



IPC

BY TENNANT COMPANY

Whistleblowing Policy
IP Cleaning S.r.l. and IPC Tools S.p.A.

Summary

Introduction	3
1. Definitions	3
2. Purpose and scope	4
2.1. Exclusions from the scope of application	5
3. Protection system	6
3.1. Protected persons	6
3.2. Protection and support measures	6
3.3. Protection of the reported person	8
4. Management of internal reports	8
4.1. Internal channel: Ethics Point	8
4.2. Ethics Committee	9
4.3. Internal Reporting Management Process	10
4.3.1. Receipt of the Report	10
4.3.2. Preliminary Review	10
4.3.3. Preliminary investigation	10
4.3.4. Feedback to the Whistleblower	11
4.3.5. Documentation retention	11
4.4. Conflict of interest	11
4.5. Whistleblower liability	12
5. External reporting - ANAC	12
6. Public disclosure	13
7. Disciplinary system	13
8. Training and information	14
Attachment: PRIVACY POLICY	15

Introduction

With European Directive 2019/1937, the European Union has renewed the legislation concerning the protection of persons who report breaches of Union law, in order to create a minimum standard for the protection of their rights in all member states.

In implementation of the Directive, Italy adopted Legislative Decree No. 24 of March 10, 2023, defining guarantees for the protection of whistleblowers and all persons involved in reporting, ensuring that they are protected with regard to the confidentiality of their identity.

By adopting this Policy, the Italian companies IP Cleaning S.r.l. and IPC Tools S.p.A. of the Tennant Group, with the aim of ensuring a safe and fair environment and establishing a culture based on fairness, legality, and transparency, intend to comply with the above regulatory requirements, as well as the guidelines provided by ANAC.

This Policy therefore aims to remove factors that may discourage or hinder recourse to the institution, such as doubts and uncertainties about the procedures to follow and fears of retaliation or discrimination, protecting anyone who intends to report potential unlawful conduct that violates the principles expressed in the Code of Conduct and in compliance with the Organization, Management, and Control Model pursuant to Legislative Decree 231/1001. Management and Control pursuant to Legislative Decree 231/1001.

The objective is to provide clear operational guidelines on the subject matter, content, recipients, and methods of transmission of reports.

The report management procedure guarantees the confidentiality of the identity of the reporter and of all persons involved from the moment the report is received and in all subsequent contacts.

1. Definitions

ANAC: National Anti-Corruption Authority

Public disclosure: means the act of making information about violations public through the press or electronic media or by any means of global dissemination capable of reaching a large number of people.

IPC: refers to the companies IP Cleaning S.r.l. and IPC Tools S.p.A belonging to the Tennant Group.

Retaliation: refers to unjustified disciplinary actions, or any behavior, act, or omission, even if only attempted or threatened, that causes or may cause unjust harm to protected persons (e.g., dismissal, demotion, harassment).

O.d.V.: refers to the Supervisory Body of each Company.

Reported: means the person to whom the violation reported is attributed.

Report: means the communication of unlawful conduct in violation of the Code of Conduct, the Organization, Management, and Control Model pursuant to Legislative Decree 231/2001,

and IPC's internal procedures, policies, and regulations, as well as applicable laws and regulations.

External Report: means a report made to ANAC through the channel set up by the Authority.

Internal reporting: written or oral reporting made through the channels set up by IPC.

Reporting due to gross negligence: this refers to reporting carried out with negligence, imprudence, or incompetence and in the absence of truthfulness or sufficient factual elements to reasonably believe that the reported conduct actually occurred.

Reporting in bad faith: this refers to reporting made in the knowledge that the conduct did not occur, with the aim of causing unjust damage to the reported party.

Whistleblower: means the person who makes a Report through the channels provided.

2. Purpose and scope

IPC, part of the Tennant Group, is committed to maintaining the highest standards of conduct, integrity, and ethical behavior, as summarized in its Code of Conduct and other Tennant Group policies.

This Reporting Policy aims to promote and reinforce these standards and, more generally, the values of the Tennant Group, by establishing the rules to be applied in the event of a Report, in order to combat all forms of illegal or unethical conduct.

