

DIGITAL360

Procedure for handling whistleblowing reports

Last updated on 28 July 2026

CONTENTS

1. Purpose	3
2. Procedure for handling reports.....	3
3. Scope	4
3.1. SUBJECT-MATTER SCOPE	4
3.2. OBJECTIVE SCOPE OF APPLICATION	4
4. Relevant documents and legislation	5
5. Terms and definitions	5
6. Internal reports: the Organisational Model defined <i>by the Digital360 Group</i>	6
6.1. TOOLS TO SUPPORT THE PROCESS: THE IT PLATFORM	6
6.2. ROLES AND RESPONSIBILITIES	7
6.2.1. Reporting Committee (Direct Channel)	7
6.2.2. Alternative Manager (Alternative Channel)	8
6.2.3. Investigating Authorities	8
6.3. FORMS AND CHARACTERISTICS OF REPORTING	8
6.4. STAGES AND ACTIVITIES	11
6.4.1 Preliminary assessment stage.....	11
6.4.2 Preliminary investigation phase	11
6.4.3 Stage for assessing the results of the preliminary investigation.....	12
6.4.4 Feedback to the person who made the report.....	12
7. External reports.....	13
8. Guarantees and measures to protect the whistleblower	13
8.1. RIGHT TO CONFIDENTIALITY.....	14
8.2. PROHIBITION OF RETALIATION	14
8.3. SUPPORT MEASURES OFFERED BY THIRD SECTOR ORGANISATIONS	16
8.4. PROCESSING OF PERSONAL DATA	16
9. Penalties	17
ANNEX A – Group companies.....	18
ANNEX B – Reports relevant to the procedure.....	19
ANNEX C – Relevant legislation	23
ANNEX D – Instructor’s declaration of commitment	24
ANNEX E – External reports	25
ANNEX F – Guidelines for submitting internal reports via the platform	27

1. Purpose

Recognising that corporate ethics require *governance* based on trust, transparency and integrity, the **Digital360 Group** (hereinafter “the Group” or “Digital360”) encourages its employees and third parties to cooperate in order to bring to light any unlawful, fraudulent or suspicious activities, as well as any other irregularities or conduct that does not comply with the law or the Group’s internal regulatory framework.

To this end, the Digital360 Group has drawn up and approved this **Procedure, which forms an integral part of the internal regulatory framework set out in the Anti-Corruption Policy adopted by the Group**, with the aim of enabling its staff and all third parties operating directly or indirectly on behalf of the Company to report breaches of regulatory provisions that harm the public interest or the integrity of the organisation.

In particular, through this document, the Group aims to define the principles and rules, as well as the roles and responsibilities, within the whistleblowing reporting management process, in accordance with **EU Directive 2019/1937** on the protection of persons reporting breaches of Union law, as well as the **applicable legislation in each country where the companies of the Digital360 Group are based**.

This Procedure supplements the Digital360 Group’s Code of Ethics and the Anti-Corruption Policy, as well as the Organisational Models adopted pursuant to Legislative Decree 231/2001 (where applicable, with reference to the Group’s Italian companies) and any other national provisions implemented by the companies regarding the prevention of corporate crime, with reference to the Group’s foreign companies.

2. Management of the procedure

This Procedure, adopted by Digital360 S.p.A., constitutes a single document for the entire Group. For this reason, all companies within the Digital360 Group are required to accept it and implement it through their governing bodies at the earliest opportunity following the completion of the acquisition, with any amendments made necessary by local regulations.

The procedure is made available and can be consulted in the following ways:

- via the company intranet “Digital360Workspace” or another online noticeboard shared with staff;
- via the company’s website, in the *Legal & Compliance* section [at https://www.digital360.it/legal-compliance/](https://www.digital360.it/legal-compliance/), for all interested parties.

The adoption of this Procedure, and any substantial amendments thereto, shall be preceded by consultation with the trade unions, via a specific notification.

3. Scope of application

3.1. Subject Scope

This Procedure applies to Digital360 S.p.A. and to the companies of the Digital360 Group listed in Annex A – Companies within the scope of this Procedure.

From the perspective of the protected parties, this Procedure distinguishes between the **whistleblower** (or reporter, strictly speaking) – that is, the individual who reports breaches occurring within their own workplace – and **other parties** who, whilst not having made the report directly, are nevertheless deemed worthy of protection.

The first category includes:

- Employees and self-employed workers, as well as contractors, freelancers and consultants carrying out their work at the Company, including during their probationary period;
- Shareholders and members of the board of directors, management or supervisory board, including the Company's non-executive directors and those who perform such functions de facto;
- Trainees, including unpaid ones, and volunteers, who carry out their work at the Company;
- Employees or contractors of the Company's contractors, subcontractors and suppliers;
- Former employees of the Company;
- Candidates for a position at the Company who have obtained information about breaches during the selection process or at other stages of pre-contractual negotiations, and who may be subject to retaliation.

The second category (other persons protected by the procedure) includes:

- facilitators;
- people connected to the whistleblower who may face retaliation in a work context, such as colleagues who have a regular or recurring relationship with that person;
- people in the same workplace who are linked to the whistleblower by a stable emotional or family relationship;
- organisations owned by the whistleblower or for which they have worked, as well as organisations operating within the same workplace.

3.2. Objective scope of application

For the purposes of applying this Procedure, the Digital360 Group considers reports to be relevant where they concern breaches, unlawful conduct (including attempted breaches), behaviour, acts or omissions that harm the public interest or the integrity of the Company.

For a detailed breakdown of the areas relevant to reports, please refer to Annex B – Reports relevant for the purposes of this Procedure.

