Whistleblowing Policy

This policy applies to all Companies belonging to FAAC Technologies Group, including HQ FAAC SpA Unipersonale (Headquarter of the Group) and ALL Subsidiaries worldwide.

FAAC SpA is pleased to announce that FAAC Technologies Group, as part of its commitment to transparency and integrity, has introduced a procedural, web-based digital reporting system with the objective of preventing and intercepting behavioral and compliance irregularities internal to the organization and remedy them whenever possible.

Summary

Section 1: Milestones of this policy 1

1.1. What is whistleblowing 1

1.2. Scope of application 1

1.3. Creation of dedicated reporting system 2

1.4. Protection of whistleblower 2

1.5. Management of whistleblowing reports 2

1.6. Authorized persons to access the FAAC whistleblowing platform 3

1.7. Reportable events 3

1.8. Employee training and awareness 4

1.9. Monitoring and continuous improvement 4

Section 2: Procedure for submitting a report 5

2.1. Internal Reporting Office 5

2.2. Reports via the Smart Integrity Platform 6

2.3. Anonymous reports 7

2.4. Confidential reports 8

2.5. Arrange a meeting 9

2.6. Voice Reports 10

2.7. External Reports 10

Section 3: Procedure for processing a report 11

3.1. Confidentiality 11

3.2. Protection of the whistleblower 11

3.3. Protection of the persons involved 12

3.4. Process handling 12

3.5. Reporting a conflict 12

3.6. Escalation levels 13

3.7. External support 13

3.8. Release of information 13

3.9. Deletion of reports 14

Section 4: Prohibition of retaliation 14

4.1. What is Retaliation 14

4.2. Reporting retaliation 15

Section 5: Policies and applicable laws 15

Section 1: Milestones of this policy

1.1. What is whistleblowing

Whistleblowing is a key mechanism in the protection of ethics and legality within organizations.

As clearly delineated in the European Directive 2019/1937 (EU Directive implemented in Italy by Italian Legislative Decree 24/2023), whistleblowing represents a crucial channel for reporting illicit behaviors – such as corruption or violations of regulations as indicated by Italian Legislative Decree 231/2001 – as well as abuse or violence in the workplace – as indicated by Gender Equality standards (UNI/PdR 125).

FAAC Technologies Group (hereinafter referred to as "Company") provides a dedicated online web platform and establishes precise guidelines for the management of reports. This platform has been designed to ensure that every voice is heard, that every report is treated with the utmost gravity, and that maximum protection and confidentiality for the reporter and all others involved in the report is enforced.

1.2. Scope of application

The aim of the Company is to ensure compliance with Company policies and promote an ethical corporate culture by upholding the highest standards of fair dealing, honesty, and integrity in our business activities.

To achieve this vision, it is critical that employees and partners understand, follow, and adhere to the Company corporate vision and values. We have established these policies and guidelines to encourage our employees to speak up when they see activities or behaviors that they deem unethical, thus making it possible for us to cohere to our corporate values in our daily work.

The objective of this policy is to provide clear guidance on the handling of internal and external reports of violations and misconduct (also referred to as "reports" or "notices" for short).

FAAC Technologies Group "Whistleblowing Policy" is designed to:

- Invite and encourage every employee to speak up anonymously or confidentially if they feel we are not adhering to our company values. The Company has dedicated a place for employees to report misconduct. Each report will be listened to and responded to, and the findings will be used to improve workplace culture and the work experience going forward.
- Allow everyone to make reports anonymously. We are committed to protecting the identity of whistleblowers. They need not reveal themselves unless they wish to do so.
- Investigate every report of misconduct. At the end of the investigation, we will document the incidents and resolutions, as well as provide guidance on follow-up action within the legal deadlines.

This policy stands for all employees and officers of the FAAC Technologies Group Companies at the commencement of their employment or, for existing employees, at the time the Company implements this policy.

The Company reserves the right to amend this policy at any time.

1.3. Creation of dedicated reporting system

The legislation requires the establishment of a dedicated and protected channel for Whistleblowing reporting that:

- allows employees to communicate anonymously or confidentially, to guarantee that reports can be made without fear of repercussions;
- is easily accessible to all employees, regardless of their position within the company.

