Whistleblowing procedure
(whistleblowing policy)
Approved by the board of directors on November 9, 2023

Index

1. PREMISE

1.1. On 30 March 2023, Legislative Decree no. 24 of 10 March 2023 (hereinafter also referred to as the "Decree") came into force "*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 laying down provisions concerning the protection of persons who report breaches of national* legal provisions" (published in the Official Gazette no. 63 of 15 March 2023) which updates, at national level, the regulations on "whistleblowing".

1.2. The Decree aims to strengthen the protection of the whistleblower, a natural person who reports or publicly discloses information on violations acquired in the context of his or her work context, thus encouraging the collaboration of workers to facilitate the emergence of violations, understood as behaviors, acts or omissions that harm the public interest or the integrity of the public administration or private entity, through the communication of information, including well-founded suspicions, concerning violations committed or which, on the basis of concrete elements, could be committed in the organization with which the reporting person or the person who files a complaint to the judicial or accounting authority has a legal relationship (editor' s note: *within his or her work context*), as well as elements concerning conduct aimed at concealing such violations.

1.3. In fact, the Decree regulates:

a) the subjective scope of application (art. 3), distinguishing between public and private sector entities, listing the types of whistleblowers and specifying that the work context to which the Decree refers is to be understood as extended to when the legal relationship has not yet begun (if the information on violations was acquired during the selection process or in other pre-contractual phases), during the probationary period and after the termination of the legal relationship (if the information about the violations was acquired during the course of the relationship);
b) the different reporting channels: internal (art. 4), external (art. 7) and public disclosures (art. 15), detailing the conditions for the activation of the different channels and the functioning of each;
c) the methods of processing personal data (art. 13), including in communications between the competent authorities, and the retention of documentation relating to reports (art. 14);
d) the protection measures (art. 16) to be applied whenever the reporting person has reasonable grounds to believe, at the time of the report/complaint/public disclosure, that the information on violations is true and falls within the scope of the Decree. It is also specified that the reasons that led the person to report or denounce or publicly disclose are irrelevant for the purposes of protection;
e) the prohibition of retaliation, i.e. the prohibition of any conduct, act or omission, even if only attempted or threatened, put in place by reason of the report, the complaint to the judicial or accounting authority or the public disclosure and which causes or is likely to cause to the reporting person or to the person who made the complaint or made the public disclosure, directly or indirectly, unjust damage. The prohibition is regulated in a specific article of the Decree (art. 17) which also details, by way of example and not exhaustively, some cases that constitute retaliation;
f) the establishment at the National Anti-Corruption Authority (hereinafter also referred **to as "ANAC**") of the list of Third Sector entities that provide support

measures to whistleblowers (art. 18) and the possibility of communicating to ANAC the retaliation that the whistleblower believes he or she has suffered (art. 19);

g) the introduction of sanctions (applicable by ANAC or by the entities defined in the 231 Models for smaller companies) against those who:

- retaliates, obstructs or attempts to obstruct a report or violates the duty of confidentiality;
- does not set up reporting channels, does not adopt procedures for carrying out and managing internal reports or has adopted procedures that do not comply with the provisions of the Decree or has not carried out the verification and analysis of the reports received;
- has made a report that has proved to be unfounded and with reference to which the criminal liability of the whistleblower for the crimes of defamation or slander has been ascertained, including with a first instance judgment;

h) the nullity of the retaliatory or discriminatory dismissal, as well as the change of duties pursuant to Article 2103 of the Civil Code, as well as any other retaliatory or discriminatory measure adopted against the whistleblower;

i) the burden on the employer, in the event of disputes related to the imposition of disciplinary sanctions, or to demotion, dismissal, transfer, or subjection of the whistleblower to other organisational measures having direct or indirect negative effects on working conditions, subsequent to the submission of the report, to demonstrate that such measures are based on reasons unrelated to the report itself.

1.4. Tecno SpA (hereinafter also referred to as **the "Company**"), after consulting the respective trade union representatives, has made available to whistleblowers a portal for reporting - "**Whistleblowing Portal**" or "**Portal**" - suitable for guaranteeing the confidentiality of the identity of the whistleblower, of the person involved and/or in any case mentioned in the report, as well as the content of the report and related documentation.