4. Relevant documents and legislation

This Procedure has been drawn up in compliance with current regulatory provisions concerning the protection of whistleblowers, anti-corruption and the protection of personal data, and is also in accordance with the national collective labour agreements applicable to staff.

For a detailed overview of the relevant legislation, please refer to *Annex C – The legislation relevant* to this Procedure.

5. Terms and definitions

Term	Definition
Whistleblowing Committee	An independent body responsible for guiding and coordinating the process of managing reports (from the point of receipt through to carrying out the necessary investigations to verify their content). Under the Digital360 Group Model, the Committee is appointed by the Company and its members are listed on the Platform in the section dedicated to the <i>Legal Entity</i> .
Third Sector Entity (ETS)	A Third Sector Entity registered in the relevant register with ANAC and affiliated with ANAC pursuant to Article 18 of Legislative Decree 24/2023, tasked with providing support measures to whistleblowers, including information, assistance and free advice on reporting procedures and protection against retaliation.
Facilitator	An individual working within the same workplace who is tasked with assisting the whistleblower throughout the reporting process, whilst ensuring that their assistance confidential.
Alternative Manager	An independent body that replaces the Reporting Committee whenever a report concerns, even only in part, one or more members of that Committee. Its establishment is intended to ensure the effectiveness of the protection afforded to the whistleblower, by preventing situations of conflict of interest — even potential ones — on the part of the body handling the report during the assessment and investigation phases. Under the Digital360 Group Model, the Alternative Manager is appointed by the Company, and the members are listed on the Platform in the section dedicated to the <i>Legal Entity</i> .
Investigator	A person called upon to assist during the preliminary investigation phase should the Reporting Committee or the Alternative Manager so request. Some of these are specifically identified by the Company, for example within the departments or strategic corporate roles most closely involved in the management of reports of wrongdoing (as set out in paragraph 6.2.3). Other investigators may be identified and appointed for specific reports, depending on their possession of particular skills or based on specific requirements in the handling of the report.
Person involved	A natural or legal person mentioned in an internal or external report as the person to whom the breach is attributed or as a person otherwise implicated in the reported breach.

Platform	A computer system serving as the tool for receiving and managing reports, with technical features designed to protect the confidentiality of the of the Whistleblower, including through the use of encryption tools.
Whistleblower	A natural person who reports information on breaches discovered within their work context, whilst carrying out current or past work or professional activities.
Report	A written or oral communication, made in accordance with the procedures set out in this Procedure, containing information (including reasonable grounds for suspicion) concerning breaches that have been committed or which, on the basis of concrete evidence, may be committed within the Organisation with which the person making the report has a legal relationship, or any other information concerning conduct aimed at concealing such breaches.
Breach	Behaviour, acts or omissions that harm the public interest or the integrity of the Company and which are detailed <i>in Annex B – Reports relevant to the procedure</i> .

6. Internal reports: the Organisational Model defined by the Digital360 Group

6.1. Tools to support the process: the IT Platform

In defining its Model for the management of reports of breaches or unlawful conduct, the Digital360 Group has adopted a **Platform to automate and facilitate the receipt and management of reports**, which is also capable of ensuring, through IT systems and data encryption techniques, the confidentiality of the whistleblower's identity, the content of the report and the related documentation. This Platform can be accessed via the following link: https://digital360groupwb_whistleblowing.keisdata.it/

Within the Platform, each Group company has set up a dedicated instance for its individual *legal entity* in order to keep the reporting channels and their ^{management} separate¹.

In accordance with this Procedure, every internal report, as well as any subsequent communication with the Whistleblower, must take place within the Platform, where all documentation relating to the case will be entered and archived.

The Platform, which **allows for the submission of anonymous reports**, enables users to communicate with the Whistleblower during the course of internal investigations.

In designing the Model for the management of reports of breaches or unlawful conduct, the Digital360 Group has identified all users with access to the Platform, based on the **authorisation levels** set out in the table below.

¹ The segregation of the reporting channel and its management is carried out in accordance with the provisions of European legislation and Article 4(4) of Legislative Decree 24/2023. In compliance with current legislation, the Group companies covered by this Procedure may not share the same internal reporting channel or its management.

Profile	Definition
Preliminary Assessor	An authorisation profile that allows the holder to view reports received by the Company, to carry out an initial assessment of the facts presented in order to determine whether to proceed, and to initiate any dialogue with the Whistleblower to gather further information.
Direct Channel	An authorisation profile dedicated to the Reporting Committee, which allows the Committee to view reports received by the Company and to carry out the preliminary investigation and management of the report, in order to assess its admissibility and validity, including its closure.
Alternative Channel	An authorisation profile assigned to a person other than the Reporting Committee, which enables the receipt and management of reports in cases where the Whistleblower decides not to refer them to the Committee due to a conflict of interest on the part of the Committee regarding the subject matter of the report. This authorisation profile is assigned to the Alternative Manager.
Investigator	An authorisation profile that allows access to the platform and enables the holder to provide support during the preliminary investigation phase, should the Reporting Committee so request.

These roles are defined independently and separately for each Group company within the scope of this Procedure. Each user is provided with unique login credentials, which they are required to keep secure and not disclose to third parties.

6.2. Roles and responsibilities

The Whistleblowing Management Model defined by the Digital360 Group sets out the following roles and responsibilities.

6.2.1. Reporting Committee (Direct Channel)

The Reporting Committee is responsible for guiding and governing the process for managing reports of breaches or unlawful conduct; its role is to receive, analyse and direct such reports, in particular those concerning:

- Carrying out preliminary assessments of the admissibility, validity and merits of reports;
- Providing an initial response to the Whistleblower regarding whether the report has been accepted or rejected;
- Direct and coordinate the conduct of the preliminary investigation, aimed at ascertaining the facts forming the subject of the report, using the tools and techniques available and in accordance with current regulations;
- Order the closure of the investigation and provide feedback to the Whistleblower on the outcome of the report;
- Engage with and support management and company departments in implementing corrective/mitigation measures and, where appropriate, imposing disciplinary sanctions.

