DIGITAL 360

Whistleblowing Reports Management Procedure

Date of last update, March 11, 2025

SUMMARY

Digital360 S.p.A.
Viale Bodio 37, 20158 – Milano
C.F. e P.IVA: 08053820968
REA: MI – 2000431

Camera di Commercio Milano
Monza Brianza Lodi
Capitale Sociale Versato:
€2.055.034,60
PEC: digital360@pec.it

1. Purpose

Aware that corporate ethics requires governance based on trust, transparency and integrity, the **Digital360 Group** (hereinafter "**the Group**" or "**Digital360**") encourages the collaboration of its employees and third parties for the purpose of bringing to light illicit, fraudulent or suspicious phenomena and any other irregularities or conduct not in compliance with the law and the Group's internal regulatory system.

To this end, the Digital360 Group has drafted and approved this **Procedure, an integral part of the internal regulatory framework provided for by the Anti-Corruption Policy adopted by the Group**, with the intent to enable its Personnel and all Third Parties that operate directly or indirectly on behalf of the Company to report violations of regulatory provisions that harm the public interest or the integrity of the organization.
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 compliance with **EU Directive 2019/1937** concerning the protection of people who report breaches of Union law, as well as **the applicable legislation in each country where the Digital360 Group Companies are based**.

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

2. Procedure management Methods

This Procedure adopted by Digital360 S.p.A. constitutes a single document for the entire Group. For this reason, all Digital360 Group Companies are required to accept and implement it through their administrative bodies at the first useful opportunity following the completion of the acquisition transaction, with any modifications made necessary based on local regulations.

The procedure is made available and accessible in the following ways:

- through the company intranet "*Digital360Workspace*" or other IT bulletin board shared with personnel.
- through the company website, in the Legal&Compliance section https://www.digital360.it/legal-compliance/ for all interested parties.

Digital360 S.p.A.
Viale Bodio 37, 20158 – Milano
C.F. e P.IVA: 08053820968
REA: MI – 2000431

Camera di Commercio Milano
Monza Brianza Lodi
Capitale Sociale Versato:
€2.055.034,60
PEC: digital360@pec.it

3. Scope of application

3.1. Subjective Scope

This Procedure applies to Digital360 S.p.A. and to the Companies of the Digital360 Group as indicated in *Annex A-Companies within the scope of this Procedure*.

From the perspective of protected subjects, this Procedure distinguishes the **whistleblower** (or reporting person, in the strict sense), i.e., the natural person who reports violations occurring within their work context, from **other subjects** who, while not having directly made the report, are nonetheless deemed worthy of protection.

The first category includes:

- Employees and independent contractors, as well as collaborators, freelancers and consultants who carry out their work activities at the Company, including during the probationary period.
- Shareholders and members of the management, direction or supervisory body, including non-executive directors of the Company and those who exercise such functions de facto.
- Trainees, including unpaid ones, and volunteers, who provide their services at the Company.
- Workers or collaborators of contractors, subcontractors and suppliers of the Company.
- Former employees of the Company.
- Candidates for a position at the Company, who have acquired information about violations during the selection process or in other phases of pre-contractual negotiations, and who could suffer retaliation.

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

- facilitators.
- people who are connected to the reporting person who could suffer retaliation in a work context, such as work colleagues who have a regular or recurring relationship with the person.
- People in the same work context linked to the reporting person by a stable emotional or family relationship.
- entities owned by the reporting person or for which they have worked, as well as entities operating in the same work context.

3.2. Objective scope

The Digital360 Group considers relevant reports, for the purposes of applying this Procedure, violations, unlawful conduct, including attempted ones, behaviors, acts or omissions that harm the public interest or the integrity of the Company.

For detailed information on the relevant areas for Reports, reference is made to Annex B-Reports relevant for the procedure purposes of this Procedure.

