

## REPORTING PROCEDURE FOR BREACHES AND IRREGULARITIES WHISTLEBLOWING POLICY

The roles, responsibilities, legal procedures, principles to be followed and the checks to be performed for the management of the "Whistleblowing Policy" are described

<b>Drawn up by:</b>			<b>Date:</b>
<b>Verified by :</b>			<b>Date:</b>

<b>1. GLOSSARY .....</b>	<b>3</b>
<b>2. PURPOSE OF THIS DOCUMENT .....</b>	<b>3</b>
<b>3. REFERENCE REGULATIONS .....</b>	<b>3</b>
<b>4. STAKEHOLDERS AND RESPONSIBILITIES .....</b>	<b>5</b>
<b>5. OPERATING PROCEDURES .....</b>	<b>5</b>
<b>6. DISCIPLINARY SYSTEM.....</b>	<b>12</b>
<b>7. PROCEDURE UPDATE AND REVISION .....</b>	<b>14</b>
<b>8. ARCHIVING .....</b>	<b>14</b>

## 1. GLOSSARY

- **Organization:** Welt Electronic S.p.A., a company based in Italy (Florence) and focused on the sale and distribution of electronic components for the industrial and lighting markets (standard and customized), hereinafter referred to as "WELT".
- **SGS:** Struttura di Gestione delle Segnalazioni [Whistleblowing Management Structure], responsible for receiving reports of corporate breaches or irregularities within WELT.
- **HR Office:** An internal office at WELT with Human Resources management activities

## 2. PURPOSE OF THIS DOCUMENT

The purpose of this Policy is to regulate the reporting procedures for breaches or irregularities within the Company with the aim of protecting the person who submits reports and, consequently, limiting any factors that may discourage the use of whistleblowing as much as possible.

Further objectives of this "Whistleblowing" Policy can be summarised as follows:

- defining and formalizing the whistleblowing procedure by establishing the terms and responsibilities in the whistleblowing process;
- defining the rules that must be followed in order to guarantee the anonymity of the whistleblower and the confidentiality of the report;
- defining the role of the RPCT.

## 3. REFERENCE REGULATIONS

First and foremost, it is appropriate to define the reference regulations for the whistleblowing phenomenon and the regulatory framework concerning the reporting of breaches or irregularities by employees or any third parties connected to WELT who become aware thereof during the course of work and, consequently, the related legal protection that the law grants to the whistleblower.

### 3.1. European and international regulations

References at EU level can be found in the Civil Law Convention on Corruption of the Council of Europe of 4 November 1999, which establishes the need to provide appropriate "protection against any unjustified sanction for employees who have reasonable grounds to suspect corruption and who report in good faith their suspicion to responsible persons or authorities" and in the UN Convention against Corruption of 30 October 2003, which provides for the possibility of introducing adequate protective measures into the legal

system of each State for those who report to the competent authorities any events concerning the offences covered by the Convention.

With the aim of making the regulatory framework provided at EU level more homogeneous, in October 2019 a specific provision was issued, Directive 2019/1937, concerning "the protection of persons who report breaches of Union law", which strengthens and standardizes the protection measures, establishing the obligation to create internal reporting channels for private legal entities with more than 50 employees, all public sector entities (including any entities owned or controlled by such entities) or municipalities with more than 10,000 inhabitants.

### 3.2. National regulations

Whistleblowing appeared the first time in our legal system with Law 190/2012 (the so-called "Anti-Corruption" Law) which amended Legislative Decree 165/2001 by introducing Article 54 bis, entitled "Protection of public employees who report breaches".

The matter was then radically amended by Law 179/2017, "Provisions for the protection of whistleblowers who report offences or irregularities which have come to their attention in the context of a public or private employment relationship", which, on the one hand, amended Article 54 bis of the aforementioned Consolidated Law on Public Employment, fully replacing the regulatory provisions and, on the other hand, introduced the whistleblowing discipline into the private sector as well, through the integration of the measures provided for in Legislative Decree 231/2001. In particular, Article 2 of Law 179/2017 intervened in the regulation of the administrative liability of entities, adding three new paragraphs to Article 6 of Legislative Decree No. 231 of 2001, whereby the position of the anonymous whistleblower was clarified, while recognizing full protection against any retaliation or discriminatory acts "for reasons directly or indirectly related to the report".