The involvement of Committee members will be assessed on the basis of the scope of the report and their relevant areas of expertise, in accordance with the principle of data minimisation.

It should be noted that, in the event of a prolonged absence (exceeding 7 days) of one of the members, the multi-member composition nevertheless allows reports to be handled and a response to be provided to the Reporter.

6.2.2. Alternative Administrator (Alternative Channel)

The Alternative Channel is an additional channel for receiving reports, managed by a party other than the Reporting Committee (namely the Alternative Manager)

The Digital Group has established this additional channel to ensure impartiality and the protection of the Whistleblower should the report concern one of the Committee's members, and in all cases where one of the members is in a situation of conflict of interest.

Through a dedicated access point on the Platform, the Alternative Manager therefore performs the same functions as the Reporting Committee, both during the preliminary assessment phase and during the investigation phase.

As part of the latter, the Alternative Manager assigns the relevant investigating officers based on the content of the report.

6.2.3. Investigators

Investigators are individuals who may be involved in the preliminary investigation phase, where so decided by the Reporting Committee or the Alternative Manager, to assist the latter in carrying out verification activities. Furthermore, where appointed and solely for companies incorporated under Italian law that have an Organisational Model pursuant to Legislative Decree 231/2001, the Supervisory Body of the company involved in the report shall participate in the preliminary investigation (in the case of reports concerning breaches of Legislative Decree 231/2001 and the Organisational Model adopted by the companies within the scope of application pursuant to Legislative Decree 231/2001).

Each investigator must sign a declaration of undertaking to maintain the confidentiality of the whistleblower's identity and of the information relating to the report, where this is not already provided for by any applicable ethical standards (*Annex D – Investigator's Declaration of Undertaking*).

Other investigators may be identified and appointed for specific reports, depending on their possession of particular expertise or based on specific requirements in the handling of the report. In this case too, each investigator must sign the aforementioned declaration of undertaking.

6.3. Forms and characteristics of the report

Internal reports must be addressed exclusively to the Receiving Party (Reporting Committee or Alternative Manager) and should preferably be made in **writing**, using the digital methods described in detail *in Annex F – Guidelines for submitting internal reports via the Platform*.

Once the report has been submitted, the Platform will generate an alphanumeric code and the corresponding key.

The Whistleblower is therefore advised to check the Platform periodically, as any communications and requests for additional documentation from the Receiving Entity, deemed necessary to proceed, will be communicated via the Platform.

Please note that, should the code and its corresponding key be lost, the Reporter will be unable to access the report. The code and key cannot, in fact, be duplicated. It is therefore the Reporter's responsibility to take due care of them. In the event of loss, it is the Reporter's responsibility to inform the Recipient of this situation, providing all relevant information regarding the report for which the code or key has been lost.

Should the Whistleblower not wish to submit the report in writing, the report may be **made orally**, either via a voice messaging system made available on the Platform (which will allow the report to be recorded, subject to the explicit consent of the whistleblower), or, at the Whistleblower's request², through a face-to-face meeting arranged within a reasonable timeframe at the premises designated by the Company. In this case, a member of the Reporting Committee or the Alternative Manager may offer their support to the whistleblower in completing the report on the Platform, with a view to ensuring it is handled appropriately and to guaranteeing greater confidentiality of the information.

Alternatively, subject to the Reporter's consent, the documentation relating to the report will be secured by means of a recording³ suitable for storage and playback, or by means of minutes. Should minutes of the meeting be drawn up, the Reporter may review them, amend them and confirm them by signing them before they are uploaded to the Platform.

In any case, those providing support to the Reporter may NOT retain the alphanumeric code and the corresponding report key generated by the Platform; these shall remain exclusively available to the Reporter.

Please note that the **internal report must relate to one of the relevant subject areas as set out *in Annex B – Reports relevant to the purposes* of this Procedure.**

The Report must be complete and comprehensive to enable the Reporting Committee to verify its validity. The Reporter, therefore – and all the more so if they wish to remain anonymous – is

² The request may be made via the Platform to ensure the confidentiality of the request itself.

³ Via the voice messaging system on the Platform.

required to provide all available and relevant information to enable the Reporting Committee and the investigators to carry out the necessary and appropriate checks and enquiries to verify the validity of the facts forming the subject of the report, such as, by way of example:

- the time and place at which the events forming the subject of the report took place;
- a clear and complete description of the facts covered by the report;
- the personal details or other information enabling the identification of the person(s) who carried out the reported acts (e.g. job title, place of work where they carry out their duties);
- any other information that may provide useful evidence regarding the existence of the reported facts;
- the names of any other individuals who may be able to provide information regarding the facts reported;
- any supporting documents relating to the report.

The requirements described above do not necessarily have to be met simultaneously, given that the Whistleblower may not have full access to all the required information at the time of submitting the report; however, it must be possible to piece this information together during the preliminary investigation.

The personal motives or psychological state of the Whistleblower are irrelevant for the purposes of handling the report.

Should the report not fall within the scope set out in Annex B, the Reporting Committee or the Alternative Manager may forward it to the relevant department, whilst simultaneously informing the reporter where known.

If the report is submitted to a party other than the Reporting Committee, as identified and authorised by the Company (for example, to one's line manager or superior), and the whistleblower expressly states that they wish to benefit from the protections relating to whistleblowing, or if such an intention can be inferred from the report, the report is considered a "whistleblowing report" and must be forwarded, within seven days of receipt, to the Reporting Committee, whilst simultaneously notifying the whistleblower of the forwarding.