Digital360 S.p.A.
Viale Bodio 37, 20158 – Milano
C.F. e P.IVA: 08053820968
REA: MI – 2000431

Camera di Commercio Milano
Monza Brianza Lodi
Capitale Sociale Versato:
€2.055.034,60
PEC: digital360@pec.it

4. Reference Documents and Regulation

This Procedure is drafted in compliance with current regulatory provisions regarding the protection of persons who report violations, anti-corruption and protection of personal data and is also compliant with the National Collective Labor Agreements applicable to personnel.

For detailed information on the reference regulations, reference is made to *Annex C-Reference regulations of this Procedure*.

5. Terms and Definitions

Term	Definition
Reporter, reporting person or Whistleblower	Natural person who reports information about violations acquired within their work context, in the performance of work or professional activities, present or past.
Report	Written or oral communication, made in the manner described by this Procedure, containing information (including well-founded suspicions) regarding violations committed or which, based on concrete elements, could be committed in the Organization with which the reporting person has a legal relationship, or any other element regarding conduct aimed at concealing such violations.
Reporting Committee	Autonomous body tasked with directing and coordinating the report management process (from the reception phase to conducting the necessary investigations to verify the content). According to the Digital360 Group Model, the Committee is appointed by the Company and the members are indicated in the Platform in the section dedicated to the Legal Entity.
Facilitator	Natural person operating within the same work context with the task of assisting the reporting person in the reporting process, keeping their assistance activity confidential.
Involved Person	Natural or legal person mentioned in the internal or external report as a person to whom the violation is attributed or as a person otherwise involved in the reported violation.
Violation	Behaviors, acts or omissions that harm the public interest or the integrity of the Company and which are detailed in *Annex B-Reports relevant for the procedure purposes.*
Platform	Computer system that represents the tool for receiving and managing Reports, with technical characteristics suitable for protecting the confidentiality of the Reporter's identity, including through the use of encryption tools.

Digital360 S.p.A.
Viale Bodio 37, 20158 – Milano
C.F. e P.IVA: 08053820968
REA: MI – 2000431

Camera di Commercio Milano
Monza Brianza Lodi
Capitale Sociale Versato:
€2.055.034,60
PEC: digital360@pec.it

6. Internal Reports: the Organizational Method defined by the Digital360 Group

6.1. Support Tools: the IT Platform

In defining its own Model for managing reports of violations or unlawful conduct, the Digital360 Group has adopted a **Platform to automate and facilitate the reception and management of reports**, capable of ensuring, through IT methods and data encryption techniques, the confidentiality of the reporter's identity, the content of the report and related documentation. This Platform can be accessed at the following link https://digital360groupwb_whistleblowing.keisdata.it/.

Within the Platform, each Group Company has provided a dedicated instance for the individual Legal Entity in order to keep the reporting channels and related management separate[1].

Under this Procedure, every internal report as well as every subsequent communication with the Reporter must take place within the Platform, where all case documentation will be entered and archived.

The Platform, which **allows anonymous reports to be sent**, enables users to dialogue with the Reporter during internal investigations.

In designing the Model for managing reports of violations or unlawful conduct, the Digital360 Group has identified all users with access to the platform, based on the **authorization levels** shown in the following table.

Profile	Definition
Pre-assessor	Authorization profile that allows viewing reports received by the Company, conducting initial evaluations of the exposed facts to assess their procedural viability, as well as initiating any dialogue with the Reporter for collecting additional information.
Reporting Committee	Authorization profile that allows viewing reports received by the Company and conducting investigative and report management activities, in order to assess their admissibility and validity, including closure of the same.
Investigator	Authorization profile that allows accessing the platform and intervening as support in the investigative phase when requested by the Reporting Committee.

[1] The segregation of the reporting channel and its related management takes place in accordance with European regulations and Art. 4 paragraph 4 of Legislative Decree 24/2023. In compliance with applicable legislation, the Group Companies within the scope of this Procedure cannot share the same internal reporting channel and its related management.