FAAC Technologies Group has identified, purchased, and parameterized a specific platform by an external international supplier, DISS-CO, which will operate on a global level and be rendered accessible to all our employees around the world (see below in Section 2.2 "Reports via the Smart Integrity Platform").

1.4. Protection of whistleblower

One of the key aspects of the legislation is the protection of the whistleblower.

This means that anyone who decides to make a report is protected against any form of discrimination, retaliation, or penalty. Confidentiality of the whistleblower's identity is a top priority, and the legislation includes strict measures to prevent any form of retaliation.

The platform reporting protocol adopted by FAAC Technologies Group guarantees the confidentiality and safety of those who decide to report any incidents of abuse or harassment.

1.5. Management of whistleblowing reports

The Whistleblower EU Legislation establishes clear and transparent procedures for the management of whistleblowing reports.

This includes preliminary analysis of the report, in-depth investigation, and possible corrective measures.

All reports must be handled promptly, with careful documentation of every step of the process, to ensure transparency and accountability.

In compliance with the above-mentioned legislation, FAAC Technologies Group will guarantee a response time within 7 days. Within this response time, the Company will inform the whistleblower of the reception of the whistleblowing report and begin the verification process of its content.

Finally, FAAC Technologies Group also aims to close the investigation and assessment, and to communicate the outcome of the verification to the reporter, within 3 months, so long as there are no obstacles in the case creating a course of delay.

1.6. Authorized persons to access the FAAC whistleblowing platform

Any person who is or has been engaged in any of the following activities in relation to the Company shall be deemed an "Authorized Person" covered by the Company's Whistleblowing Policy:

- **Employee**: persons who, for a specified period of time, perform services for which they receive remuneration, for and under the direction of another person;
- Workers in specific employment relationships, including part-time and fixed-term employees, and persons who have concluded an employment contract or employment relationship with a temporary employment agency;
- Freelancers and self-employed persons who have a contractual relationship with the company
- Contractors, including subcontractors and suppliers;
- Persons working under the supervision and management of contractors, subcontractors and suppliers;
- Interns, working students, and job applicants;
- Customers, agents and distributors;
- Consultants, service providers, suppliers, other business partners, auditors;
- Relatives, dependents, spouses or dependents of a spouse of any of the above persons;
- Supervisory bodies, managing directors, advisory board members, board members;
- Other stakeholders not above-mentioned.

This policy is intended to apply to the above-mentioned persons in all countries in which the company conducts business.

If local laws, rules or regulations provide a higher level of protection than what is contained in this policy, local legislation shall prevail.

1.7. Reportable events

Eligible persons may file a report of a violation that could constitute the following:

- Fraud, embezzlement, breach of trust;
- Corruption (active and passive bribery);
- Theft;
- Consumption or trafficking of drugs;
- Violence or threat of violence (physical, verbal, and/or digital);
- Damage to property;
- Unethical behavior;
- Price fixing;
- Harassment, discrimination (gender, racial, age and/or religious etc.), victimization, bullying, mobbing;

- Violation of company policies and/or Code of Ethic.

This list is not exhaustive.

Events of any kind that constitute a breach of national, EU, or international laws should be reported. Reasonable suspicion is enough to prompt a report.

The term "violation" is intended as abusive practices as defined by the case law of the Court of Justice, i.e. acts or omissions which do not appear to be illegal in formal terms, but which are incompatible with the object or purpose of the relevant legislation.

Once the report has been sent and verified, the authorized person becomes a "whistleblower" for the purposes of this policy.

Whistleblowers can also report the following:

- Information necessary to detect breaches that have already occurred;
- Violations that have not yet occurred but are reasonably likely to occur;
- Acts or omissions that the whistleblower has reasonable grounds to believe to be violations;
- Attempts to conceal violations.

Reporting false information in bad faith or knowingly is not permitted and will result in sanctions against the whistleblower.

1.8. Employee training and awareness

To ensure that all employees are aware of their rights and of report protocol, FAAC Technologies Group will perform training and awareness programs.

These programs are essential to create a corporate culture based on ethics and transparency, encouraging employees to speak openly about any concerns.

As already done in the past, when introducing the Group Code of Ethics, FAAC Technologies Group plans to implement specific training initiatives for all company levels, particularly emphasizing that any form of violence and/or sexual harassment is completely unacceptable and ensuring that everyone understands the Company's condemnation of this behavior and its pledge to hold individuals accountable for such behavior.