The Whistleblower may be:

- Employees, including part-time and temporary employees, during their probationary period
- Temporary agency workers
- People whose employment relationship has ended at the time of the Report, if the information reported was obtained during the employment relationship
- Job applicants, if the information was obtained during the selection process
- Self-employed workers
- Freelancers and consultants
- Volunteers and interns
- Shareholders
- Persons with administrative, management, control, supervisory, or representative functions

Reports may concern conduct, acts, or omissions that may violate the public interest or the integrity of IPC and constitute:

- Administrative, accounting, civil, or criminal offenses
- Offenses falling within the scope of European Union or national legislation
- Acts or omissions that harm the financial interests of the European Union
- Acts or omissions concerning the European internal market

- Potential misconduct or alleged violation of the principles and values of the Code of Conduct, the Organization, Management, and Control Model pursuant to Legislative Decree 231/2001, or the Group's internal policies, regulations, and procedures

With reference to the concept of "unlawful conduct," it should be noted that, in the opinion of ANAC, the legislation is aimed at preventing or combating various phenomena that may constitute criminal, civil, or administrative offenses, as well as irregularities in the management or organization of an entity's activities to the extent that they constitute a symptomatic indication of irregularities due to the improper exercise of the public functions assigned to it.

Illegal activities that have not yet been carried out but which the whistleblower reasonably believes may occur in the presence of specific and consistent elements may also be reported. The content of the reported fact must present elements from which it can be clearly inferred that there is damage, prejudice, an obstacle, or an alteration to the correct and impartial performance of an activity, including in terms of credibility and corporate image.

Furthermore, the Report must be made "**in good faith**" and in the public interest or in the interests of IPC's integrity: the system is, in fact, intended to promote ethical and honest behavior by entities and must not, therefore, be used for individual needs or purposes. Any additional reasons, including personal ones, that lead the Whistleblower to make the Report are to be considered irrelevant for the purposes of recognizing the protections provided for by the regulation in question.

2.1. Exclusion from the scope of application

The following cannot be the subject of a Report:

1. disputes, claims, or requests related to the personal interests of the whistleblower or the person who filed a complaint with the judicial authorities that relate exclusively to their individual employment or public service relationships, or that relate to their employment or public service relationships with their superiors;
2. reports of violations already covered by mandatory European Union or national legislation indicated in Part II of the Annex to the Decree or by national legislation implementing the European Union acts indicated in Part II of the Annex to Directive (EU) 2019/1937, even if not indicated in Part II of the Annex to the Decree;
3. reports of breaches of national security, as well as procurement related to defense or national security, unless such aspects are covered by relevant secondary EU law.

The following are not covered by the scope:

- information that is manifestly unfounded,
- information that is already in the public domain,

- or information obtained solely on the basis of unreliable rumors or hearsay (so-called "gossip").

It is not permissible to repeat reports with the same content whose outcome has already been communicated to the whistleblower.

3. Protection system

3.1. Protected persons

The protection provided by this Policy applies only to Reports concerning facts or information that the Whistleblower has become aware of directly. The Whistleblower shall be entitled to the protection provided if, at the time of the Report, they had reasonable grounds to believe that the information reported was true and fell within the scope of the Policy and applicable law.

Protection also applies to the following persons:

- a) Facilitator: a natural person who assists the Whistleblower in the Reporting process, operating within the same working environment and whose assistance must be kept confidential;
- b) Persons in the same working environment as the Whistleblower, complainant or person making a public disclosure who are related to them by a stable emotional bond or family relationship up to the fourth degree;
- c) Work colleagues of the Whistleblower, complainant or person making a public disclosure, who work in the same working environment as the Whistleblower and who have a regular and ongoing relationship with that person;
- d) Entities owned exclusively or in majority by third parties by the whistleblower, complainant, or person making a public disclosure;
- e) Entities where the whistleblower, complainant or person making a public disclosure work.

3.2. Protections and support measures

IPC guarantees the following protections:

a. Confidentiality

IPC ensures confidentiality regarding the identity of the Whistleblower, the facilitator, and the persons mentioned in the Report, as well as any other information contained in the Report throughout the entire reporting process. Therefore, all persons involved in the handling of the Report are obliged not to disclose any information from which the identity of the Whistleblower could be directly or indirectly inferred from the time the Report is received until it is closed, even if the Report is found to be incorrect.

This protection of confidentiality implies a prohibition from disclosing the identity of the Whistleblower without their express consent to persons other than those responsible for managing the Report.