Subsequently, after a long period of inactivity on the Whistleblowing issue, Legislative Decree No. 24 of 10 March 2023 was issued implementing EU Directive 2019/1937, on the protection of persons who report violations of EU law, which has had a significant impact on the private sector.

Until then, indeed, the only entities subject to obligations relating to the whistleblowers' reporting and protection system were entities with an Organizational Model under Legislative Decree No. 231/2001. With the adoption of the Directive, the combination of Whistleblowing and 231 Models has become outdated: indeed, all companies that during the last year have employed, on average, more than 50 workers (with fixed-term or permanent employment contracts), as well as any entities that, regardless of the number of employees, operate in particular fields (financial services, products and markets,

prevention of money laundering and terrorist financing) are required to implement an internal system for the protection of whistleblowers.

In this respect, it should be noted that Legislative Decree 24/2023 also amended Article 6 of Legislative Decree 231/01 by defining the key points of connection between the two groups of regulations.

For the purposes of drafting this document, the ANAC Guidelines – approved by resolution No. 311 of 12 July 2023 on the protection of persons reporting breaches of Union law and the protection of persons reporting breaches of national laws - procedures for the submission and handling of external reports – have also been considered.

#### **4. STAKEHOLDERS AND RESPONSIBILITIES**

The figure of the so-called Whistleblower was developed in the United States to describe an individual who reports illegal activities within the organization he/she belongs to. Some believe that a whistleblower is somewhat like a referee who whistles a "fault": an image juxtaposed with that of the employee who reports an offence.

In a broader sense, the whistleblower is a worker who, during the work activity, "discovers" or becomes aware of an offence, a possible fraud, danger or any other serious risk that may cause concrete harm to third parties (e.g. suppliers, customers) or to the company itself and decides to report it, thus exposing himself/herself to the risk of vexation, retaliation and harassment.

These reports are an effective control tool, as they guarantee an internal protection mechanism within the company. However, in order for such reports to be encouraged, the person who reports the offence needs to be "protected" from possible retaliation or harassment, starting from the climate in which he/she operates.

In accordance with the provisions of Legislative Decree 24/23, the recipients of this Policy are all those who have direct and/or indirect employment and/or professional relationships with the Organization and therefore:

- **Employees;**
- **Self-employed persons who work for private sector entities;**
- **Freelancers and consultants who work for private sector entities;**
- **Volunteers and trainees, either paid or unpaid, working for private sector entities;**
- **Members of the Executive Board;**
- **Members of the Board of Directors.**

#### **5. OPERATING PROCEDURES**

##### **5.1. Subject matter of the report**

**Any unlawful conduct or alleged unlawful conduct – that is, any conduct not in compliance with the Code of Ethics and the internal procedures of WELT – observed during and/or due to the performance of the work duties or due to the employment/collaboration relationship must be reported. Therefore, these must be facts that occur within the Organization or otherwise related thereto.**

**The reports taken into consideration are only those that concern facts observed directly by the whistleblower, rather than based on mere suspicions or current rumors, nor should they be information that is already totally in the public domain. In addition, the whistleblower should not act for purely personal purposes.**

**By way of example, the report may relate to acts or omissions, either committed or attempted, that are:**

- **criminally relevant;**
- **carried out in breach of the Code of Ethics, the internal control principles and any other internal procedures or company provisions that may be sanctioned by disciplinary means;**
- **carried out in breach of the EU regulations specified in Annex 1 to Legislative Decree No. 24/2023 and all the provisions implementing it;**
- **likely to cause reputational damage to WELT;**
- **likely to cause damage to the health or safety of employees, citizens or users, or likely to cause damage to the environment;**
- **likely to be detrimental to employees, users or any other persons who work within WELT.**

**On the other hand, what CANNOT be reported, based on Article 1, paragraph 2 of Legislative Decree No. 24/2023, is the following:**