1.9. Monitoring and continuous improvement

The standard requires that the reporting management system is subject to continuous monitoring and periodic reviews: this allows all employees to identify any areas for improvement and make sure that the system remains effective and updated with best practices and regulatory changes.

It is no coincidence that the application of the Italian Legislative Decree 24/2023 requires thinking in terms of Identification of Risk (in the logic of Health and Safety in Workplace regulations), Risk Assessment and Events, Prevention Plan, and Evaluation of Working Environments with specific reference to harassment-related risks.

This allows FAAC Technologies Group to identify and address potential risks effectively and proactively.

FAAC Technologies Group will also plan regular surveys with employees to monitor the occurrence of harassing or sexist attitudes. These surveys help to better understand the workplace climate and to intervene where necessary.

Section 2: Procedure for submitting a report

2.1. Internal Reporting Office

Reports can be sent to the Internal Reporting Office via the DISS-CO "Smart Integrity Platform" accessible from the following link:

https://customer-portal.smartintegrityplatform.com/IT/faacgroup-237/third-party/home

This link is also published on all FAAC Technologies Group subsidiary websites and accessible to "Authorized Persons" (as described above in Section 1.6).

If you as a Whistleblower provide an email address in the platform, you will receive all communications and notifications from the following e-mail address: notification@diss-co.tech.

Please check your spam folder if you have not received any email reply.

Administrators of the Internal Reporting Office and the processing of reports are:

NAME: Andrea Lanzoni
FUNCTION: FAAC Technologies Group Internal Auditing Director & Group DPO
ADDRESS: FAAC SpA, Via Calari 10, 40069 Zola Predosa (Bologna) ITALY
E-MAIL: odv231@faactechnologies.com

NAME: Anna Tassinari *(backup)*
FUNCTION: FAAC Technologies Group Internal Auditor
ADDRESS: FAAC SpA, Via Calari 10, 40069 Zola Predosa (Bologna) ITALY
E-MAIL: odv231@faactechnologies.com

If you have any questions about the Privacy Policy, please contact:

NAME: Andrea Lanzoni
FUNCTION: FAAC Group DPO (Data Protection Officer)
ADDRESS: FAAC SpA, Via Calari 10, 40069 Zola Predosa (Bologna) ITALY
E-MAIL: dpo@faactechnologies.com

The provider of the Smart Integrity Platform is DISS-CO, a legal tech company based in the EU. Technical support can be reached at support@diss-co.tech during normal business hours (excluding weekends and public holidays).

2.2. Reports via the Smart Integrity Platform

Employees – as well as all Authorized persons – can send reports to the Internal Reporting Office conveniently and securely via our web-based Smart Integrity platform.

You have the option to report confidentially or anonymously. In both cases, your identity as a whistleblower is protected.

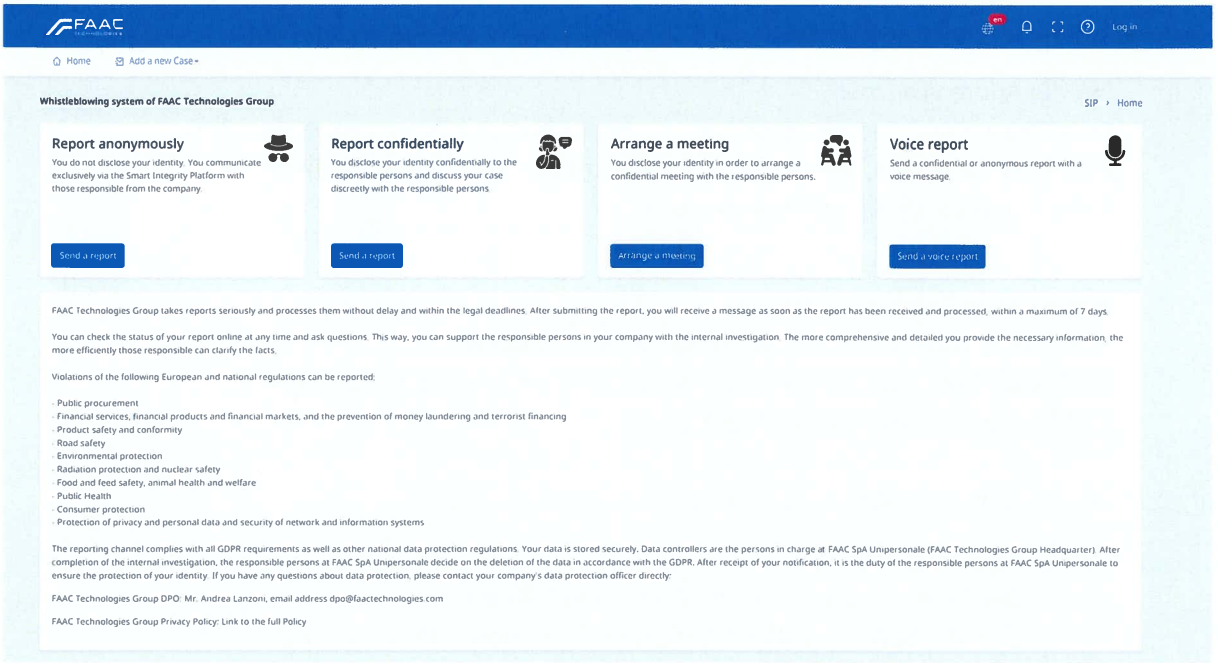
ATTN: Since including your own email is optional, be sure to take note of the Username and Password chosen. You will have to use these credentials to enter in the report again to see the follow up.