Digital360 S.p.A.
Viale Bodio 37, 20158 – Milano
C.F. e P.IVA: 08053820968
REA: MI – 2000431

Camera di Commercio Milano
Monza Brianza Lodi
Capitale Sociale Versato:
€2.055.034,60
PEC: digital360@pec.it

This identification of profiles is provided autonomously and separately for each Group Company within the scope of this Procedure.

Each user has unique access credentials that they are required to keep secure and not disclose to third parties.

6.2. Roles and Responsibilities

The report management Model defined by the Digital360 Group provides for the following roles and responsibilities.

6.2.1. Reporting Committee

The function of directing and governing the process of managing Reports of violations or unlawful conduct is the responsibility of the Reporting Committee, which has the task of receiving, analyzing and directing reports, in particular:

- Conducting preliminary evaluations of procedural viability, admissibility and validity of reports;
- Providing initial feedback to the Reporter regarding acceptance or rejection of the Report;
- Directing and coordinating the conduct of the investigation, aimed at ascertaining the facts subject to the Report, using available tools and techniques compliant with applicable regulations;
- Ordering the closure of investigations and providing feedback to the Reporter on the outcome of the report;
- Activating and supporting management and corporate departments in implementing corrective/mitigation measures and in the possible imposition of disciplinary sanctions. The involvement of Committee members will be evaluated based on the scope of the report and related competencies, consistent with the minimization principle.

6.2.2. Investigators

Each investigator must sign a commitment declaration to maintain confidentiality of the reporter's identity and information related to the report, where not already provided for by any applicable professional ethics standards (*Annex D-Investigator's Commitment Declaration*).

Other investigating subjects could be identified and designated for specific reports, based on possession of particular competencies or based on specific needs in managing the report. Also in this case, each investigator must sign the above-mentioned commitment declaration.

6.3. Forms and Characteristics of the Report

The internal report must be addressed exclusively to the Receiving Subject (Reporting Committee) and may be made, preferably, in **written form**, using the IT methods described in detail in Annex F-Guidelines for sending internal reports through the Platform.

Digital360 S.p.A.
Viale Bodio 37, 20158 – Milano
C.F. e P.IVA: 08053820968
REA: MI – 2000431

Camera di Commercio Milano
Monza Brianza Lodi
Capitale Sociale Versato:
€2.055.034,60
PEC: digital360@pec.it

After entering the report, the Platform will generate an alphanumeric code and the related key.

It is therefore recommended that the Reporter periodically check the platform, as communications and requests for document integration from the Receiving Subject, deemed necessary to proceed, will be communicated through the same.

It is to be clarified that, in case of loss of the code and related key, the Reporter cannot access the report. The code and key, in fact, cannot be replicated. It is therefore reminded that it is the reporter's responsibility to take adequate care of them. In case of loss, it becomes the reporter's responsibility to inform the Receiving Subject of such situation, communicating any useful information regarding the report for which they have lost the code or key.

If it is not possible to proceed with the report in written form, the internal report may also be made **orally**. The oral report can be made through a voice messaging system made available within the Platform, which will allow recording the report, with the explicit consent of the reporting person.

Finally, upon request of the Reporter, the report may be made orally, through a direct meeting scheduled within a reasonable timeframe at the premises identified by the Company. In this case, an internal subject of the Reporting Committee will guide the Reporter in completing the report in the Platform, for adequate management of the same. Alternatively, with the Reporter's consent, documentation of the report will be guaranteed through recording suitable for storage and listening or through minutes. If minutes of the meeting are drafted, the Reporter can verify, correct and confirm them by signing before their insertion in the Platform.

In any case, whoever provides support to the Reporter CANNOT retain the alphanumeric code and related key of the report generated by the Platform, which will remain in the exclusive availability of the Reporter.

***

It is reminded that the Internal Report must concern one of the relevant objective areas as reported in *Annex B-Reports relevant for the procedure purposes of this Procedure*.