In order to reveal the identity of the Whistleblower, in addition to consent, written notification of the reasons for such disclosure is required in the following cases:

- disciplinary proceedings: where disclosure of the Whistleblower's identity is essential for the defense of the person against whom the disciplinary charge is brought
- proceedings initiated following internal or external reports where such disclosure is also essential for the defense of the reported person.

Therefore, any disclosure without the Whistleblower's consent is considered legitimate only if it fulfills a legal obligation or is requested by the judicial authorities in the manner and within the limits provided for by the Code of Criminal Procedure.

b. Protection against retaliation

Whistleblowers are protected by a total ban on any retaliation that may be adopted, threatened, or attempted as a result of the report made. The same protection also applies to facilitators, people in the same work environment, coworkers who have a regular and ongoing relationship with the whistleblower, and even legal entities in cases where they are entities owned by the whistleblower, complainant, public discloser, or entities where they work or entities operating in the same work environment.

IPC undertakes to ensure that the Whistleblower cannot be sanctioned, demoted, dismissed, transferred, or subjected to any other organizational measure having direct or indirect negative effects on their working conditions for reasons directly or indirectly related to the Report. According to ANAC, this also includes conduct or omissions by the Company towards the Whistleblower aimed at limiting and/or restricting the exercise of the worker's duties in such a way as to reveal a vexatious intent or otherwise worsen the working situation.

In the context of judicial or administrative proceedings or, in any case, out-of-court disputes concerning the ascertainment of conduct, acts, or omissions prohibited under this article against the persons referred to in point 3, it is presumed that such conduct, acts, or omissions were carried out because of the Report, public disclosure, or reporting to the judicial or accounting authorities.

The burden of proving that such conduct or acts are motivated by reasons unrelated to the Report, public disclosure, or complaint lies with the person who carried them out.

Alleged retaliation must be reported exclusively to ANAC, which will carry out the appropriate investigations.

If the Ethics Committee of the Company receives notification of retaliatory measures, it shall offer the necessary support to the whistleblower, indicating that the notification must be forwarded to ANAC in order to obtain the protections provided for.

Protection in the event of retaliation is **not guaranteed** when the whistleblower's criminal liability for defamation or slander, or for the same offenses committed in reporting to the judicial or accounting authorities, or their civil liability for the same reasons in cases of reports made in bad faith or with gross negligence, has been established, even by a first instance judgment. If the whistleblower is found liable, they will also be subject to disciplinary action.

c. Limitation of liability

The protection provides for the exclusion of liability in the event that the whistleblower discloses, for just cause, information covered by official, corporate, professional, scientific, or

industrial secrecy (Articles 326, 622, and 623 of the Italian Criminal Code) or violates the obligation of loyalty (Article 2105 of the Italian Civil Code).

In the latter case, the Whistleblower must act to protect "the interest in the integrity of public and private administrations, as well as the prevention and repression of malfeasance" and must not have learned the information "by virtue of a professional consulting or assistance relationship with the entity, the company or the natural person concerned" and must not disclose information and documents that are subject to business, professional or official secrecy "in a manner that exceeds the purposes of eliminating the unlawful act."

In particular, disclosure must not take place outside the communication channel specifically set up for Reports, which are to be understood as referring to the persons designated by law as recipients of the report/complaint (Ethics Committee, ANAC, judicial authorities).

3.3. Protection of the reported person

IPC guarantees the reported person the right to be informed (within a reasonable period of time) of the allegations and any disciplinary measures taken against them, as well as the right to defend themselves. In addition, the reported person may be heard at their request, including through a written procedure involving the collection of written comments and documents.

As soon as objective elements emerge suggesting that the Report is unfounded and has been submitted in bad faith or with gross negligence, the Ethics Committee shall assess the adoption of measures in this regard and, if a criminal offense has been reported, report it to the competent authorities.

IPC hopes that staff at all levels will cooperate in maintaining a climate of mutual respect for the dignity, honor, and reputation of each individual within the company and is committed to discouraging and preventing abusive, discriminatory, or defamatory behavior among colleagues.