Additionally, if you did not indicate any email address, you will NOT receive any communications or notifications by email.

In any case, your email will not be visible to the administrators of the Company if you choose to report anonymously. It will only be used by the system to notify you.

All communications and notifications sent by the Smart Integrity Platform will be sent from the email address notification@diss-co.tech and will be received on the email address provided by the user at the initial login on the platform.

Whistleblowing web platform "landing page":



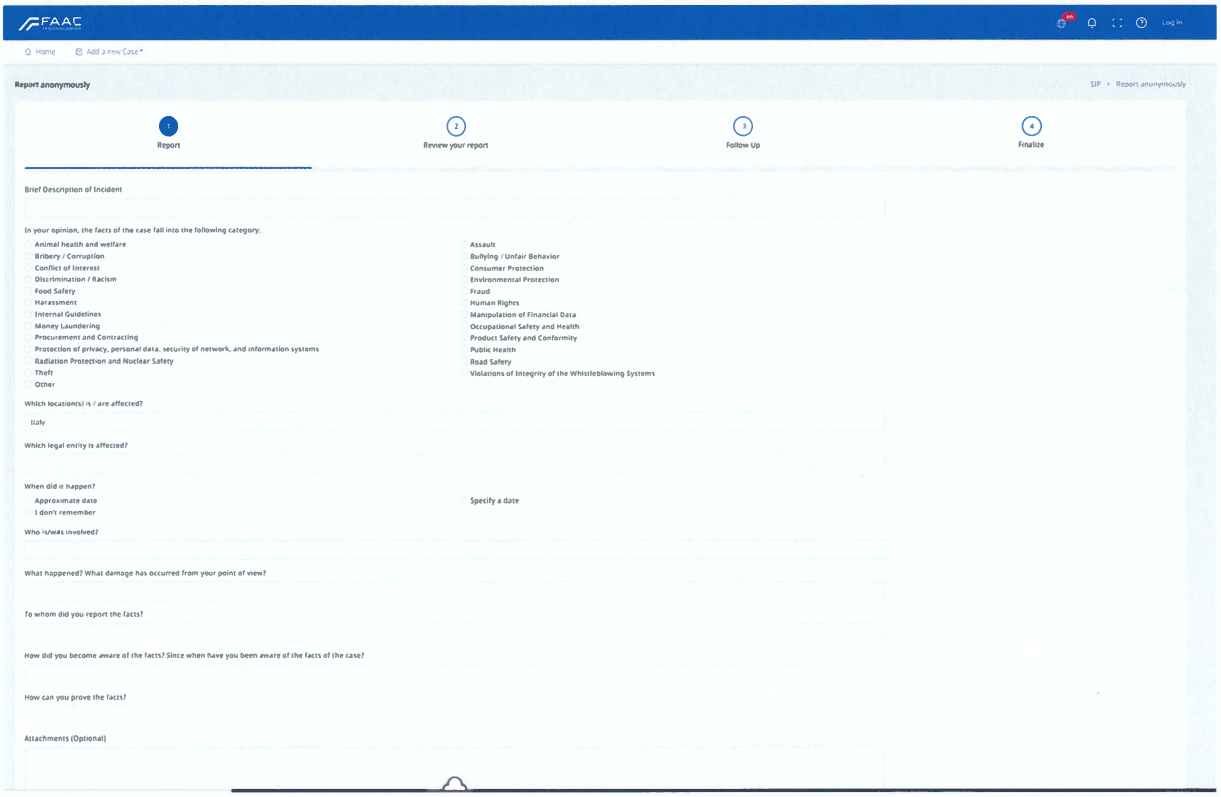
2.3. Anonymous reports

You have the option of sending messages anonymously.
This means that your user data (username, contact details, IP address, terminal device, browser data) will not be forwarded to the internal office.

You should include as many details as possible in the report. You can attach files to your message. The metadata of the file attachments that allow conclusions to be drawn about your identity will be automatically removed by the Smart Integrity Platform.

If you report anonymously, please consider the following:

- Consider in advance which people in the Company have access to the information that you want to report. This could allow those involved to narrow down the group of individuals who could possibly act as whistleblowers.
- Try to formulate the facts neutrally. Do your best to avoid phrases or formulations that would allow conclusions to be drawn about your identity.



2.4. Confidential reports

You have the option to send messages confidentially.
This means that the data that you provided when you logged in will be forwarded to the internal office. When you use the link on the Company's website, you will be asked to provide your contact details when submitting a confidential report.

You should include as many details as possible in the report. You can attach files to your message. The metadata of the file attachments that allow conclusions to be drawn about your identity will be automatically removed by the Smart Integrity Platform.