The Report must be complete and exhaustive to allow verification of its validity by the Reporting Committee. The Reporter, therefore, especially if they wish to maintain their anonymity, is required to provide all available and useful elements to enable the Reporting Committee and investigators to proceed with due and appropriate verifications and investigations to confirm the validity of the facts subject to the Report, such as, by way of example:

- the circumstances of time and place in which the facts subject to the report were committed;
- a clear and complete description of the facts subject to the report;

Digital360 S.p.A.
Viale Bodio 37, 20158 – Milano
C.F. e P.IVA: 08053820968
REA: MI – 2000431

Camera di Commercio Milano
Monza Brianza Lodi
Capitale Sociale Versato:
€2.055.034,60
PEC: digital360@pec.it

- the personal details or other elements that allow identifying the subject(s) who carried out the reported facts (e.g., qualification, service location where they carry out the activity);
- any other information that may provide useful confirmation about the existence of the reported facts;
- indication of any other subjects who may report on the facts subject to the report;
- any documents supporting the report.

The requirements described above do not necessarily have to be met simultaneously, considering that the Reporter may not be in full possession of all the required information at the time of sending the report, but they must be reconstructable in the investigative phase.

Personal reasons or the psychological status of the Reporter are not relevant for the purposes of taking charge of the Report.

Should the report be presented to a subject other than the Reporting Committee as identified and authorized by the Company (for example, to their Manager or hierarchical superior) where the reporter expressly declares wanting to benefit from whistleblowing protections or such intention is inferable from the report, the report is considered a "whistleblowing report" and must be transmitted, within seven days of its receipt, to the Reporting Committee, giving simultaneous notice of the transmission to the reporting person.

Otherwise, if the reporter does not expressly declare wanting to benefit from protection, or said intention is not inferable from the report, said report is considered an ordinary report.

6.4. Phases and activities

6.4.1 Pre-evaluation

The **Reporting Committee** is responsible for the Pre-evaluation phase of the report and carries out the following activities:

- It issues acknowledgment of **receipt of the report** to the Reporter **within 7 days** of reception;
  • It **maintains dialogue with the Reporter**, who may be asked, if necessary, for additions to the report;
  • It **diligently follows up on received reports**, promptly initiating preliminary analysis of the Report in order to verify its compliance with applicable regulations and this Procedure, particularly evaluating the admissibility and validity of the complaint.

The Pre-evaluation phase may alternatively conclude:

- With the archiving of the report, in case it does not fall within the objective scope of this Procedure and conditions for procedural viability are lacking *(see Annex B-Reports relevant for the procedure purposes*).

Digital360 S.p.A.
Viale Bodio 37, 20158 – Milano
C.F. e P.IVA: 08053820968
REA: MI – 2000431

Camera di Commercio Milano
Monza Brianza Lodi
Capitale Sociale Versato:
€2.055.034,60
PEC: digital360@pec.it

- With the opening of the INVESTIGATIVE PHASE, aimed at undertaking every most appropriate action to evaluate the existence of the reported facts.

6.4.2 Investigation

The **Reporting Committee** is responsible for the investigative phase, in which it is supported by the **Investigators** competent from time to time based on the subject of the report (as identified in the previous paragraph 6.2.3, or investigators identified ex novo among subjects, internal or external[2], competent with respect to the specific report).

In the case of external investigators, where following up on the report requires sharing information related to the report suitable for revealing the Reporter's identity, the Reporting Committee, before proceeding to share such information, will collect consent from the Reporter for disclosure of their identity according to the methods indicated in the following par. 8.1 (Right to Confidentiality).

If the report concerns a violation of Legislative Decree 231/2001 or the Organization, Management and Control Model (where adopted by the reference Company), the members of the Supervisory Body are promptly informed, as Investigating Subjects.