Therefore, IPC guarantees adequate protection for the Reported Party in the event of Reports made in bad faith, censuring the above conduct and providing adequate information in cases where such bad faith is established. In this regard, the disciplinary system adopted by the Company expressly provides for sanctions against those who make reports in bad faith and with gross negligence that prove to be unfounded.

4. Management of Internal Reports

4.1. Internal Channel: Ethics Point

IPC encourages Whistleblowers to submit reports in good faith based on facts of which they become aware, in order to maintain the highest standards of conduct, integrity, and ethical behavior globally, as summarized in its Code of Conduct and other Tennant Group policies.

IPC has established an Internal Reporting Channel that guarantees the confidentiality of the identity of the Whistleblower, the Reported Person, and any other person mentioned in the Report, as well as the content of the Report and related documentation.

To support investigations and facilitate an appropriate response, Reports should include:

1. a clear and complete description of the facts reported;
2. the circumstances of time and place in which the facts were committed;
3. the personal details or other information that allow the identification of the person(s) who committed the reported acts;
4. the indication of any other persons who may report on the facts reported;
5. indication of any documents that may confirm the validity of these facts;
6. any other information that may provide useful feedback on the existence of the reported facts.

The channel identified for making Reports also allows *Whistleblowers* to indicate their identity or remain anonymous.

The EthicsPoint platform allows for timely case management and subsequent communication with whistleblowers and guarantees their complete anonymity and confidentiality.

Tennant EthicsPoint is a comprehensive and confidential reporting tool that allows you to make reports:

1. Written: by accessing the web portal from a desktop or mobile device at tennant.ethicspoint.com;
2. Oral: via the dedicated telephone number available 24 hours a day, 7 days a week, on 800 172 444.

The platform guarantees the highest standards of security and data protection and is therefore considered the **preferred channel** for making Reports. It should also be noted that this is considered the only channel for reporting possible violations of IPC's Organization, Management, and Control Models and Legislative Decree 231/01.

If the Report is received through channels other than the two mentioned above, it must be forwarded to the Ethics Committee within seven days of receipt, with the Whistleblower being notified of the forwarding at the same time.

4.2. Ethics Committee

IPC has set up an Ethics Committee for the management of Reports, composed of members with adequate legal, ethical, and integrity expertise, as well as adequate knowledge of the organization and functioning of IPC, such as:

1. HR Manager Italy;
2. Members of the Supervisory Body pursuant to Legislative Decree 231/01;
3. Global Compliance Counsel;
4. Senior VP, General Counsel & Corporate Secretary – Tennant Company.

The Ethics Committee thus composed meets the requirements of impartiality and independence required by law, being able to freely carry out, with operational and evaluative autonomy, all activities necessary for the management of Reports.

4.3. Internal Reporting Management Process

4.3.1. Receipt of the Report

Members of the Ethics Committee will simultaneously receive Reports submitted via the EthicsPoint platform. Upon receipt of a Report, the Ethics Committee will meet to formally open the case.

Through the EthicsPoint portal, the Whistleblower will receive a response from the Committee within seven days of the date of receipt of the report, informing him/her that the Report has been received and examined and that the Whistleblower may be contacted later for further information and to provide feedback on the outcome of the Report management procedure.

As part of the management of the Internal Reporting channel, the Ethics Committee:

- a. shall notify the Whistleblower of receipt of the report within seven days of receipt;
- b. maintains communication with the Whistleblower and may request further information from the latter, if necessary;
- c. follows up diligently on the reports received;
- d. provides feedback on the Report within three months of the date of acknowledgment of receipt or, in the absence of such acknowledgment, within three months of the expiry of the seven-day period from the submission of the report.

4.3.2. Preliminary verification

The Ethics Committee shall carry out a preliminary verification to determine the admissibility of the Reports received.

In particular, the Ethics Committee shall assess whether the Report:

- a. is submitted by legitimate parties and that the subject matter falls within the scope of application;
- b. is based on facts that are sufficiently precise and detailed in terms of time and place;
- c. contains personal details or other information that allows the person to whom the unlawful conduct is attributed to be identified.

The Ethics Committee may communicate with the Whistleblower via the platform and request further information to support the Report.

After this initial verification, the Ethics Committee may decide:

1. to close cases that are insufficiently detailed, manifestly unfounded, or relate to conduct or facts that are not relevant to this Policy, providing appropriate information to the Whistleblower; or
2. open the preliminary investigation referred to in the following point.