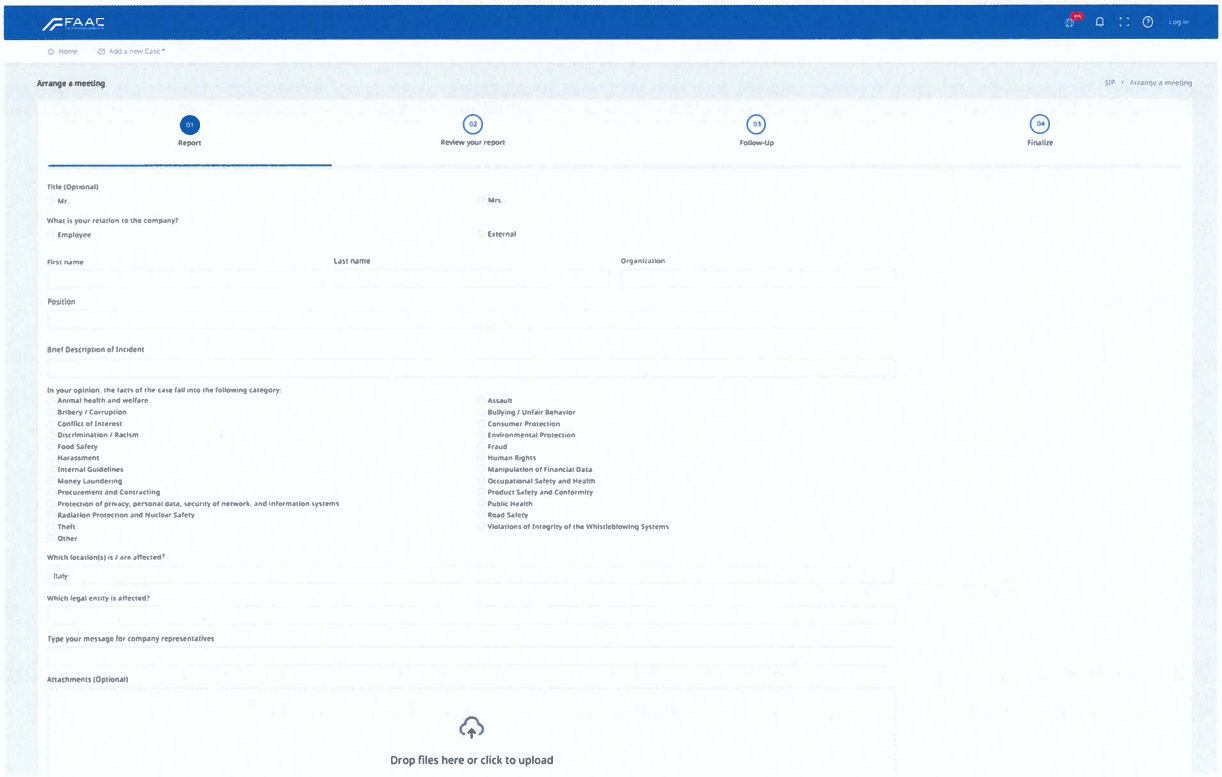


2.5. Arrange a meeting

You have the possibility of arranging a meeting for the submission of a report.

Use the "Arrange a meeting" function on the Smart Integrity Platform and provide some information about the issue. This helps the Internal Reporting Office to classify the facts and to designate a contact person for the meeting.

Use the Smart Integrity Platform to exchange information about the issue in advance. This keeps the data in the secure environment of the platform.

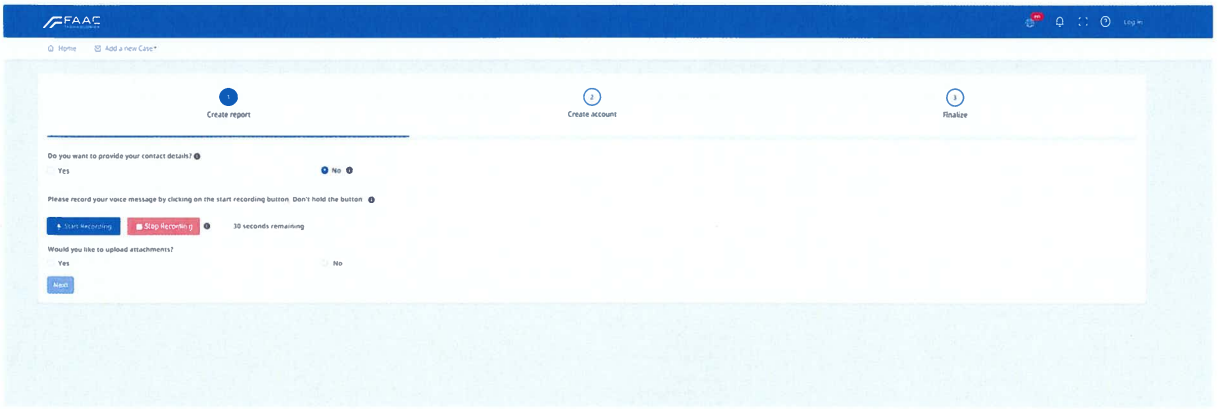


2.6. Voice Reports

You have the possibility of sending a voice message for the submission of a report.
For anonymous communication, the anonymous voice message can be used.

- The maximum duration of each voice message is 30 seconds. If your message is longer, you can record more than one message.
- If the user ends the voice message registration or closes the tab/window of the browser without clicking "Next", the data of the voice message will be deleted for security reasons.

Once the voice message is submitted, it will be received by the Internal Reporting Office.



2.7. External Reports

We encourage our employees to always report information about violations or reasonable suspicion of a violation internally first and have it reviewed by the Internal Reporting Office.

Indeed, if the suspicion is not substantiated or the information turns out to be incorrect or incomplete, the whistleblower that used the internal channel will not face consequences for reporting incorrect information.

An external report is the oral or written communication of information about violations to the competent authorities.

Cases in which whistleblowers can report externally are the following:

a) If whistleblowers do not receive a response within the statutory period after an internal report
b) If whistleblowers fear or are exposed to reprisals
c) If the violation is of public interest. *Examples of public interest notifications are:*
   - *Management misconduct that has caused or could have caused significant harm to affected parties;*
   - *Environmental damage caused by wrong decisions or actions by those affected in the company that have or could have a significant impact on the public;*

- *Systematic actions that could be construed as fraud against investors, shareholders or members of the company;*
- *Price-fixing agreements with competitors;*
- *Actions or conditions that could or might endanger the physical safety of customers and employees, for example systematic errors in train or aircraft maintenance.*

In any case, we advise employees who choose the external reporting route to seek legal advice.