The investigative phase represents the set of activities aimed at verifying the content of reports and acquiring elements useful for the subsequent evaluation phase, in which maximum confidentiality must be guaranteed regarding the Reporter's identity and the subject of the report. This phase has the main purpose of verifying the truthfulness of the information under investigation and formalizing the ascertained facts, through internal verification activities using objective investigative techniques and support from competent corporate structures involved with respect to the Report content.

Where hearings of the Reporter (or other interested subjects, witnesses or experts) are necessary, the information collected and/or documents delivered must be archived and stored exclusively in the Platform for traceability of operations performed.

6.4.3 Investigation Results Evaluation

The internal investigative phase must conclude with a judgment regarding the admissibility of the report; alternatively:

- With the archiving of the report - inadmissible that proves to be unfounded or where it was not possible to ascertain the facts or for other reasons;
- With communication to corporate referents of the Company involved of the outcome of the internal investigation, through transmission of a summary Report of actions taken and

[2] It is possible that external parties to the Company may be involved in this phase (e.g., experts, consultants, or personnel from other Group Companies).

Digital360 S.p.A.
Viale Bodio 37, 20158 – Milano
C.F. e P.IVA: 08053820968
REA: MI – 2000431

Camera di Commercio Milano
Monza Brianza Lodi
Capitale Sociale Versato:
€2.055.034,60
PEC: digital360@pec.it

information acquired, in case the report proves to be founded and the facts reported therein are ascertained. This Report will acknowledge:

- evidence collected.
- information acquired.
- ascertained facts.
- actions undertaken for the investigation.
- any mitigation and/or corrective actions.

Following transmission of the Report, mitigation and/or corrective actions may be defined and undertaken by the Company involved, in addition to those aimed at imposing, if appropriate, disciplinary sanctions in line with applicable regulations, reference collective labor agreements and applicable procedures to protect the Company's interests (e.g., disciplinary measures, legal actions, termination of existing relationships).

6.4.4 Feedback to the Reporter

Throughout the investigative phase, the Reporting Committee will continue to maintain relationships with the Reporter, informing them of the progress of the investigation, at least regarding the main decision points.

To ensure maximum transparency in managing the report, the Whistleblower can always access the Platform and know the processing status of the report, using **the alphanumeric code and key generated by the Platform at the end of entering the report**.

Within three months from the date of the acknowledgment of receipt, the Reporting Committee must provide feedback to the Reporter, informing them of the follow-up given or intended to be given to the report. In any case, once the investigation is completed, the Reporting Committee will communicate to the Reporter the outcome of the reporting procedure, which will allow closing the report in the Platform, for proper preservation of documentation.

7. External Reports

When provided for by the regulations of the states where the Companies of the Digital360 Group are based and when specific conditions occur, the Reporter may make a report through an external channel. For the specific discipline applicable in each State, reference is made to *Annex E-External Reports of this procedure*.

Digital360 S.p.A.
Viale Bodio 37, 20158 – Milano
C.F. e P.IVA: 08053820968
REA: MI – 2000431

Camera di Commercio Milano
Monza Brianza Lodi
Capitale Sociale Versato:
€2.055.034,60
PEC: digital360@pec.it

8. Guarantees and Protective Measures for the Reporter

The entire process of receiving and managing Reports must guarantee the Reporter's rights. For this purpose, in compliance with applicable regulations, the Digital360 Group has not only provided for the possibility of sending anonymous Reports, but has also provided guarantees and measures for protecting the Reporter, which will be applied when the following conditions occur:

- The violation falls within the objective scope of application of the regulations (details of which are provided below and in Annex B-Reports relevant for the procedure purposes).
- The violation concerns behaviors, acts or omissions suitable for harming or prejudicing the public interest or the integrity of the Company.
- There are founded reasons[3] that lead the reporting person to reasonably believe in the existence of unlawful conduct or a violation.

If it is not possible to verify such requirements, the report will be archived and the Reporting Person will be informed.
The protection measures set forth in this Procedure are not guaranteed when, in relation to the report:

- The criminal liability of the Reporting Person is established, including by a non-final first-instance judgment, for crimes of defamation or slander.
- The civil liability of the Reporting Person is established for having reported false information intentionally with malice or gross negligence.