- **any disputes, claims or requests related to a personal interest of the whistleblower or of the person who has filed a complaint with the judicial authorities that relate exclusively to their individual employment or public employment relationships, or concerning their employment or public employment relationships with the whistleblower's superiors;**
- **reports of breaches that are already regulated on a mandatory basis in European Union directives and regulations and in the implementing provisions of the Italian legal system which are already the subject of appropriate reporting procedures;**
- **reports of national security breaches, as well as tender contracts related to defence or national security aspects, unless such aspects fall under the relevant secondary legislation of the European Union.**

## **5.2. Contents of the report**

**HEADQUARTER:** Welt Electronic SpA, Via della Treccia, 33 - 50145 Firenze - Tel. +39 055 302631  
info@weltelectronic.it - weltelectronic@pec.it - gdpr@weltelectronic.it - www.weltelectronic.it

**PRODUCTION:** Via della Treccia, 8 - 50145 Firenze - Tel. +39 055 302631

**LOCAL OFFICES:** Ancona: +39 071 9256421, Bologna: +39 051 0827548, Genova - Torino: +39 011 7410099, Padova: +39 02 4585637, Roma: +39 06 41206044

**COMPANY DATA:** Trib. FI45117 - R.E.A. FI388341 - C.F. e P.I. 03714360488 - Capitale Sociale: € 2.000.000 i.v. - Registro Pile IT19040P00005244



Reports must be detailed and based on precise and consistent elements, concern facts that can be ascertained and observed directly by the whistleblower and contain all the necessary information to unequivocally identify the perpetrators of the unlawful conduct.

The whistleblower is therefore required to provide all the elements useful to ascertain the validity of the facts reported in order to allow adequate checks and investigations on the subject of the report.

In particular, the report must contain:

- a) the identity of the reporting person;
- b) a clear and complete description of the facts reported and how the reporting person became aware of them;
- c) if known, the time and place of the acts committed;
- d) if known, the personal details or any other elements allowing the identification of the individual(s) who has/have carried out the reported facts;
- e) the indication of any other subjects who may report on the facts concerned;
- f) the indication of any documents that may confirm that the report is well-founded;
- g) any other information that may provide useful feedback on the existence of the reported facts.

### 5.3 Anonymous reports

Reports from which it is not possible to infer the identity of the whistleblower are considered anonymous.

Anonymous reports are treated as ordinary reports, if they are substantiated. If the **Struttura di Gestione delle Segnalazioni [Whistleblowing Management Structure, hereinafter referred to as SGS]** receives anonymous reports through the channels provided, these will be considered as ordinary reports.

In cases of anonymous reporting, if any reporting person has subsequently been identified and has suffered retaliation, the anti-retaliation measures still apply to them.

### 5.4 Recipients and reporting methods

SGS has been identified as an external party, with tax-accounting professionalism (Dr. Luca Marini). The whistleblower, when detecting a possible conflict of interest within the Organization's structure, may choose to submit the report to the HR Office of the Organization.

In accordance with Article 4 of Legislative Decree No. 24 of 10 March 2023, WELT has established specific reporting management channels, suitable for protecting the identity of the whistleblower, which are described below.

- a) IT channel

The IT channel for the management of reports is identified by the IT Department according to a careful balance between efficiency and cost-effectiveness.

The IT channel can be reached through the links found on the Organization's website in the.

<https://areariservata.mygovernance.it/#!/WB/Welt-Electronic> section. Access to the channel is subject to the "no-logs" policy in order to prevent the identification of the whistleblower who intends to remain anonymous: this means that the company's IT systems are not able to identify the access point to the portal (IP address) even if the access is made from a computer connected to the company network. Reports forwarded via this channel are received and handled by SGS.

**b) Traditional postal service**

Reports may also be sent by means of the traditional postal service. In these cases, in order for WELT – through SGS – to ensure the correct management of the report, it is advisable for the whistleblower to use two sealed envelopes: the first with the whistleblower's identification data together with a photocopy of his/her identification document; the second with the report, in order to separate the identification data of the whistleblower from the report. Both must then be placed in a third sealed envelope which shall be addressed as follows:

**Welt Electronic S.p.A.  
Via della Treccia No. 33  
50145 Firenze (ITALY)**

The indication "WELT ELECTRONIC S.P.A. REPORT – CONFIDENTIAL" will be added."