External reporting offices in Italy:

In Italy, where FAAC SpA Unipersonale (HQ of FAAC Technologies Group) is located, the Public Authority appointed by law for external reports is:

ANAC Autorità Nazionale Anticorruzione ("National Authority against Corruption")
c/o Palazzo Sciarra, Via Minghetti 10, 00187 Roma (ITALY) phone +39 06 62289571
https://www.anticorruzione.it/-/whistleblowing (available in Italian only)

ANAC Platform for Whistleblowing notification (available in Italian only):
https://whistleblowing.anticorruzione.it/#/



Section 3: Procedure for processing a report

3.1. Confidentiality

The Internal Reporting Office is responsible for maintaining the confidentiality of the information related to the report.

3.2. Protection of the whistleblower

The Internal Reporting Office is responsible for protecting the whistleblower who has reported in good faith a reportable event to the Internal Reporting Office via the Smart Integrity Platform or via other means. It is company priority to protect the whistleblower from reprisals or retaliation. In this regard, we refer to Section 4 of this Policy.

Whistleblowers who have made an anonymous report and who have been identified at any point during the internal investigation, or who have voluntarily disclosed their identity, shall also be protected. The Internal Reporting Office is obliged to protect the identity of the whistleblower in all cases.

3.3. Protection of the persons involved

Affected persons are natural or legal persons who are indicated in the report or disclosure as having committed the violation or with whom the designated person is associated.

Example: According to the allegation in the report, Maria knowingly signed off on false time-sheet reports of Company A Ltd as factually correct.

The persons involved in this case are Maria, the persons who filled the time sheets, and the management and employees of Company A Ltd who are involved in the process of approving and handling the time sheet reports and related payments. Other people who knew about the facts are also involved. The Internal Reporting Office is responsible for the protection of Maria and other involved persons until the end of the internal investigation. If the allegation turns out to be unsubstantiated or false, the protection continues even after the end of the investigation.

3.4. Process handling

The Internal Reporting Office will notify the whistleblower of the receipt of the report via the Smart Integrity Platform within a maximum of seven (7) days.

The status of the report will be changed from "New" to "Open" or "Assigned" once the report has been read and processed.

Whistleblowers are required to cooperate during the internal investigation and to answer queries from the Internal Reporting Office promptly and truthfully.

Within a maximum of three (3) months after receipt of the report, whistleblowers are informed by the Internal Reporting Office about the follow-up measures.

Follow-up actions aim to verify the validity of the allegations mentioned in the report and, if necessary, to address the reported violation through internal inquiries, investigations, and legal means.

3.5. Reporting a conflict

If there is a conflict in the Internal Reporting Office, the management must be informed immediately.

Responsibility for internal investigations shall be delegated to an independent internal person or to an external person.
Management shall ensure that the persons in conflict with the report do not have access to the corresponding report on the Smart Integrity Platform.

If there is a conflict of interest within management, the Internal Reporting Office must comply with the escalation levels under Section 3.6, "Escalation Levels."

3.6. Escalation levels

After receiving the report, the Internal Reporting Office carries out an initial verification of the facts and may ask the whistleblower for clarification or further information. If the reported allegations turn out to be correct or partially correct, the Internal Reporting Office carries out an initial risk assessment as configured in the Smart Integrity Platform.

If the risk of the report is classified as high or very high, the Whistleblowing Committee of FAAC Technologies Group must be contacted immediately.

If there is an internal conflict regarding any members of the Whistleblowing Committee of FAAC Technologies Group, the Internal Reporting Office is authorized and obliged to contact the member/members of the Whistleblowing Committee of FAAC Technologies Group not directly involved.

The internal conflict and the measures taken to deal with it must be documented in the internal communication area of the corresponding report on the Smart Integrity Platform.

Current composition of Whistleblowing Committee in FAAC Technologies Group (based in FAAC SpA):

- Internal Reporting Office members:
  - Group Internal Auditing Director & Group DPO, also OdV member
  - Group Internal Auditor, also OdV member
- Chairman of OdV (Organismo di Vigilanza, as defined by Italian law Dlgs. 231/2001)
- Group Executive Chairman
- Group CPO (Chief People Officer)

3.7. External support

The Company reserves the right to request external support for the internal investigation. A data processing agreement or a confidentiality agreement must be drafted with the persons and/or Companies assigned.