8.1. Right to Privacy

The identity of the Reporting Person and any other information from which such identity can be inferred, directly or indirectly, cannot be disclosed**, without the express consent of the same Reporting Person**, to persons other than those competent to receive or follow up on reports, expressly authorized to process such data pursuant to articles 29 and 32, paragraph 4, of regulation (EU) 2016/679 and national legislation on the protection of personal data.

It is recalled that the protection of the **confidentiality of the Reporting Person** is also ensured in jurisdictional and disciplinary proceedings.

The disclosure of the identity of the Reporting Person and any other information or element of the report whose revelation could lead to directly or indirectly deducing the identity of the reporting person is permitted only when this represents a necessary and proportionate obligation imposed by

[3] See Art. 16 of Legislative Decree 24/2023. On the same topic, see Recital 32 of the Directive, which specifies that "This requirement is an essential safeguard against malicious and frivolous or unfounded reports, so as to ensure that persons who, at the time of reporting, have deliberately and knowingly provided false or misleading information, are excluded from protection. At the same time, this requirement ensures that the reporting person continues to benefit from protection where they have made an inaccurate report in good faith. (...). The reasons that induced reporting persons to make the report should be irrelevant for the purpose of deciding on the granting of protection."

Digital360 S.p.A.
Viale Bodio 37, 20158 – Milano
C.F. e P.IVA: 08053820968
REA: MI – 2000431

Camera di Commercio Milano
Monza Brianza Lodi
Capitale Sociale Versato:
€2.055.034,60
PEC: digital360@pec.it

applicable law in the reference Country, in the context of investigations by national authorities or judicial proceedings, including for the purpose of safeguarding the right of defense of the person involved.

In derogation of the confidentiality obligation, Italian legislation also provides that the identity of the reporting person may be revealed only in the following cases:

- in the context of a disciplinary proceeding, when the accusation is based, in whole or in part, on the report and knowledge of the identity of the reporting person is indispensable for the defense of the accused[4].
- in the context of proceedings instituted following internal or external reports, where such revelation is also indispensable for the defense of the person involved[5].

In any case, even where current legislation allows the possibility of revealing the identity of the Reporting Person, **before disclosing such information, it is necessary to obtain their express consent and communicate to them in writing the reasons underlying the necessity of disclosing their identity.**

The Company is also required to protect the identity of the **people involved and the persons mentioned** in the report until the conclusion of proceedings initiated as a result of the report in compliance with the same guarantees provided in favor of the Reporting Person.

8.2. Prohibition of Retaliation

The Model for the management of reports of violations or unlawful conduct defined by the Digital360 Group also imposes an explicit prohibition on adopting any form of retaliation against the Reporting Person and other protected subjects.

Any behavior, act or omission, even if only attempted or threatened, carried out by reason of the report, which causes or may cause the reporting person, directly or indirectly, unjust harm is considered retaliation.

The following are some cases that constitute retaliation:

- dismissal, suspension or equivalent measures.
- demotion or failure to promote.
- change of functions, change of workplace, salary reduction, modification of working hours.
- suspension of training or any restriction of access to it.
- negative merit notes or negative references.
- adoption of disciplinary measures or other sanctions, including monetary ones.
- coercion, intimidation, harassment or ostracism.
- discrimination or otherwise unfavorable treatment.

[4] See Art. 12 paragraph 5, second sentence, Legislative Decree 24/2023

[5] See Art. 12 paragraph 6, Legislative Decree 24/2023.