Conversely, if the whistleblower does not expressly state that they wish to benefit from the protections, or if such an intention cannot be inferred from the report, the report is treated as an ordinary report.

6.4. Stages and activities

6.4.1 Preliminary assessment stage

The **Reporting Committee or the Alternative Manager** is responsible for the preliminary assessment phase of the report and carries out the following activities:

- Issues the Whistleblower **with an acknowledgement of receipt** of the report **within 7 days** of receipt;
- **Maintains contact with the Whistleblower**, who may be asked, if necessary, to provide further details regarding the report;
- **It follows up diligently on the reports received**, promptly initiating a preliminary analysis of the report in order to verify its compliance with applicable regulations and this Procedure, in particular by assessing the admissibility and validity of the complaint.

The preliminary assessment phase may be concluded in one of the following ways:

- by the report being dismissed, should it fall outside the scope of this Procedure and the conditions for proceeding are not met (see *Annex B – Reports relevant to the procedure*);
- by the commencement of the INVESTIGATION PHASE, aimed at taking all appropriate action to assess the validity of the reported facts.

6.4.2 Preliminary Investigation Phase

The **Reporting Committee** or the Alternative Manager is responsible for the preliminary investigation phase, in which it is supported by **the investigators** competent on a case-by-case basis depending on the subject matter of the report (as identified in paragraph 6.2.3 above, or investigators *newly* appointed from among internal or ^{external}⁴ parties competent in relation to the specific report).

In the case of external investigators, where it is necessary to share information relating to the report that could reveal the Whistleblower's identity in order to follow up on the report, the Reporting Committee or the Alternative Manager shall, before proceeding to share such information, obtain the Whistleblower's consent to the disclosure of their identity in accordance with the procedures set out in paragraph 8.1 below (Right to Confidentiality).

Should the report concern a breach of Legislative Decree 231/2001 or the Organisation, Management and Control Model (where adopted by the relevant Company), the members of the Supervisory Body, in their capacity as investigating officers, shall be promptly informed.

⁴ It is possible that individuals from outside the Company may be involved at this stage (e.g. experts, consultants or staff from another Group company).

The preliminary investigation phase comprises all activities aimed at verifying the content of the reports and gathering evidence useful for the subsequent assessment phase, during which the utmost confidentiality must be ensured regarding the identity of the Whistleblower and the subject matter of the report.

The main purpose of this phase is to verify the accuracy of the information under investigation and to document the established facts, through internal verification activities using objective investigative techniques and with the support of the relevant company departments concerned with the content of the report.

Should it be necessary to interview the Whistleblower (or other interested parties, witnesses or experts), the information gathered and/or the documents submitted must be archived and stored exclusively on the Platform for the purposes of tracing the operations carried out.

6.4.3 Assessment phase of the preliminary investigation's findings

The internal preliminary investigation phase must conclude with a judgement on the admissibility of the report; alternatively:

- by dismissing the report – deeming it inadmissible because it is unfounded, or because it has not been possible to ascertain the facts, or for other reasons;
- by notifying the company representatives of the organisation concerned of the outcome of the internal investigation, by sending a summary report detailing the actions taken and the information gathered, should the report be found to be well-founded and the facts reported therein be verified. This report shall acknowledge:
 - the evidence gathered;
 - the information obtained;
 - the facts established;
 - the steps taken during the preliminary investigation;
 - any mitigating and/or corrective actions.

Following the submission of the Report, the Company concerned may define and implement mitigating and/or corrective measures, in addition to those aimed at imposing, where appropriate, disciplinary sanctions in accordance with the provisions of applicable legislation, the relevant collective labour agreements and the applicable procedures designed to protect the Company's interests (e.g. disciplinary measures, legal proceedings, termination of the existing employment relationship).

6.4.4 Feedback to the whistleblower

Throughout the investigation phase, the Reporting Committee will continue to liaise with the Whistleblower, keeping them informed of the progress of the investigation, at least with regard to the key decision-making stages.

To ensure maximum transparency in the handling of the report, the Whistleblower may at any time access the Platform and view the processing *status* of the report, using **the alphanumeric code**

and the key generated by the Platform upon submission of the report.

Within three months of the date of the acknowledgement of receipt, the Reporting Committee or the Alternative Administrator must provide feedback to the Whistleblower, informing them of the action taken or intended to be taken in response to the report. In any event, once the investigation has been completed, the Reporting Committee or the Alternative Manager will notify the Whistleblower of the final outcome of the reporting procedure, which will enable the report to be closed on the Platform for the purposes of proper record-keeping.

7. External Reports

Where provided for by the legislation of the countries in which the Digital360 Group companies are based, and where specific conditions apply, the Whistleblower may make a report via an external channel. For the specific rules applicable in each country, please refer to Annex E – External Reports of this procedure.

8. Guarantees and Protective Measures for the Whistleblower

The entire process of receiving and handling reports must safeguard the rights of the Whistleblower. To this end, in accordance with current legislation, the Digital360 Group has not only provided for the option to submit anonymous reports, but has also put in place safeguards and measures to protect the Whistleblower, which will be applied where the following conditions are met:

- the breach falls within the objective scope of application of the legislation (details of which are provided below and in Annex B – Reports relevant to the procedure);
- the breach concerns conduct, acts or omissions likely to harm or prejudice the public interest or the integrity of the Company;
- there are reasonable grounds⁵ leading the whistleblower to believe that unlawful conduct or a breach is likely to have occurred.

If these requirements cannot be met, the report will be closed and the Whistleblower will be informed accordingly.