**c) Canale orale**

In addition to the reporting channels mentioned above, the reporting person may also submit internal reports orally by requesting a direct meeting with SGS, to be arranged within a reasonable timeframe. The request for the meeting can be made through the channels provided for hereinabove under (a) and (b).

If the internal report is made orally during a meeting with SGS, it shall – with the consent of the whistleblower – be documented by SGS or by the support staff identified and instructed for this purpose, either by recording onto a storage and listening device or by means of a written document. In the case of this written document, the reporting person can verify, rectify and confirm the meeting by signing the aforesaid document.

\*\*\*

It is understood that the reporting person may also rely on the external reporting channels specified in Legislative Decree No. 24 of 10 March 2023, namely:



- **ANAC External Channel**

The whistleblower may make an external report if, upon submission, one of the following conditions is met:

- a) there is no provision for the mandatory activation of the internal reporting channel within his/her work context, or this – though mandatory – is not active or – though active – does not comply with the provisions of Article 4;
- b) (b) the whistleblower has already submitted an internal report in accordance with Article 4 and the report has not been followed up;
- c) (c) the whistleblower has reasonable grounds to believe that, if he or she were to make an internal report, the report would not be effectively followed up or that the report might give rise to the risk of retaliation;
- d) (d) the whistleblower has reasonable grounds to believe that the breach may constitute an imminent or obvious danger to the public interest.

The National Anti-Corruption Authority (ANAC) activates an external reporting channel that guarantees, also through encryption tools, the confidentiality of the identities of the whistleblower, the person involved and the person mentioned in the report, as well as the contents of the report and any related documentation. The same confidentiality is also guaranteed when the report is made through channels other than those initially indicated or is received by personnel other than those in charge of processing the reports, to whom it is in any case forwarded without delay.

External reports shall be made either in writing via the IT platform or orally through telephone lines or voice messaging systems or, at the request of the reporting person, through a face-to-face meeting to be set within a reasonable timeframe.

The external report submitted to an entity other than ANAC shall be forwarded to the latter, within seven days of its receipt, while notifying the reporting person thereof.

- **Public Disclosure**

According to the Decree, the whistleblower may make information on breaches available to the public through the press or by electronic means or otherwise through means of dissemination capable of reaching a large number of people. A whistleblower who makes a public disclosure benefits from the protection provided for by the Decree if, at the time of public disclosure, one of the following conditions is met:

- a) the whistleblower has previously submitted a report through internal corporate and external channels or has made an external report directly, under the terms and in the manner provided for in this Policy, and no response has been received;
- b) (b) the whistleblower has reasonable grounds to believe that the breach may constitute an imminent or obvious danger to the public interest;
- c) (c) the whistleblower has reasonable grounds to believe that the external report may involve a risk of retaliation or may not be effectively followed up due to the specific

circumstances of the case in point, such as where evidence may be concealed or destroyed, or where there is a well-founded fear that the recipient of the report may be colluding with or involved in the perpetrator of the violation.

\*\*\*

Whatever the internal reporting channel chosen by the reporting person, the Organization guarantees, also through encryption tools, the confidentiality of the identities of the whistleblower, the person involved and the person mentioned in the report, as well as the contents of the report and any related documentation.

WELT is committed to protecting the confidentiality of the whistleblower even when the report is made through methods other than those established in accordance with Legislative Decree 24/2023 or is received by parties other than SGS.

### 5.5 Management and verification of the validity of reports

This procedure assumes that:

- The whistleblower is acting in good faith. A whistleblower who voluntarily submits a report in bad faith may be subject to disciplinary measures (for example, conservative disciplinary measures, dismissal, termination of the contractual relationship, actions for damages, etc.);
- SGS manages the reports received from both the whistleblower and the person reported in a fair, impartial and confidential manner, involving only the Head of the investigation, as defined in this procedure.

Upon receipt of the report, SGS must provide the whistleblower with an acknowledgement of receipt about the report within 7 days of receipt of the report.