Digital360 S.p.A.
Viale Bodio 37, 20158 – Milano
C.F. e P.IVA: 08053820968
REA: MI – 2000431

Camera di Commercio Milano
Monza Brianza Lodi
Capitale Sociale Versato:
€2.055.034,60
PEC: digital360@pec.it

- failure to convert a fixed-term employment contract into a permanent employment contract, where the worker had a legitimate expectation of such a conversion.
- non-renewal or early termination of a fixed-term employment contract.
- damage, including to the person's reputation, particularly on social media, or economic or financial prejudice, including loss of economic opportunities and loss of income.
- inclusion in improper lists based on a formal or informal sectoral or industrial agreement, which may result in the person's inability to find employment in the sector or industry in the future.
- early termination or cancellation of a contract for the supply of goods or services.
- cancellation of a license or permit.
- request for psychiatric or medical examinations.

To enjoy protection:

a) The Reporting Person must reasonably believe, considering the circumstances of the specific case and the data available at the time of reporting, that the information about the reported violations is truthful. Simple assumptions or corridor rumors are not sufficient, nor are matters of public knowledge.
b) The subject has reported facts even without being certain of their actual occurrence or reporting even inaccurate facts due to a genuine error or in any case when dealing with founded suspicions.
c) The report must fall within the objective scope and must be based on what is provided by current legislation.
d) There must be a close connection between the report and the unfavorable behavior/harm/omission suffered - directly or indirectly - by the reporting person. This discipline does not apply, by definition, to anonymous reports as it is designed to protect the reporting person from risks of retaliation. However, it may apply when, following an anonymous report, the name of the informant is revealed, who may request to avail themselves of the protection provided by the decree.

8.3. Personal Data Processing

Within the framework of report management, the Group Companies process the personal data of Reporting Persons and possibly other categories of interested subjects indicated by them in the Reports as joint controllers pursuant to art. 26 Regulation (EU) 2016/679 (hereinafter, "**GDPR**"), in compliance with privacy legislation, including the GDPR, and in accordance with the information notice pursuant to arts. 13 and 14 of the GDPR attached to this procedure.

Compliance with the principle of "storage limitation"

Reports and all related documentation are stored according to the terms established pursuant to applicable legislation and indicated in the attached privacy notice.

Digital360 S.p.A.
Viale Bodio 37, 20158 – Milano
C.F. e P.IVA: 08053820968
REA: MI – 2000431

Camera di Commercio Milano
Monza Brianza Lodi
Capitale Sociale Versato:
€2.055.034,60
PEC: digital360@pec.it

Rights recognized to data subjects

The person involved, the Reporting Person and all interested subjects may exercise the rights provided by the GDPR, in compliance with current legislation. It is understood that such rights cannot be exercised when their exercise could result in actual and concrete prejudice to the confidentiality of the reporting person's identity.

Additional obligations

Companies as joint controllers are required to:

- register the processing of personal data in the register of processing activities pursuant to art. 30 of the GDPR.
- perform an impact assessment (DPIA) pursuant to art. 35 GDPR, regarding the processing of report management.
- authorize the processing by the members of the Reporting Committee as well as the personnel, members of the Supervisory Body involved in report management, pursuant to art. 29 GDPR.
- designate suppliers involved in the report management process who process personal data on behalf of the Companies as data processors, pursuant to art. 28 GDPR.

9. Sanctions

Failure to comply with this Procedure and the protection measures provided therein entails the possibility of application, by the Digital360 Group, of its internal disciplinary system, in line with what is provided by applicable national employment legislation and relevant collective labor agreements.

The Company reserves the right to undertake any initiatives, including in judicial proceedings, in full compliance with current and applicable regulatory provisions. This Procedure leaves unaffected the criminal, civil and disciplinary liability of the Reporting Person in the case of slanderous, defamatory reports or in cases of malice and gross negligence.

It is noted that the Company or the person who reveals or disseminates information about violations covered by the obligation of secrecy[6], or relating to the protection of copyright or the protection of personal data, or reveals or disseminates information about violations that offend the reputation of the person involved, is not punishable when both of the following conditions exist:

– At the time of revelation or dissemination there are founded reasons to believe that the information is necessary to discover the violation.
– The report was made in compliance with the conditions provided by current legislation to benefit from protections (founded reason to believe that the information about violations was true and fell among the violations reportable under the law; internal and external reports made in compliance with the methods and conditions dictated by law).