4.3.3. Preliminary investigation

The purpose of this phase is to carry out the necessary activities to determine the relevant facts of the Reports that, after the preliminary phase, have been considered sufficiently detailed to proceed with the investigation and verify the validity of the facts described.

Any investigations are carried out by the Ethics Committee and will be conducted in accordance with the following principles:

- a) investigations may reveal information or evidence of unlawful conduct. The Ethics Committee is responsible for verifying the legal aspects, providing general legal and compliance advice on relevant issues and indicating whether there is an obligation to inform the local authorities;
- b) any person involved in the investigation will be required to respect the obligation of confidentiality regarding the identity of the Whistleblower and any other persons mentioned in the Report and must be given prior and necessary authorization to process personal data;
- c) investigations must be conducted ensuring that appropriate measures are taken for the collection, use, disclosure, and storage of personal information and ensuring that the needs of the investigation are balanced with the need to protect confidentiality;
- d) other functions, employees, external consultants, and anyone else necessary for the performance of the above activities may be involved in the investigations, provided that they have the necessary technical expertise and meet the requirements of independence and impartiality.

At the end of the investigation, the Ethics Committee may:

- Close the report if it considers it unfounded, giving reasons for its decision;
- Ascertain the validity of the report and inform the Board of Directors of the findings of the investigation, including the results of the investigation and the proposed action plan with the corrective measures deemed necessary to resolve any critical issues identified.

4.3.4. Feedback to the Whistleblower

At the end of the preliminary investigation, the Ethics Committee will inform the Whistleblower of the outcome of the Report.

The Whistleblower will in any case receive feedback within three months of the date of confirmation of receipt by the Ethics Committee regarding the management of the Report.

4.3.5. Data Retention.

All personal data will be processed in accordance with Regulation (EU) 2016/679 and Legislative Decree No. 196 of June 30, 2003.

Therefore, Reports and related documentation shall be retained for the time necessary to process the Report and in any case for no longer than 5 years from the date of notification of the final outcome of the Reporting procedure, in compliance with the confidentiality obligations set forth in European and national legislation on the protection of personal data.

4.4. Conflict of interest

The Policy ensures that the management of Reports is entrusted exclusively to persons who are not in a conflict of interest.

All conflicts of interest must be disclosed without hesitation and recorded in the case file. Therefore, if the Report refers to conduct by one or more members of the Ethics Committee, or to areas falling within their responsibility, or to shortcomings in control/supervision obligations:

- members in conflict situations shall not take part in the management of the case;
- the Company's Board of Directors must be notified so that the integrity, impartiality, and independence of the Ethics Committee can be restored.

In such cases, it is still possible to resort to the entities indicated by law (e.g., ANAC).

The above points shall also apply in the event of a conflict of interest arising at a later stage, with the replacement of the persons involved in their respective roles.

4.5. Responsibility of the Whistleblower

This procedure does not affect the criminal and disciplinary liability of *the Whistleblower* in the event of slanderous or defamatory reports pursuant to the Criminal Code and Article 2043 of the Civil Code.

Any abuse of this procedure, such as reports that are manifestly unfounded and/or made for the sole purpose of damaging the reported person or other parties, and any other case of improper use or intentional exploitation of the institution covered by this procedure, shall also be grounds for disciplinary action and other appropriate measures.

5. External Reporting - ANAC

Pursuant to Article 7 of Legislative Decree No. 24 of March 10, 2023, ANAC has set up an External Reporting channel that guarantees, including through the use of encryption tools, the confidentiality of the identity of the Whistleblower, the Reported Person, and the person mentioned in the report, as well as the content of the report and related documentation.

External Reports are therefore those that the interested party can submit directly to ANAC. In particular, reports may be submitted in writing using the dedicated IT platform available on the Authority's institutional website.

At the date of this procedure, the platform is accessible at the following link:

link: <https://whistleblowing.anticorruzione.it/#/>

Alternatively, the interested party may also make an External Report orally:

- using the dedicated telephone lines;
- using the specially designed voice messaging systems;
- by requesting a direct meeting with ANAC officials.