The protective measures set out in this Procedure are not guaranteed where, in relation to the report:

- the Whistleblower's criminal liability for offences of defamation or slander has been established, even by a non-final first-instance judgement;

⁵ See Article 16 of Legislative Decree 24/2023. On the same subject, see Recital 32 of the Directive, which states that *'This requirement is an essential safeguard against malicious, frivolous or unfounded reports, so as to ensure that persons who, at the time of making the report, deliberately and knowingly provided incorrect or misleading information, are excluded from protection. At the same time, this requirement ensures that the whistleblower continues to benefit from protection where they have made an inaccurate report in good faith. (...) The reasons that led the whistleblower to make the report should be irrelevant for the purposes of deciding whether to grant protection.'*

- The whistleblower's civil liability is established for having reported false information intentionally provided with intent or gross negligence.

8.1. Right to confidentiality

The identity of the whistleblower and any other information from which that identity may be deduced, directly or indirectly, may not be disclosed, **without the express consent of the whistleblower**, to persons other than those competent to receive or follow up on reports, who are expressly authorised to process such data in accordance with Articles 29 and 32(4) of Regulation (EU) 2016/679 and national legislation on the protection of personal data.

Please note that the protection of **the whistleblower's confidentiality** is also ensured in judicial and disciplinary proceedings.

The disclosure of the whistleblower's identity and of any other information or detail contained in the report from which the whistleblower's identity may be directly or indirectly inferred is permitted only where this constitutes a necessary and proportionate obligation imposed by the applicable law in the relevant country, in the context of investigations by national authorities or judicial proceedings, including for the purpose of safeguarding the right of defence of the person concerned.

Notwithstanding the obligation of confidentiality, Italian legislation also provides that the identity of the whistleblower may be disclosed only in the following cases:

- in the context of disciplinary proceedings, where the allegation is based, in whole or in part, on the report and knowledge of the whistleblower's identity is essential for the defence of ^{the accused}⁶;
- in proceedings initiated following internal or external reports, where such disclosure is also essential for the defence of the person ^{concerned}⁷.

In any event, even where current legislation permits the disclosure of the whistleblower's identity, **before such information is disclosed, it is necessary to obtain their express consent and to inform them in writing of the reasons underlying the need to disclose their identity.**

The Company is also required to protect the identity of **the persons involved and those mentioned in the report** until the conclusion of the proceedings initiated as a result of the report, in accordance with the same safeguards provided for the whistleblower.

8.2. Prohibition of Retaliation

The Policy for the management of reports of breaches or unlawful conduct established by the Digital360 Group also imposes an explicit prohibition on taking any form of retaliatory action against the Whistleblower and other protected persons.

⁶ See Article 12(5), second sentence, of Legislative Decree 24/2023

⁷ See Article 12(6) of Legislative Decree 24/2023

***Retaliation* is deemed to be any behaviour, act or omission – even if merely attempted or threatened – carried out as a result of the report, which causes or may cause the whistleblower, directly or indirectly, unjust harm.**

The following are examples of acts constituting retaliation:

- dismissal, suspension or equivalent measures;
- demotion or failure to be promoted;
- a change in duties, a change of workplace, a reduction in salary, or a change in working hours;
- the suspension of training or any restriction on access to it;
- negative performance appraisals or negative references;
- the imposition of disciplinary measures or other sanctions, including financial penalties;
- coercion, intimidation, harassment or ostracism;
- discrimination or otherwise unfavourable treatment;
- failure to convert a fixed-term employment contract into a permanent employment contract, where the employee had a legitimate expectation of such conversion;
- the non-renewal or early termination of a fixed-term employment contract;
- damage, including damage to a person's reputation, particularly on social media, or economic or financial harm, including the loss of economic opportunities and loss of income;
- inclusion on inappropriate lists on the basis of a formal or informal sectoral or industrial agreement, which may make it impossible for the person to find employment in that sector or industry in the future;
- the early termination or cancellation of a contract for the supply of goods or services;
- the revocation of a licence or permit;
- a request to undergo psychiatric or medical examinations. To be eligible

for protection:

- a. the Whistleblower must reasonably believe, in light of the circumstances of the specific case and the information available at the time of the report, that the information regarding the reported breaches is true. Mere assumptions or rumours, as well as information in the public domain, are not sufficient;
- b. the person must have reported facts even though they were not certain that they had actually occurred, or may have reported inaccurate facts due to a genuine error, or in any case where there are well-founded suspicions;
- c. the report must fall within the objective scope and must have been made in accordance with the provisions of current legislation;
- d. there must be a close link between the report and the adverse conduct, act or omission suffered – directly or indirectly – by the person making the report.

By definition, these rules do not apply to anonymous reports, as they are designed to protect the whistleblower from the risk of retaliation. However, they may apply if, following an anonymous report

the identity of the informant is revealed, in which case the informant may request to avail themselves of the protection provided for by the decree.

8.3. Support measures offered by Third Sector Organisations

Third Sector Entities (TSEs) registered in the relevant Register at ANAC and with which the Authority enters into specific agreements are required to provide support measures to whistleblowers (Article 18(1) and (2) of Legislative Decree 24/2023). Specifically, the role of Third Sector Entities is to provide expert support to the whistleblower, as well as to promote understanding of the whistleblowing framework and a proper awareness of the tools available, not least with a view to improving the quality of reports. By way of example, ETSs help explain the scope of application of Legislative Decree 24/2023, the conditions under which reports may be made and the procedures for doing so, as well as the protections provided. They may also offer psychological support and free counselling. This activity, which may take place before or after a report is made, also helps to ensure greater protection for whistleblowers who have suffered retaliatory measures.