2. EXPIRATION

2.1. This Whistleblowing Policy (hereinafter the "**Policy**") applies to the Company as of 17 December 2023 in conjunction with the entry into force of Legislative Decree 24/2023 for the Company.

3. PURPOSE OF THE POLICY AND RECIPIENTS

3.1. The purpose of this Policy is to regulate the process of receiving, analysing and processing reports, sent or transmitted by anyone, including anonymously with reference to Tecno SpA.

3.2. The "Recipients" of this procedure are:

a) Shareholders, top management and members of the Company's corporate

bodies;
b) the Company's employees;
c) partners, customers, suppliers, consultants, collaborators, associates and, more generally, anyone who has an interest relationship with the Company (hereinafter also referred to as the "**Third Parties**"),

regardless of the moment - present, past or future - in which the work context concerned takes place.

3.3. Recipients, who are aware of facts that may be the subject of reports, are invited to report promptly in the manner described below, refraining from undertaking independent analysis and/or in-depth analysis.

4. LA SEGNALAZIONE/WHISTLEBLOWING

4.1. "*Whistleblowing*" means any report of violations of national regulatory provisions (including relevant unlawful conduct pursuant to Legislative Decree 231/2001 and violations of Model 231 adopted by the Company and, therefore, of the Code of Ethics of Tecno SpA and/or of the procedures related to them of Tecno SpA) or of the European Union, submitted to protect the public interest as well as the integrity of the Company, of which the whistleblower has become aware in the context of work.

4.2. For the Company, violations pursuant to art. 2 paragraph 1 letter a of the Decree. Specifically:

a) relevant unlawful conduct pursuant to Legislative Decree 231/2001 or violations of Model 231 (and the Code of Ethics) and/or the procedures of the internal regulatory system of Tecno SpA, which do not fall within the following points b) to e);
b) offences falling within the scope of the European Union or national acts indicated in the annex to the Decree or the national acts implementing the European Union acts indicated in the annex to Directive (EU) 2019/1937, although not indicated in the annex to the Decree, relating to the following sectors: public procurement; financial services, products and markets and the 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;
c) acts or omissions affecting the financial interests of the Union (e.g. fraud);
d) acts or omissions relating to the internal market (including: competition, state aid and tax infringements);
e) other acts or conduct which defeat the object or purpose of the provisions laid down in Union acts in the areas referred to in points (b), (c) and (d).

4.3. Reports should be made whenever there are reasonable grounds to believe that the information about the breaches is true.

4.4. In order to facilitate subsequent checks and analyses, it is useful to clearly indicate:

- a description of the fact;
- the circumstances, time and place, in which the reported violation occurred;
- personal details or other elements that make it possible to identify the person to whom the reported facts are attributed.

The whistleblower, if available, may attach documents (texts, images, audio, video, etc.) that may provide evidence of the facts being reported, as well as indicate the names of other subjects who could contribute to the investigation.

4.5. Founded reports containing information that the whistleblower knows to be false are not worthy of protection.

4.6. Reports must be made in a spirit of responsibility, be of interest to the common good and fall within the types of non-conformities for which the system has been implemented.

5. PORTALE WHISTLEBLOWING

5.1. The Tecno SpA Whistleblowing Portal, established after consultation with the respective trade union representatives, can be reached via the company's website https://tecnospa.com/ or at the following address https:// tecnospa.integrityline.com/

5.2. Access to the Portal is subject to the "no-log*″ 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.

5.3. Reports, written or vocal, transmitted through the Portal are received by the Chairman of the Company's Supervisory Body (hereinafter also referred to as the "Chairman **of the Supervisory Body**") who, within 7 days from the date of receipt of the report, shall issue the whistleblower with an acknowledgement of receipt of the report, indicating whether it is deemed to:

- not applicable to the "*whistleblowing*" system (e.g. customer complaints, reports of events that occurred in other work contexts in which the Company or its Subsidiaries do not operate...);

or

- with profiles of interest (and consequently the reporting management process is activated).