5.1. Conditions for making an external report to ANAC

The above External Reporting channels may only be used if one or more of the following conditions are met:

- the Internal Reporting channel set up by IPC is not active or, even if active, does not comply with the provisions of Article 4 of Legislative Decree 24/2023;
- the Whistleblower has already made an Internal Report in accordance with this procedure, but no action has been taken (for example, no response has been received within the time limits set out in this Policy);
- the Whistleblower has reasonable grounds to believe that, if they decide to make an Internal Report, it will not be followed up effectively;
- the Whistleblower has reasonable grounds to believe that, if they decide to make an Internal Report, this would result in a risk of retaliation against them;
- the Whistleblower has reasonable grounds to believe that the violation may constitute an imminent or obvious danger to the public interest.

6. Public disclosure

Pursuant to Article 15 of Legislative Decree 24/2023, whistleblowers who make a public disclosure may avail themselves of all the protection measures commonly provided for those who use an internal or external reporting channel.

However, in order for such protection to be extended, the public disclosure must take place under the following conditions:

- The whistleblower has previously made an internal and external report or has made an external report directly under the conditions and in the manner provided for in the previous paragraph, without, however, receiving a response from the relevant offices within the deadline set for the transmission of the report;
- The whistleblower has reasonable grounds to believe that the violation may constitute an imminent or obvious danger to the public interest;
- 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 case.

The possibility of resorting to public disclosure, availing oneself of the safeguards and protective measures provided for, is permitted exclusively with reference to the disclosure of information relating to:

- illegal acts falling within the scope of the European Union or national acts indicated in the annex to Legislative Decree No. 24 of March 10, 2023, or national acts implementing the European Union acts indicated in the annex to Directive (EU) 2019/1937;
- acts or omissions affecting the financial interests of the Union referred to in Article 325 of the Treaty on the Functioning of the European Union;
- acts or omissions relating to the internal market, as referred to in Article 26(2) of the Treaty on the Functioning of the European Union;
- acts or conduct that undermine the purpose or objective of the provisions of Union acts in the areas referred to above.

7. Disciplinary system

Certain conduct in violation of this policy may be considered grounds for disciplinary liability, which may therefore result in disciplinary sanctions being imposed on those who:

- a. have retaliated, obstructed or attempted to obstruct reporting or violated the obligation of confidentiality;
- b. have not established or adopted procedures for reporting or managing reports, or such procedures do not comply with regulatory requirements;
- c. have not carried out verification and analysis of the reports received;
- d. have made a report and have been found civilly liable for the same offense, in cases of intent or gross negligence, unless the reporting person has also been convicted in the first instance for defamation or slander or for the same offenses committed in the report to the judicial or accounting authority.

The principles of proportionality and graduality will be respected in the application of the sanction.

8. Training and information

Pursuant to Article 5, paragraph 1, letter e) of Legislative Decree 24/2023, this Policy provides information on the channel, procedures, and requirements for making Internal and External Reports.

The HR department undertakes to keep this Policy up to date.

This Policy has been prepared by the HR Department and approved by the Board of Directors of IP Cleaning S.r.l. and IPC Tools.

The Policy is made available to recipients by publication on the company website.

Attachment: PRIVACY POLICY

Pursuant to Article 13 of Regulation (EU) No. 2016/679 (hereinafter "GDPR") IP Cleaning S.r.l. and IPC Tools S.p.A. (hereinafter "IPC" and "Data Controller") hereby provide information on the processing of personal data carried out in relation to the management system for reports of potential misconduct or suspected illegal acts received by IPC.

Data Controller

The Data Controllers are:

- IP Cleaning S.r.l., st. Treviso 63, Portogruaro (VE), 30026 (Summaga) Italy, VAT number 01205180191
- IPC Tools, st. dell'Artigianato II, 1, Villa del Conte (PD), 35010, Italy, VAT number 00930840285

Data controller and recipients of reports

IPC, as part of the Tennant Group, manages reports through the internal EthicsPoint channel provided by NAVEX. Pursuant to Article 28 of the GDPR, Tennant has appointed NAVEX as Data Processor (for more information on how NAVEX handles your personal data, please visit: <https://www.navex.uscom/en-/privacy-statement/>).

The digital platform is provided for the management of reports. IPC has also appointed an Ethics Committee, which is responsible for managing the reporting process. The members of the Ethics Committee have been appointed as persons authorized to process personal data.

