# WHISTLEBLOWING PERSONAL DATA PROTECTION POLICY

**Policy pursuant to articles 13 and 14 of the Regulation (EU) 2016/679 and the current Italian legislation in relation to personal data protection – reporting of infringements to Italian and European standards (so-called whistleblowing)**

**Data controller:** Tinvention S.r.l.
The data controller shall process personal data of data subjects within the established channels in accordance with the applicable regulation, in order to consent to report infringements to Italian and European standards, which may affect the public interest or the integrity of Tinvention (so-called whistleblowing). The data controller also shall manage such reports.
This policy shall be read together with the "Procedure for managing whistleblowing" on the internal channel at https://tinvention.wbisweb.it which contains information about infringements with different levels of detail. These infringements shall be reported on the assumptions and the modalities for making a report and on the protections contained in the applicable regulation and addressed to the subjects of the report.

**Subjects of the report:** the policy shall apply to the subjects who report the above-mentioned infringements, to the reported subjects who are indicated as allegedly responsible, to the subjects involved in the infringements, to the subjects who are aware of the facts or are mentioned in the report and to facilitators.

**Purposes and modalities of the data processing:** the data controller shall process personal data for receiving and managing reports, including investigation stage, application of corrective measures, monitoring data application and informing the whistleblower on the results of the procedure, defending the data controller in court and/or defending the whistleblower.
Data process shall take place using manual, computing and telematic tools, which are strictly correlated to the specified purposes and it shall guarantee security and confidentiality of data, in accordance with the current regulation and by applying the provided technical and organizational measures.

**Legal basis:** the data processing is carried out according to a legal obbligation to which the data controller is subject (article 6, paragraph 1, point (c) GDPR), pursuant to the applicable regulation in the field of whistleblowing Legislative decree 24/2023.
Whenever particular categories of data are provided during a reporting procedure, the data controller shall process them by virtue of the following derogations provided in the article 9 GDPR, which consist of:

- the necessity for the purposes of carrying out the obbligations and exercising specific rights of the data controller or of the data subject in the field of employment and social security and social protection law (article 9, paragraph 2, point (b) GDPR);
- the necessity for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity (article 9, paragraph 2, point (f) GDPR). Personal data processing is necessary in case of litigation or pre-litigation in order to assert or defend a legal, administrative, in arbitration or conciliation claim of the data controller or of a third party;
- legit interest of the data controller in order to comply with what has been required by clients and/or potential clients to take part in contract notices;
- Furthermore, in terms of disclosure of the whistleblower's identity to other subjects, different from those responsible to receive the report and to use the report when the whistleblower's identity is necessary to defend the person who was reported, in compliance with what is provided in article 12 paragraphs 2 and 5 of the legislative decree 24/2023, legal basis is denoted by consent.

The whistleblower's consent is necessary also for storing recordings and/or transcriptions of phone calls, text messages, conversations (article 14 paragraphs 2 and 4 of legislative decree 24/2023).

**Categories of personal data and sources of data origin:**
According to the data controller's experience, the following personal data of data subjects shall be processed:

- identification data;
- contact details;
- data concerning alleged reported conducts, attributed to the reported person, in which the subject may be involved or may be aware of;
- pictures and other documentation attached to the report;
- particular categories of personal data which are possibly contained in the report;
- legal data;
- content of communications exchanged between the whistleblower and the subjects who manage the report.
- possible particular data subject of the report

The personal data of the subjects different from the whistleblower are generally provided by the whistleblower through the report or by other subjects (when those are heard during the investigation).

**Communication of data:** only the subjects specifically authorized by the data controller in the role of members of the managing body of the reporting channel and possibly those involved in the analysis and in the investigation shall be aware of such data. In any case, the whistleblower's identity, and any other deducible information, shall be disclosed to subjects different from subjects authorized/designated to manage the report or the investigation on behalf of the data controller, only with the authorization of the whistleblower or whenever is mandatory or legitimate pursuant to the applicable regulation. In exceptional cases, when the disclosure of the identity is essential to defend the reported person (in the field of disciplinary proceedings) or the involved person (in the field of internal procedures), the whistleblower shall be informed, always through the platform, about the reasons of such communication which shall take place only prior consent, like indicated in the paragraph related to legal basis. The protection of confidentiality is guaranteed also to other subjects, until the conclusion of the procedure which has started because of the report and in accordance with the safeguards provided in favor of the whistleblower. Nevertheless, in case the report is subject of complaint to competent authorities, the obbligation of confidentiality of the identity of the involved or mentioned persons shall fail in the ways and under the conditions provided by the applicable regulation.
Moreover, data or part of the data shall be shared with the following external subjects, as appropriate, acting as autonomous data controller or data processor:

- lawyers and consultants, who provide consulting or investigation services;
- legal, supervisory or police bodies, in the cases provided by law;

Data shall be processed to the extent of strictly essential and in the face of dedicated safeguards, companies which provide to the data controller the platform for the report, informative systems and/or companies which are involved in their maintenance and security.
Personal data shall not be diffuse; they are not transferred outside the EEA or - in case they are - the transfer is assisted by the safeguards in the Chapter V of R. EU 2016/679, moreover, data shall not be subject to entirely automated decisional processes.

**Time of storage:** in accordance with principles of proportionality and necessity, personal data shall be stored in a way that consents the identification of the subjects for the necessary time to process the report and no longer than five years after the date of the communication to the whistleblower about the final result of the procedure of report. Exceptions are: possible specific legislative obligations or the occurred necessity of the data controller to act or defend itself in court, which make necessary to process and to store data for longer time.

**Obligation of providing data:** it is possible to make a report anonymously or not, like indicated in the "Procedure for managing whistleblowing". In case of anonimous report, the data controller may not be able to investigate the report effectively. Therefore, where applicable, the whistleblower is encouraged to report every infringement providing all the required information, so to consent to the data controller to require

further information. In any case, the data controller ensures that all the personal data processed in the field of the report remain strictly confidential.

**Rights of the data subject:** the data subject shall exercise the right at any time to obtain the confirmation as to whether the existence of their data and to know their content and their origin, to verify their accuracy or require the integration or the update, or the rectification (articles 15 and 16 of GDPR). Moreover, he or she has the right to require the erasure, the limitation to the process, the withdrawal of consent, the data portability.

The rights in the articles 15-22 of the R: EU 2016/679 shall be exercised through claim procedure to the personal data protection supervisor https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/4535524

However, the data controller shall highlight that the exercise of the rights of data subjects shall be limited or excluded, pursuant to what has been provided by the Privacy policy, in case an effective and concrete prejudice to the confidentiality of the whistleblower's identity may result from the exercise of such rights.

The data controller has designated a personal data protection processor which shall be contacted at: privacy@tinvention.net

The data controller is entitled to make to this policy all the modifications considered useful, also in relation to the evolution of the current regulation, giving it the greatest visibility to data subjects.

Released on 01/02/2024