5.4. Through the Portal it is also possible to request a direct meeting with the SB, the structure responsible for the management of reports. In this case, the Company's Supervisory Body (hereinafter also referred to as the "**SB**") in providing the acknowledgement of receipt proposes at least 3 possible appointments to the whistleblower.

5.5. If there are situations of conflict of interest in the management of the report by a member of the SB (i.e. for a report involving the internal member of the SB or its Function or persons who are part of it), the SB operates only with the members who

are not interested.

6. WHISTLEBLOWING MANAGEMENT

6.1. The reports referred to in §5.3 above are therefore subject to the following investigation procedure.

The Company's Supervisory Body, as the competent structure for the management of reports:

a) issue the whistleblower with acknowledgment of receipt of the report within 7 days from the date of receipt within the terms set out in §5.3 above;
b) maintains dialogue with the whistleblower and may request additions from the latter, if necessary;
c) diligently follows up on the reports received as set out in §6.3 and §6.4 below;
d) Once the investigation has been completed, it shall provide feedback on the report within 3 months from the date of the acknowledgement of receipt or, in the absence of such notice, within 3 months from the expiry of the 7-day period from the submission of the report.

6.2. The Company makes available in a dedicated section of the website, clear information with reference to the Portal and the procedures for use, including the conditions for making internal and external reports.

6.3. The reports will be subject to a preliminary analysis carried out by the SB. Where necessary, the SB will avail itself of the support of the Company Functions or Departments for the analysis of the report, which will be appropriately anonymized, and/or external professionals, in order to verify the presence of data and information useful for assessing the validity of the report.

Through the Portal:

- the whistleblower may be asked for further information and/or documentation;
- The whistleblower can communicate updates/evolutions of the report.

6.4. SB notifies the whistleblower of the outcome of the preliminary analysis if it emerges that there are no sufficiently detailed elements or that the facts referred to are unfounded, informing them that the report will be archived with the relevant reasons. Where, as a result of the preliminary analyses, useful and sufficient elements emerge or can be deduced to assess the report as well-founded, the SB initiates the next phase of specific investigations. In particular, it provides:

a) initiate specific analyses using, if deemed appropriate, the Company's Functions or Management;
b) agree with the *management* in charge of the Function involved in the report, any "*action plan*" necessary for the removal of the control weaknesses detected;
c) agree with the Management (and/or with other Departments and Functions concerned) on any initiatives to be taken to protect the Company's interests (e.g. legal actions, suspension/cancellation of suppliers from the Supplier Register);

d) in the case of reports in relation to which the bad faith of the whistleblower and/or the merely defamatory intent are ascertained (possibly also confirmed by the groundlessness of the report itself), report the incident to assess the initiation of disciplinary proceedings against the whistleblower;
e) at the end of the in-depth analysis carried out, submit the results to the competent structure for evaluation so that the most appropriate measures are taken, where necessary involving the Board of Statutory Auditors on the issues within its competence;
f) terminate the investigation at any time if, in the course of the investigation, it is ascertained that the report is unfounded.

6.5. The activities described above are not necessarily carried out in a sequential manner.
6.6. The SB, as the Competent Structure for the management of reports, after consulting the Board of Statutory Auditors of the Company, provides the final feedback to the whistleblower upon completion of the checks/in-depth analysis and in any case no later than 3 months from receipt of the report.

7. PROTECTION AND RESPONSIBILITY OF THE WHISTLEBLOWER

7.1. The whistleblower is granted the following protection:

a) the confidentiality of one's identity, referring not only to the name, but also to all the elements of the report (including the voice of the whistleblower himself, in the case of oral reports made through the portal) as well as the documentation attached to it, to the extent that their disclosure, even indirectly, may allow the identification of the whistleblower. The processing of these elements must therefore be based on the utmost caution, starting with the obscuring of the data if for investigative reasons other subjects must be made aware of them;
b) retaliatory or discriminatory measures, direct or indirect, adopted following the report made in good faith, such as, but not limited to, disciplinary sanctions, demotion, dismissal, transfer, worsening of working conditions. The retaliatory intent exists whenever it can be said that the reason that led to the adoption of the measure against the whistleblower is the desire to "punish" him for having reported. In such cases, it is the responsibility of the Company or its Subsidiaries to prove that such measures are unrelated to the report.

