the obligation to protect the identity of the Informant. They may not reveal to anyone the identity of the Informant or any information that could lead to the identification of the Informant. They will take all reasonable measures to reduce the risk of identification of the Informant.
In exceptional cases, and only if the Whistleblower provides written consent or if the information is to be provided to local law enforcement authorities, the Whistleblower’s identity may be shared for the sole purpose of facilitating investigations. The Whistleblower has the right to define the persons to whom his or her identity may or may not be disclosed. Even if written consent is given, Whistleblowers must use extreme caution and avoid disclosing it to the subjects of the report to avoid the risk of retaliation.

The information on the report, including the identity of the Informant, may be communicated to judicial and/or administrative authorities and to law enforcement agencies.
Non-confidential information (e.g., the reference number of the report, its status, etc.) may be communicated, for example, in the context of internal reports on the implementation and dissemination of this Policy. However, in particular in the case of reports in progress, such communication may only occur after having verified that it does not compromise the investigation.
Violations of confidentiality are subject to the application of the sanctions provided for by the employment contract (category CCNL) or by the Disciplinary System Ex Legislative Decree 231/01 and to civil or criminal sanctions, in accordance with current legislation.

4.2 - Prohibition of retaliation

In the case of a good faith Whistleblower, Dielle S.p.a. applies a strict non-retaliation policy, provided that the report falls within the scope of this Policy.
The Whistleblower will not be subject to detrimental treatment or retaliation for reporting misconduct. “Retaliatory and/or discriminatory treatment” means dismissal, unjustified disciplinary action, or any other unfavorable treatment in connection with reporting a concern (e.g., demotion, transfer, isolation, threats).
If you believe you have been subjected to such treatment, immediately inform the Manager or make a specific report.
This clause applies to the following persons:

- Informant;
- Anonymous informant subsequently identified;
- Facilitator (natural person who assists the whistleblower in the reporting process, operating within the same work context and whose assistance must be kept confidential);
- Third party related to the Informant, such as colleagues or relatives;
- Legal entity of which the Informant is the owner, for which he works or to which he is in any case connected in a work context.

4.3 - Sanctions

Employees and Other Interested Parties who engage in retaliatory and/or discriminatory treatment towards the Whistleblower and other individuals identified in section 4.2 of the Policy for reasons directly or indirectly connected to the report or to hinder or attempt to hinder the report may be subject to the disciplinary sanctions that will be contained in the Organizational Model 231 and provided for by the employment contract (CCNL of the category), or to the termination of the contractual relationship.
Furthermore, the author of the retaliation may be subject to civil or criminal sanctions, in accordance with the legislation in force.

4.4 - Anonymous report

The Informant can submit an anonymous report. However, he/she must keep in mind that:

- An anonymous report may be more easily rejected if it does not contain sufficient information to conduct a meaningful investigation;
- The anonymous report will not be able to have a feedback within 7 days for the acceptance and subsequent closure within the pre-established terms;
- Disclosure of the Whistleblower's identity will facilitate investigations and the search for further information on the report and will enable the company to protect the Whistleblower more effectively;
- Anonymous reporting may make it more difficult for the Whistleblower to obtain legal protection.

5. PERSONAL DATA PROTECTION

5.1 - Personal data that may be collected

The following personal data may be collected through the reporting channel used and during factual investigations/verifications:

- The identity, location and contact details of the Informant;
- The identity, location and contact details of the persons concerned by the report and of witnesses;
- The identity, location and contact details of persons involved in receiving or processing a report;
- The data referred to in articles 9 and 10 of the GDPR relating to the Informant and/or the persons concerned by the report and to witnesses and/or persons involved in receiving or processing a report;
- The facts reported;
- The elements collected as part of the verification of the reported facts;
- The report on the verification operations;
- Measures taken in relation to the reporting.