Employees who are contacted by the external support within the scope of an internal investigation are required to cooperate and provide truthful information about the facts mentioned in the allegation.

3.8. Release of information

The persons involved have the right to be informed about the internal investigation, provided that the report concerns them personally.
Corresponding information can be communicated to the data subjects in encrypted form by the Internal Reporting Office.

In certain cases, the Internal Reporting Office may withhold information until the internal investigation has been completed.
In any case, the identity of the whistleblower must be protected and treated confidentially.

3.9. Deletion of reports

The Internal Reporting Office is obliged to delete notifications in compliance with the GDPR. If the reports do not contain any relevant information, or if they contain fictitious or non-real information, the reports can be deleted immediately after receipt and examination.

In other cases, the processing of notifications is as follows:

- Upon the expiration of the retention period, which is five (5) years after the end of the proceedings (e.g. in the case of civil, labor, or criminal proceedings), the Internal Reporting Office is in charge of documenting, justifying, and executing the deletion. In exceptional cases, a longer retention period can also be justified. The reason must be entered in the internal communication area.
- As soon as the deletion has been confirmed, the message contents, as well as the files and communication details externally and internally, are completely and irrevocably deleted after 24 hours.

The Internal Reporting Office can view the list of deleted messages (the deletion log). The following data is kept indefinitely for the purpose of tracking data deletions:

- Case ID
- Reporting date
- Category
- Subject
- Reason for deletion
- Date of deletion
- Name of the Internal Reporting Office member who deleted the report
- Name of the Internal Reporting Office admin who confirmed the deletion

Section 4: Prohibition of retaliation

4.1. What is Retaliation

Retaliation is defined as any direct or indirect action or omission in a professional context that is triggered by an internal or external report or disclosure and that causes or may cause the whistleblower to suffer an unjustified disadvantage. This also applies if associated or related persons are subject to reprisals.

Examples of reprisals:

- Termination of employment contracts
- Transfer
- Overstepping for promotion
- Assignment of menial tasks or tasks unrelated to the previous job
- Withdrawal of responsibility
- Defamation or slander
- Termination of contracts with service providers or freelancers
- Non-renewal of contracts
- Exclusion from application procedures
- Rejection of applications
- Placing the service provider on a "blacklist"
- Non-inclusion of the service provider's application in tenders
- Financial discrimination

4.2. Reporting retaliation

If, despite the legislation prohibiting retaliation, affected parties take such actions/measures against the whistleblower, it must be reported immediately to the Internal Reporting Office.

Please use the communication option via the Smart Integrity Platform for this purpose.

Section 5: Policies and applicable laws

Link to policies and applicable laws:

Policies

- **Code of Ethics of FAAC Technologies Group**
  https://faactechnologies.com/wp-content/uploads/2022/06/codice-etico-en.pdf

- **Privacy Policy of FAAC Technologies Group**
  https://www.iubenda.com/privacy-policy/27777535/legal

- **Smart Integrity Platform User Terms**
  https://customer-portal.smartintegrityplatform.com/IT/faacgroup-237/third-party/user_policy

- **Smart Integrity Platform Privacy Policy**
  https://customer-portal.smartintegrityplatform.com/IT/faacgroup-237/third-party/data_privacy

Applicable laws

- **EU Directive 2019/1937**
https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32019L1937&qid=1720428070901

- **Italian Legislative Decree 24/2023**
https://www.gazzettaufficiale.it/atto/serie_generale/caricaDettaglioAtto/originario?atto.dataPubblicazioneGazzetta=2023-03-15&atto.codiceRedazionale=23G00032&elenco30giorni=false

- **Italian guidelines issue by ANAC (only Italy) nr 311 12.07.2023**
https://www.anticorruzione.it/documents/91439/146849359/Delibera+n.+311+del+12+luglio+2023+-+linee+guida+whistleblowing+versione+schematizzata.pdf/7c8290da-f1b0-1c1f-8bc0-3904f023f299?t=1689332548748

Version	Date	Update on	Update by	Review by	Approval by
Nr 1	25/07/2024		Andrea Lanzoni Anna Tassinari	CPO	Executive Chairman

FAAC Technologies Group

FAAC SpA Unipersonale
Via Calari 10, 40069 Zola Predosa (Bologna) Italy

Whistleblowing policy approved and signed on 25/07/2024

Management Signature