7.2. Sanctions are provided for those who violate the whistleblower's protection measures (see also § 1.3 letter g) of the Policy and art. 21 of the Decree.
7.3. Sanctions are also provided for against the whistleblower, which may also be imposed by ANAC, in compliance with the conditions set out in the Decree, in the case of reports made 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 or other subjects affected by the report.

8. PROTECTION OF THE REPORTED

8.1. The reported person is recognized as having the protection of the confidentiality of

his/her identity, in order to avoid prejudicial consequences, even if only of a reputational nature, within the work context in which the reported person is inserted.

8.2. The identity of the reporting person and any other information from which this identity can be deduced, directly or indirectly, may not be revealed, without the express consent of the reporting person himself, to persons other than those competent to receive or follow up on the reports, expressly authorized to process such data in accordance with *privacy legislation*.

The report is not sufficient to initiate any disciplinary proceedings against the reported person. In the context of disciplinary proceedings, the identity of the reporting person cannot be revealed, if the objection to the disciplinary charge is based on separate and additional investigations with respect to the report, even if they are consequent to the same. If the complaint is based, in whole or in part, on the report and knowledge of the identity of the reporting person is indispensable for the defence of the accused, the report will be used for the purposes of disciplinary proceedings only in the presence of the express consent of the reporting person to the disclosure of his or her identity.

The whistleblower shall be notified in writing, through the Portal, of the reasons for the disclosure of confidential data in the context of disciplinary proceedings against the whistleblower and, when the disclosure of the identity of the whistleblower and the information referred to in §8.2 are indispensable for the purposes of defending the person involved, in the process of managing the report referred to in §6.

8.3. The protection of the reported person applies without prejudice to the provisions of the law that impose the obligation to communicate the name of the reported person suspected of being responsible for the violation (e.g. requests from the Judicial Authority).

8.4. Reports may not be used beyond what is necessary to adequately follow them up.

9. HOW TO TRANSMIT THE REPORT

9.1. After accessing the Portal, the whistleblower will be guided in filling out a questionnaire consisting of open and/or closed questions that will allow him/her to provide the elements characterizing the report (facts, temporal context, economic dimensions, etc.).

9.2. At the end of the questionnaire, the Portal will ask the whistleblower whether or not he/she intends to provide his/her identity, without prejudice to the protection of the confidentiality of his/her identity. In any case, the whistleblower may provide his/her personal details at a later date, always through the Portal.

9.3. When the report is sent, the Portal will issue the whistleblower with a unique identification code (*ticket*). This number, known only to the whistleblower, cannot be recovered in any way in case of loss. The *ticket* will be used by the whistleblower to access, again through the Portal, their report in order to: monitor its progress; insert additional elements to substantiate the report; provide their personal details; answer any in-depth questions. In fact, the Portal makes it possible to establish a virtual conversation (*chat*) between the whistleblower and the recipient, ensuring, at the will of the whistleblower, anonymity.

9.4. Reports received from subjects and/or through channels other than those governed

by this Policy must be forwarded by the recipient to the SB within 3 working days. The SB must register the report in the Portal by reporting the facts described to it by the recipient/whistleblower and attaching any documents (e-mails, images, etc.) provided by them; the SB communicates to the whistleblower, as far as possible, *the* ticket of the report and the temporary password. With these credentials, the whistleblower can access the Portal to integrate, if desired, his/her personal data and be updated with reference to the report. The first time you log in, the portal asks you to enter a permanent password.

9.5. The recipient who forwards a report to the SB is considered a facilitator for the purposes of this procedure and, as such, bound to the confidentiality of the identity of the whistleblower and the information as well as subject to the envisaged safeguards and responsibilities.

10. PERIODIC CARRYOVER

10.1. At least every six months, the Supervisory Body provides a summary report of the reports received by the Board of Directors and the Board of Statutory Auditors.