It should be noted that, in the event that the report is submitted to an entity other than the SGS identified and authorized by WELT, the report must be forwarded, within seven days of its receipt, to SGS through the channels provided for in the above paragraph, while notifying the reporting person thereof.

Once the report has been taken into account, SGS must then provide feedback to the whistleblower within 3 months. To this end, the verification of the validity of the report is entrusted to the receiving SGS of WELT, which sees to it in compliance with the principles of impartiality and confidentiality, carrying out any activity deemed appropriate, including the personal hearing of the whistleblower and any other parties who may report on the facts concerned.

SGS may also rely on the support and collaboration of corporate structures and functions whenever needed due to the nature and complexity of the checks to be performed, as well as external consultants. As a matter of priority, the internal HR Office can give adequate

support to SGS in carrying out the investigation, thanks to its knowledge of the company organization and to its specific skills.

Of course, in identifying any possible internal and/or external parties to be involved in support of its activities, SGS must make sure not to involve any individuals who may be affected by the contents of the report.

At the end of the investigation, a summary report of the investigations carried out and the evidence that emerged is drawn up and shared with the HR Office of WELT. It will be the responsibility of the latter to inform the competent corporate functions or structures of any corrective actions to be implemented to make the Organization's internal control system more efficient.

The findings of the investigation are also submitted to the Executive Board for the adoption of any sanctioning procedures.

If, at the end of the verification activity, the report is found to be well-founded, based on the nature of the violation ascertained, in addition to sharing the results with the functions, bodies and structures indicated above, a complaint may be filed with the Judicial Authority.

## **5.6 No retaliation – sanctions and liability regime**

Whistleblowing is a measure that makes it possible to strengthen the dissemination of a culture of ethics, transparency and legality within WELT. This important goal can only be achieved if the reporting party, in addition to having the tools available to make reports, can also and more importantly be sure that he/she will be protected in order not to suffer retaliation from colleagues or superiors or to risk remaining unheard.

For these reasons, Legislative Decree 24 and WELT explicitly provide for the prohibition of retaliation to protect the whistleblower and the other individuals provided for by the law, including attempted or threatened retaliation, which will or may cause unjust damage to the individual/entity, either directly or indirectly.

However, in order for retaliation to arise and, consequently, for the individual to benefit from protection, there must be a close link between the report, its disclosure and the complaint and the adverse behaviour/act/omission suffered, directly or indirectly, by the reporting person, by the complainant or by the publicly disclosing person.

On the other hand, for the purposes of protection, the personal and specific reasons that led the individual to make the report, public disclosure or complaint are irrelevant. When these general conditions are not met, protection cannot be guaranteed even to persons other than the one who reports, files the complaint or makes the public disclosure if, due to the role assumed in the reporting/complaint process and/or the particular relationship that binds them to the whistleblower or complainant, they indirectly suffer retaliation.

The Organization, in adopting this procedure, is aware of the administrative sanctions applicable by ANAC under Article 21 of Legislative Decree 24/2023.

Disciplinary measures are also applicable to the whistleblower in the event of reports found to be ungrounded, made with gross negligence or willful misconduct, or found to be manifestly opportunistic and/or carried out for the sole purpose of harming the person reported or other individuals.

Disciplinary measures will be proportionate to the extent and seriousness of the unlawful conduct ascertained and may go as far as termination of employment, in compliance with the provisions of the law and the applicable regulations of the CCNL [National Collective Bargaining Agreement].

SGS may also be subject to contractual sanctions, if there has been a deficiency in the application of the confidentiality measures or failure to assess the report.

All ascertained violations of the measures put in place to protect the whistleblower are also sanctioned in the same way.

## **5.7 Definition of the procedures for the management of Personal Data Protection**

The data controller for the personal data relating to the Whistleblowing Procedure is identified as WELT, which will process the personal data of all the persons involved in the report in compliance with the principles established by the GDPR, providing the data subjects with appropriate information pursuant to Article 13 and Article 14 of the GDPR, as well as taking appropriate measures to protect the rights and freedoms of data subjects.