The list of ETS organisations can be found at the following link: <https://www.anticorruzione.it/-/whistleblowing>

8.4. Processing of personal data

As part of the management of reports, Group companies process the personal data of whistleblowers and, where applicable, other categories of data subjects identified by them in the reports, in compliance with data protection legislation, including the GDPR, and in accordance with the privacy notice pursuant to Articles 13 and 14 of the GDPR attached to this procedure.

Compliance with the principle of ‘storage limitation’

Reports and all related documentation are retained in accordance with the time limits established under applicable legislation and set out in the attached privacy notice.

Rights of data subjects

The person concerned, the Whistleblower and all data subjects may exercise the rights provided for under the GDPR, in accordance with current legislation. It is understood that these rights may not be exercised if doing so would result in actual and concrete harm to the confidentiality of the whistleblower’s identity.

Further obligations

The Companies are required to:

- record the processing of personal data in the register of processing activities in accordance with Article 30 of the GDPR;
- carry out a data protection impact assessment (DPIA) in accordance with Article 35 of the GDPR, in relation to the processing of reports;

- authorise the members of the Whistleblowing Committee or the Alternative Manager, as well as staff and members of the Supervisory Body involved in the management of reports, to process personal data, in accordance with Article 29 of the GDPR;
- designate the suppliers involved in the whistleblowing management process who process personal data on behalf of the Companies as data processors, in accordance with Article 28 of the GDPR.

9. Sanctions

Failure to comply with this Procedure and the protective measures set out herein may result in the Digital360 Group applying its internal disciplinary system, in accordance with the provisions of applicable national employment law and the relevant collective labour agreements.

The Company reserves the right to take any necessary action, including legal proceedings, in full compliance with current and applicable regulatory provisions. In particular, this Procedure is without prejudice to the criminal, civil and disciplinary liability of the Whistleblower in the event of a malicious or defamatory report, or in cases of wilful misconduct or gross negligence.

It should be noted that the Company or any person who discloses or disseminates information on breaches covered by a duty of confidentiality⁸, or relating to copyright protection or the protection of personal data, or who discloses or disseminates information on breaches that damage the reputation of the person involved, shall not be liable to prosecution, provided that both of the following conditions are met:

- at the time of disclosure or dissemination, there are reasonable grounds to believe that the information is necessary to bring the breach to light;
- the report was made in accordance with the conditions laid down by current legislation to qualify for protection (reasonable grounds to believe that the information on the breaches was true and fell within the scope of breaches reportable under the law; internal and external reports made in accordance with the procedures and conditions laid down by law).

In addition to internal sanctions imposed by the organisation, where provided for by current legislation, the national authorities of the countries in which the companies of the Digital360 Group are based may also impose administrative fines on natural or legal persons, as provided for by current legislation.

⁸ This provision excludes the disclosure of classified information, or information covered by professional or medical confidentiality, or concerning the deliberations of judicial bodies, in respect of which the applicable legal provisions remain in full force.

ANNEX A – Companies within the scope of consolidation

Legal Entity	Country
Accompany S.r.l.	Italy
CryptoNet Labs S.r.l.	Italy
D360 Holding S.p.A.	Italy
Digital360 S.p.A.	Italy
Digital360 Gov S.r.l.	Italy
Digital Attitude S.r.l.	Italy
Digixem360 S.r.l.	Italy
Elite Divisions S.r.l.	Italy
FPA S.r.l.	Italy
ICTandStrategy S.r.l.	Italy
ICT LAB PA Ltd	Italy
Imageware S.r.l.	Italy
Methodos S.p.A.	Italy
Partner4Innovation S.r.l.	Italy
Spin Consulting S.r.l.	Italy
Wish Innovation S.r.l.	Italy

ANNEX B – Reports relevant to the procedure

ITALY Section

For the purposes of applying this Procedure, the Digital360 Group considers as relevant reports, exclusively, any conduct, acts or omissions that **harm the public interest or the integrity of the organisation**, of which it has become aware in the workplace, and which consist of:

A. breaches of national and European provisions constituting offences relating to the following sectors⁹:

- i. public procurement;
- ii. financial services, products and markets, and the prevention of money laundering and terrorist financing;
- iii. product safety and compliance;
- iv. transport safety;
- v. environmental protection;
- vi. radiation protection and nuclear safety;
- vii. food and feed safety, and animal health and welfare;
- viii. public health;
- ix. consumer protection;
- x. protection of privacy and personal data, and the security of networks and information systems;

B. breaches of European provisions consisting of:

- xi. acts or omissions that harm the Union's financial interests;
- xii. acts and omissions relating to the ^{internal} market¹⁰;
- xiii. acts and conduct that undermine the object or purpose of the provisions of Union acts in the areas referred to above;
- xiv. offences against the ^{European} Union's common foreign and security policy¹¹;
- xv. breaches of EU Regulation 2024/1689 on artificial intelligence (AI ACT);

C. breaches of national provisions consisting of:

- xvi. administrative, accounting, civil or criminal offences;
- xvii. unlawful conduct as defined under Legislative Decree 231/2001;

D. breaches of internal company regulations, such as:

- xviii. the Organisation, Management and Control Model adopted pursuant to Legislative Decree 231/2001;
- xix. the Digital360 Group Code of Ethics;
- xx. the Digital360 Group's Anti-Corruption Policy;
- xxi. Policies relating to *Diversity, Inclusion and Gender Equality*
- xxii. National collective agreements and, more generally, internal regulations (procedures, policies, operational instructions, etc.).

⁹ These are all offences falling within the scope of application of the European Union or national acts set out in the annex to Legislative Decree 24/2023, or of national acts implementing the European Union acts set out in the annex to Directive (EU) 2019/1937. ¹⁰ This includes infringements of EU competition and State aid rules, as well as infringements relating to the internal market connected with acts that breach corporate tax rules or mechanisms designed to obtain a tax advantage that undermines the object or purpose of the applicable corporate tax legislation.