Categories of personal data

The Data Controller may need to process the following personal data after receiving a report:

a. common personal data pursuant to Article 4, point 1 of the GDPR. 4, point 1 of the GDPR of the whistleblower (if the report is not anonymous), of the reported person and of any other persons involved and/or mentioned in the report, such as:

- personal details (e.g., first name, last name, date and place of birth),
- contact details (e.g., landline and/or mobile phone numbers, postal/email addresses),
- organizational data (e.g., job title, position),
- photographs, videos, or audio/video contributions;

b. Special categories of personal data pursuant to Article 9 of the GDPR, if included in the report;

c. personal data relating to criminal convictions and offenses pursuant to Article 10 of the GDPR, if included in the report. 10 of the GDPR, if included in the report.

Through the digital platform, the whistleblower can make the report anonymously, without being identified. Therefore, personal data is only processed if the whistleblower makes a non-anonymous report, or if someone is mentioned in the report.

Purpose and legal basis of the processing

The processing of personal data is carried out in accordance with Legislative Decree 24/2023, which provides for the implementation of internal reporting systems through which whistleblowers can report potential misconduct of which they have become aware in the workplace. Therefore, pursuant to Article 6(1)(c) of the GDPR, the legal basis for the processing derives from the fulfillment of a legal obligation to which the Data Controller is subject. For these purposes, the processing will therefore cover all operations necessary for:

- a. the execution of the activities of receiving, analyzing, verifying, and archiving the report;
- b. the introduction of any disciplinary measures or the adoption of other measures, to be assessed on a case-by-case basis;
- c. internal risk control requirements.

Furthermore, personal data may be processed by the Data Controller for the defense or assertion of its rights in civil, administrative, or criminal proceedings, and therefore, pursuant to Article 6, paragraph 6, letter f) of the GDPR, the legal basis for such processing is the pursuit of the legitimate interest of the Data Controller.

Retention period for personal data

The Data Controller shall retain personal data only for the period necessary to manage the report received and in any case for a period not exceeding 5 years from the date of communication of the final outcome of the whistleblower management process. After this period, the data will be deleted. In accordance with the principles of necessity and proportionality, personal data that is clearly not useful for the management of a specific report will not be collected or, if accidentally collected, will be deleted without delay.

How we process your data

Personal data necessary and instrumental for the proper management of the relationship are stored in written form, or in the form of voice recordings, through automated and computerized systems, and only if necessary on paper, according to logic strictly related to the purposes indicated above. In any case, processing is carried out in such a way as to guarantee the security and confidentiality of the data, with particular reference to the identity of the whistleblower, the reported person, and all persons involved and/or mentioned in the report.

Sharing of data with third parties and dissemination

For the purposes described above, the Data Controller may disclose personal data to third parties belonging to the following categories:

- a. judicial authorities and police forces and/or other public administrations, within the limits and for the fulfillment of obligations provided for by law, by a regulation or by EU legislation, which will process them as independent Data Controllers;
- b. consultants who will be duly appointed as Data Processors.

NAVEX is based in the United States. NAVEX complies with the EU-US privacy framework ("EU-U.S. Data Privacy Framework"). NAVEX Global, Inc. is certified by the US Department

of Commerce as adhering to the Data Privacy Framework Principles with respect to the processing of personal data received from the European Union.

Rights of the data subject

In relation to the processing of personal data, each data subject may exercise the following rights provided for in Articles 15 to 22 of the GDPR:

- a. right of access
- b. right to rectification
- c. right to erasure
- d. right to restriction of processing
- e. right to data portability
- f. right to object to processing
- g. right to withdraw consent
- h. right not to be subject to a decision based solely on automated processing.

Furthermore, every data subject has the right to lodge a complaint with the "Personal Data Protection Authority." Pursuant to Art. 2-undecies of Legislative Decree no. 196/2003, the exercise of the rights provided for in Articles 15 and 22 of the GDPR may be limited if the exercise of such rights could result in actual and concrete harm to the confidentiality of the identity of the whistleblower who reports violations of which he or she has become aware by virtue of his or her employment relationship or duties. Therefore, in the event of specific restrictions, the rights in question may be exercised through the "Data Protection Authority" in the manner set out in Article 160 of the same Decree. You may exercise these rights by contacting the Data Controller at the following email address: ipcprivacy@tenantco.com.