The internal parties involved in the management of the investigation operate subject to specific authorization from the Data Controller and on the basis of the instructions given by the latter. The processing of personal data relating to the receipt and management of reports shall be carried out in compliance with the principles set out in Articles 5 and 25 of Regulation (EU) 2016/679, providing the reporting persons and the persons involved with appropriate information pursuant to Articles 13 and 14 of Regulation (EU) 2016/679, as well as adopting appropriate measures to protect the rights and freedoms of data subjects.

The external parties that provide services instrumental to the management of reports are described as Data Processors pursuant to Article 28 of Regulation (EU) 2016/679. These parties are required to provide guarantees regarding the adoption of adequate safety measures in accordance with Article 32 of Regulation (EU) 2016/679 as well as ensure an adequate level of compliance with the provisions in force on processing, including the application of the provisions of Legislative Decree 24/2023 on the protection of the identity of the whistleblower.

The Organization ensures that the management of reports and the related data processing for privacy purposes will therefore be carried out in compliance with the applicable law provisions, pursuant to the principles of European Regulation 2016/679 on privacy (GDPR). Specifically, WELT guarantees, throughout the procedure, that WELT:

- has shared the procedure with the Data Protection Officer in charge;
- will provide the whistleblower and any other parties involved with all the appropriate information on the processing of personal data;
- will process personal data in full compliance with the GDPR;
- will carry out a specific impact assessment (DPIA) on the data processing;
- will identify the appropriate technical and organizational measures to ensure an adequate level of security;
- will regulate the relations with the external parties involved in the processing of personal data;
- will not process and/or store personal data that is manifestly not useful for the processing of the report.

As to the management of the exercise of data subjects' rights, according to the European regulations on personal data protection, the national law may in certain specific cases limit the scope of the data controller's obligations and the rights generally granted to data subjects with regard to their personal data provided for in CHAPTER III of Regulation (EU) 2016/679 (Article 23 of Regulation (EU) 2016/679).

Pursuant to Article 13, paragraph 3 of Legislative Decree 24/2023, in the context of reports there is a limitation of the rights of data subjects pursuant to Article 2-undecies of Legislative Decree No. 196 of 30 June 2003. This limitation applies because the exercise of these rights could result in an actual and concrete prejudice to the confidentiality of the identity of the whistleblower and of the persons possibly involved/mentioned in the report. Therefore, the whistleblower may exercise the right of access to his/her data, rectification or integration, deletion and limitation of processing in the same manner as he/she made the report.

The whistleblower, pursuant to Article 77 of Regulation (EU) 2016/679, is also entitled to lodge a complaint with the Data Protection Authority, in the event that he/she believes that the processing violates the aforementioned Regulation.

The exercise of the rights referred to in CHAPTER III of Regulation (EU) 2016/679 by other data subjects, such as the person reported or any other persons involved, may be delayed, limited or excluded if such exercise may result in an actual and concrete prejudice to the confidentiality of the identity of the whistleblower as provided for in Article 2-undecies, letter f of Legislative Decree No. 196 of 30 June 2003 (implementing Article 23 of Regulation (EU) 2016/679).

In such cases, these subjects may exercise the aforementioned rights through the Data Protection Authority in the manner set out in Article 160 of Legislative Decree No. 196 of 30 June 2003.

## **6. DISCIPLINARY SYSTEM**

Whoever acts in breach of this Procedure and/or the ethical and control principles defined in the Code of Ethics adopted by the Organization and referred to herein will incur the codified disciplinary measures

## **7. PROCEDURE UPDATE AND REVISION**

Whenever there are changes to the Organization's operations in terms of the management of the reporting of breaches and irregularities – "Whistleblowing Policy" – it is appropriate to update and revise this procedure, in order to make this document compliant with the procedures applied and with the delegation of power in force

## **8. ARCHIVING**

All documentation produced as part of the activities governed by this Procedure is stored at the headquarters of SGS and the HR Office.

The documentation is stored without time limits or otherwise in compliance with Article 2220 of the Italian Civil Code for no less than 10 years.

In addition, accounting documents are stored in such a way as to ensure their integrity.