¹¹ These are infringements of the EU measures referred to in Chapter I-bis, Title I, Book II of the Criminal Code, as well as Article 12, paragraph 1-bis, of Legislative Decree No 286 of 25 July 1998

Exclusions from the scope of application

There are restrictions on the scope of application of the subject matter covered by reports.

Information on reportable breaches does not include **reports that are manifestly unfounded, information that is already entirely in the public domain, or information obtained solely on the basis of unreliable rumours or hearsay** (so-called ‘office gossip’).

Furthermore, reports based on unfounded suspicions or rumours concerning personal matters that do not constitute an offence are excluded from the scope of this Procedure. This is because it is necessary both to take into account the interests of third parties who are the subject of the information contained in the report and to prevent the Company from carrying out internal investigations that risk being of little use and, in any case, costly.

The scope of this Procedure also does NOT include:

- a) complaints, claims or requests linked to a personal interest, which relate exclusively to one’s own individual employment relationship, or which concern one’s employment relationship with superiors;
- b) reports of breaches that are already mandatorily governed by European Union or national legislation concerning financial services, products and markets, and the prevention of money laundering and terrorist financing; transport safety and environmental protection, or by national legislation implementing European Union legislation in the same areas (details of the relevant legislation are set out in the Annex to Legislative Decree 24/2023, Part II);
- c) reports of breaches relating to national security, as well as to procurement contracts concerning defence or national security matters, unless such matters fall within the scope of the relevant secondary legislation of the European Union.

A further limitation on the scope of application of this Procedure concerns specific national or European Union provisions relating to:

- d) classified information;
- e) legal and ^{medical} professional privilege¹²;
- f) the confidentiality of the deliberations of judicial bodies;
- g) matters of criminal procedure.

¹² The confidentiality of communications between lawyers and their clients (‘legal professional privilege’) is protected under national law and, where applicable, under EU law, in accordance with the case-law of the Court. Furthermore, the obligation to maintain the confidentiality of communications between healthcare providers, including therapists, and their patients, as well as the confidentiality of medical records (‘medical confidentiality’), as provided for by national and Union law, must not be prejudiced.

Spain Section

For the purposes of applying this Procedure, the Digital360 Group considers as relevant reports, exclusively, any conduct, acts or omissions that **harm the public interest or the integrity of the organisation**, of which it has become aware in the workplace, and which consist of:

E. breaches of national and European provisions constituting offences relating to the following sectors ¹³:

- xxiii. public procurement;
- xxiv. financial services, products and markets, and the prevention of money laundering and terrorist financing;
- xxv. product safety and compliance;
- xxvi. transport safety;
- xxvii. environmental protection;
- xxviii. radiation protection and nuclear safety;
- xxix. food and feed safety, and animal health and welfare;
- xxx. public health;
- xxxi. consumer protection;
- xxxii. protection of privacy and personal data, and the security of networks and information systems;

F. breaches of European provisions consisting of:

- xxxiii. acts or omissions that harm the Union's financial interests;
- xxxiv. acts and omissions relating to the ^{internal} market¹⁴;
- xxxv. acts and conduct that undermine the object or purpose of the provisions of Union acts in the areas referred to above;
- xxxvi. offences against the European Union's common foreign and security policy;
- xxxvii. breaches of EU Regulation 2024/1689 on artificial intelligence (AI Act);

G. breaches of national provisions consisting of:

- xxxviii. administrative, accounting, civil or criminal offences;
- xxxix. administrative offences resulting in financial loss to the Treasury and the Social Security system;

H. breaches of internal company regulations, such as:

- xl. the Digital360 Group Code of Ethics;
- xli. Digital360 Group Anti-Corruption Policy;
- xl.ii. Policies relating to *Diversity, Inclusion and Gender Equality*
- xl.iii. National collective agreements and, more generally, internal regulations (procedures, policies, operational instructions, etc.).

¹³ This refers to all offences falling within the scope of application of European Union or national legislation specified in the national legislation implementing the European Union acts listed in the Annex to Directive (EU) 2019/1937.

¹⁴ This includes infringements of EU rules on competition and State aid, as well as infringements relating to the internal market connected with acts that breach corporate tax rules or arrangements designed to secure a tax advantage that undermines the object or purpose of the applicable corporate tax legislation.

Exclusions from the material scope

There are limitations on the scope of application of the objective scope of reports.

Information that is manifestly unfounded, information that is already entirely in the public domain, and information obtained solely on the basis of unreliable rumours or hearsay (so-called ‘office gossip’) are not included within the scope of reportable breaches.

Furthermore, reports based on unfounded suspicions or rumours concerning personal matters that do not constitute an offence are excluded from the scope of this Procedure. This is because it is necessary both to take into account the interests of third parties who are the subject of the information contained in the report and to prevent the Company from carrying out internal investigations that risk being of little use and, in any case, costly.

The scope of this Procedure also does NOT include:

- a) complaints, claims or requests linked to a personal interest, which relate exclusively to one’s own individual employment relationship, or which concern one’s employment relationship with superiors;
- b) reports of breaches that are already subject to mandatory regulation under European Union or national legislation concerning financial services, products and markets, the prevention of money laundering and terrorist financing, transport safety and environmental protection, or under national legislation implementing European Union acts in the same areas;
- c) reports of breaches relating to national security, as well as to procurement contracts concerning defence or national security matters, unless such matters fall within the scope of the relevant secondary legislation of the European Union.

A further limitation on the scope of application of this Procedure concerns specific national or European Union provisions relating to:

- d) classified information;
- e) legal and ^{medical} professional privilege¹⁵;
- f) the confidentiality of the deliberations of judicial bodies.