10.2. This *report* contains a summary of the progress of the analyses, including the results of the completed checks and the possible adoption (or not) of disciplinary measures.

11. PRIVACY POLICY

11.1. The questionnaire on the Portal is structured to ask only for the personal data strictly necessary for the report; it is the whistleblower's right, after having read the *privacy policy*:

- provide data relating to your identity;
- enter the personal data that you deem useful for the purpose of managing your report.

11.2. Any personal and sensitive data contained in the report, including those relating to the identity of the whistleblower or other individuals, will be processed in compliance with the rules for the protection of personal data and the "GDPR Policy" adopted by the Company.

11.3. The competent structure (as defined in §5.3) is the only one entitled to identify any personal data that is not useful for the processing of the report and, consequently, it is up to you to delete the same from the Portal without recalling it (e.g. indicating "remove reference to address of residence and/or educational qualification" without indicating the details). The SB must:

- file in the Portal the reasoned indication for cancellation;
- arrange for the deletion without delay;
- inform the whistleblower of the information deleted because it is considered

personal data not useful for the processing of the report.

12. RECORD-KEEPING

12.1. In order to ensure the management and traceability of reports and related activities, the Supervisory Body, as the competent structure for the management of reports, takes care of the archiving of all supporting documentation of the report for the time necessary to process the report and in any case for a period of a maximum of 5 years from the communication of the final outcome of the reporting procedure.

12.2. When the report is made in oral form through audio recording, it is documented in the portal, with the consent of the whistleblower, by the staff in charge by recording on a device suitable for storage and listening or by full transcription. In the case of a transcript, the whistleblower may verify, rectify or confirm the content of the transcript by means of his/her signature.

12.3. If, if requested by the whistleblower on the Portal, the report is made during a meeting with the staff in charge, the documentation can be made, subject to the whistleblower's authorization, by recording or by means of a report. In the latter case, the whistleblower can verify and, where necessary, rectify the content and finally confirm the report by signing the document or message on the Portal.

12.4. When the report, and any in-depth analysis relating to it, is made orally through forms that do not allow the registration of the whistleblower, for technical reasons or for lack of consent, the exchange of information is documented through a detailed report prepared by the staff in charge and made available to the whistleblower through the Portal. The whistleblower can verify and, where necessary, rectify the content and finally confirm the transcription by signing the document or message on the Portal.

13. EXTERNAL REPORTING

13.1. The whistleblower may make an external report if:

a) the internal reporting channel described above is not active or, even if active, does not comply with the provisions of the Decree;
b) the whistleblower has already made an internal report and it has not been followed up;
c) the whistleblower has reasonable grounds to believe that, if he or she were to make an internal report, it would not be followed up or that it could lead to the risk of retaliation;
d) The whistleblower has reasonable grounds to believe that the breach may constitute an imminent or obvious danger to the public interest.

13.2. External reports can be made in written form through the IT platform or orally through the telephone lines/voice messaging systems set up by ANAC or, at the request of the whistleblower, by direct meeting set within a reasonable time. In this regard, please refer to the specific section of the ANAC website (https://www.anticorruzione.it/).

14. PUBLIC DISCLOSURES

14.1. The whistleblower may resort to public disclosure, through the press or electronic means or in any case through means of dissemination capable of reaching a large number of people, if:

a) the whistleblower has already made an internal and external report or has directly made an external report and has not received feedback on the measures taken to follow up on the report;
b) the whistleblower has reasonable grounds to believe that the breach may constitute an imminent or obvious danger to the public interest;
c) The whistleblower has reasonable grounds to believe that the external report may entail the risk of retaliation or may not be effectively followed up due to the specific circumstances of the specific case, such as those in which evidence may be concealed or destroyed or where there is a well-founded fear that the person receiving the report may be colluding with the infringer or involved in the breach itself.

15. POLICY UPDATE

15.1. The Policy and the Portal are available in a dedicated section of the Company's website.

15.2. The Policy is subject to periodic verification to ensure its constant alignment with the relevant legislation as well as according to the operations and experience gained.