5.2 - Informant's Rights

In order to comply with confidentiality requirements, the information provided under this Whistleblowing Policy must be concrete and directly related to the subject of the report.
Pursuant to art. 13 of the GDPR, the Whistleblower will receive all necessary information on the processing of the personal data provided, before the reporting stage (the privacy policy and this procedure are present on the company website and are distributed to all employees with the usual company communication methods). The Whistleblower is informed of the follow-up given to the report once a decision has been made.
In any case, the Manager and the Inspector (if designated) must not reveal the identity of the Whistleblower or any information that could lead to the identification of the Whistleblower by the persons concerned by the report, except to the competent judicial authorities or unless the Whistleblower has given his consent. The right of limitation pursuant to art. 18 of the GDPR remains unaffected.

5.3 - Rights of the person subject to the report

According to art. 14 of the GDPR, following the report, the persons subject to the report (for example, witnesses, victims or alleged perpetrators of crime) must be informed within a reasonable time, however the reported person cannot exercise the rights that are due with reference to personal data (see art.2 undecies privacy code). However, according to art. 14, paragraph 5, letter b), of the GDPR, the communication of such information can be avoided if such obligation to communicate "risks making impossible or seriously impairing the achievement of the purposes of that processing". This eventuality occurs in the case in which the disclosure of the information to the data subject would seriously impede the needs of the investigation, for example when there is a risk of destruction of evidence. In these cases, the information is provided only when the risk has been eliminated. Such information must be provided in a way that ensures that it is correctly communicated to the data subjects. It must not contain any indication of the identity of the Informant or of the third parties involved.

5.4 - Data retention

The data collected through the reporting channels and the related documentation are retained for a limited period of time strictly necessary for their processing and in any case not exceeding five years from the date of communication of the final outcome of the reporting procedure, in compliance with confidentiality obligations.

5.5 - Data Security

The security of personal data transmitted and processed both in the context of reports sent by letter and in person reports is guaranteed in order to avoid any alteration, modification or unauthorized disclosure.
The security and confidentiality of personal data are guaranteed during the collection of such data, as well as during their transmission or storage, through the adoption of adequate security measures that have been the subject of DPIA.
Access to personal data is permitted only to those authorised to process it and subject to strict confidentiality obligations, based on the need to know for the purposes of the investigation.
During the period of retention of personal data, the data stored on the reporting platform will be archived and separated from the other elements of the reporting platform.

6. GOVERNANCE

6.1 - Who is responsible for this Policy?

The Manager is responsible for this Policy and for evaluating the effectiveness of the measures taken in response to reports made under this Policy. The Manager has operational responsibility for this Policy and must ensure that all managers and other employees who may be responsible for dealing with issues or investigations under this Policy receive regular and adequate training. The Manager regularly reviews this Policy from a legal and operational perspective, respecting the procedures for informing or consulting workers' representatives.
The Manager ensures that this Policy is disseminated as widely as possible and is made available to all in the "Whistleblowing" section of the websites www.dielle.it and www.diellemodus.it.

6.2 - Annual report

Every year, the Manager draws up a report on the implementation of this Policy and in particular on the key indicators (number of reports by category, number of anonymous reports, number of reports made in person, number of justified reports, possible reasons underlying the evolution of the number of cases, etc.). The report is addressed in particular to the Sole Director of Dielle S.p.a. and to the various governing bodies (for example the Board of Auditors and Supervisory Body Ex D.lgs.231/01).
The identity of the Informants and the persons to whom the reports refer must never be disclosed, but only aggregated/statistical data may be communicated.

7. MISCELLANEOUS

7.1 - Policy
This policy is effective as of **December 15, 2023**.

7.2 – Language
This Policy was originally written in Italian. Any translation of this Policy into another language is for convenience only and does not affect its interpretation in any way.
In the event of any contradiction or discrepancy with versions in other languages, the Italian version shall prevail.

7.3 - Litigation
Any controversy or dispute arising from the interpretation or application of this Policy, in relation to or connected to it, will be governed by Italian law and will be under the exclusive jurisdiction of the Court of Treviso (Italy).

7.4 - Contact
If you have any questions about this Policy, please send an email to the Manager at gestoreWB@dielle.it

DIELLE SPA