¹⁵ The confidentiality of communications between lawyers and their clients (‘legal professional privilege’) is protected under national law and, where applicable, under EU law, in accordance with the case-law of the Court of Justice. Furthermore, the obligation to maintain the confidentiality of communications between healthcare providers, including therapists, and their patients, as well as the confidentiality of medical records (‘medical confidentiality’), as provided for by national and EU law, must not be prejudiced.

ANNEX C – Relevant legislation

Scope	Legislation
European Union	Directive 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons reporting breaches of Union law
	EU Regulation 679/2016 on data protection and subsequent provisions (GDPR) and national data protection legislation
Italy	Legislative Decree No. 24 of 10 March 2023 on the “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 containing provisions concerning the protection of persons who report breaches of national regulatory provisions”
	Legislative Decree No. 231 of 8 June 2001 , entitled “Regulation of the administrative liability of legal persons, companies and associations, including those without legal , pursuant to Article 11 of Law No. 300 of 29 September 2000”
	Organisational Model: Organisation, Management and Control Model adopted pursuant to Legislative Decree 231/2001, aimed at preventing the commission of specific types of offences within the corporate sphere.
	ANAC Whistleblowing Guidelines: “ <i>Guidelines on the protection of persons reporting breaches of EU law and the protection of persons reporting breaches of national regulatory provisions. Procedures for the submission and handling of external reports</i> ”, approved by ANAC by Resolution No. 311 of 12 July 2023, amended by Resolution No. 479 of 26 November 2025. “ <i>Guidelines on whistleblowing via internal reporting channels</i> ”, approved by ANAC by Resolution No. 478 of 26 November 2025.
Spain	Law 2/2023 regulating the protection of persons reporting regulatory breaches and combating corruption.

ANNEX D – Declaration of commitment by the trainer

I, the undersigned, (first name/surname) _____ (hereinafter: **“Person informed of the report”**), acting under my sole responsibility

DECLARES

A. that I have been made aware of the existence of a report concerning information on unlawful conduct (report ID: _____) for the purposes of carrying out specific investigative measures;

B. that I have been informed and undertake to maintain the duty of confidentiality to which I am bound in the performance of my duties, both with regard to the identity of the whistleblower and of any other person involved, as well as the facts forming the subject of the report;

C. that I have been informed and undertake to ensure that no retaliatory action is taken against the whistleblower or any other person who has even merely facilitated the report, or who is connected to the whistleblower by an employment relationship or a personal/family relationship.

D. that they are aware they have assumed the role of a Person Aware of the Report and that, as such, any breach of the duty of confidentiality or any act of retaliation constitutes grounds for the imposition of sanctions both by the Company and, where applicable, by the national authorities of the States in which the companies of the Digital360 Group are based, as set out in the Procedure adopted by the Company for the management of reports of wrongdoing (paragraph 9 ‘Sanctions’).

E. that they have read, understood and accepted the contents of the Procedure adopted by the Company for the management of reports of wrongdoing (*Procedure for the Management of Whistleblowing Reports*).

(place), (date)

(signature)

ANNEX E – External Reports: ITALY Section

Italian legislation provides for the possibility of making external reports to the Digital360 Group. **An external report may be made where one of the following conditions applies:**

- the internal reporting channel, whilst mandatory, is not operational or does not comply with the requirements of the law;
- the Whistleblower has already made an internal report and no action has been taken on it;
- the Whistleblower has reasonable grounds to believe that the Organisation would not take effective action on the internal report or perceives a real risk of retaliation should an internal report be made;
- the Whistleblower has reasonable grounds to believe that the breach may constitute an imminent or obvious danger to the public interest.

It should be noted that reports of unlawful conduct relevant under Legislative Decree 231/2001 or breaches of the Organisation, Management and Control Model adopted by the Company may not be the subject of an external report. Information on such breaches may only be shared via the internal channel referred to in Chapter 6 above.

The use of external reporting is, therefore, a last resort compared to internal reporting and may only be carried out where the breach to be reported is included in *Annex B – Reports relevant to the procedure*, Italy Section, under points A) and B).

It is the responsibility of the reporting person to assess whether any of the situations listed above apply before proceeding to make an external report.

External reports are made by the Whistleblower directly to ANAC, via the channels specifically provided for this purpose. These are:

- An online platform, which can be accessed via the ANAC services portal at the following URL:
<https://whistleblowing.anticorruzione.it/#/>
- Verbal reports
- Face-to-face meetings arranged within a reasonable timeframe

Furthermore, if a whistleblower believes they have suffered retaliation, they are entitled to submit a report to the National Anti-Corruption Authority (ANAC), which is responsible for the investigations assigned to it by law, using the form on the IT platform available on ANAC's official website. It is therefore important that anyone who has suffered retaliation does not submit the report to any party other than ANAC, so as not to undermine the safeguards guaranteed by the legislation, foremost among which is confidentiality.

On ANAC's official website, by clicking the link to the dedicated page, you can access the 'whistleblowing' service (<https://www.anticorruzione.it/-/whistleblowing>), where you will find clear and



easily accessible information regarding the reporting channel, the competent bodies responsible for handling reports, and the relevant procedures.

SPAIN Section

Spanish legislation provides for the possibility of making reports outside the Digital360 Group.

External reports are made by the whistleblower directly to the Autoridad Independiente de Protección del Informante (A.A.I.) and to the competent bodies of the autonomous communities via specifically designated channels.



ANNEX F – Guidelines for submitting internal reports via the platform

The Guidelines are available via the company intranet “Digital360Workspace” or another digital noticeboard shared with staff, and in the *Legal & Compliance* section at <https://www.digital360.it/legal-compliance/> for all interested parties.