[6] The reference excludes the dissemination of classified information, or information covered by professional or medical confidentiality, or concerning the deliberations of judicial bodies, for which the application of applicable legal provisions remains firm.

Digital360 S.p.A.
Viale Bodio 37, 20158 – Milano
C.F. e P.IVA: 08053820968
REA: MI – 2000431

Camera di Commercio Milano
Monza Brianza Lodi
Capitale Sociale Versato:
€2.055.034,60
PEC: digital360@pec.it

In addition to internal sanctions to the entity, where provided by current regulations, the national Authorities of the States where the Digital360 Group Companies are based may also apply to natural or legal persons any administrative monetary sanctions, as provided by current legislation.

Digital360 S.p.A.
Viale Bodio 37, 20158 – Milano
C.F. e P.IVA: 08053820968
REA: MI – 2000431

Camera di Commercio Milano
Monza Brianza Lodi
Capitale Sociale Versato:
€2.055.034,60
PEC: digital360@pec.it

ANNEX A - Companies within the scope of this Procedure

Legal Entity	Paese
Accompany S.r.l.	**Italy**
CryptoNet Labs S.r.l.	**Italy**
D360 Holding S.p.A.	**Italy**
Del Monte & Partners Comunicazione S.r.l.	**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 S.r.l.	**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**

List updated as of April 16, 2025

Digital360 S.p.A.
Viale Bodio 37, 20158 – Milano
C.F. e P.IVA: 08053820968
REA: MI – 2000431

Camera di Commercio Milano
Monza Brianza Lodi
Capitale Sociale Versato:
€2.055.034,60
PEC: digital360@pec.it

ANNEX B – Relevant reports for the procedure's purposes

Italy Section

The Digital360 Group considers relevant reports, for the purposes of applying this Procedure, exhaustively, behaviors, acts or omissions **that harm the public interest or the integrity of the entity** of which one has become aware in the work context, and which consist of:

A. violations of national and European provisions consisting of offenses regarding the following sectors[7]:

i. public procurement.
ii. financial services, products and markets and 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 protection of personal data and security of networks and information systems.

B. violations of European provisions consisting of:

xi. acts or omissions that harm the financial interests of the Union.
xii. acts and omissions concerning the internal market[8].
xiii. acts and behaviors that undermine the object or purpose of the provisions of Union acts in the sectors mentioned above.

C. violations of national provisions consisting of:

xiv. administrative, accounting, civil or criminal offenses.
xv. unlawful conduct relevant under Legislative Decree 231/2001.

D. violations of provisions internal to the individual Company, such as:

xvi. Organization, Management and Control Model adopted pursuant to Legislative Decree 231/2001;
xvii. Digital360 Group Code of Ethics;
xviii. Digital360 Group Corruption Prevention Policy;
xix. Policies relating to Diversity, Inclusion and Gender Equality
xx. National collective agreements and, more generally, internal regulations (procedures, policies, operating instructions, etc.).

[7] These are all those offenses that fall within the scope of application of European Union or national acts indicated in the acts listed in the annex to Legislative Decree 24/2023 or national acts that constitute implementation of European Union acts indicated in the annex to Directive (EU) 2019/1937.

[8] This scope includes violations of Union rules on competition and State aid, as well as violations concerning the internal market connected to acts that violate rules on corporate taxation or mechanisms whose purpose is to obtain a tax advantage that defeats the object or purpose of the applicable legislation on corporate taxation.

Digital360 S.p.A.
Viale Bodio 37, 20158 – Milano
C.F. e P.IVA: 08053820968
REA: MI – 2000431

Camera di Commercio Milano
Monza Brianza Lodi
Capitale Sociale Versato:
€2.055.034,60
PEC: digital360@pec.it

Exclusions from the objective scope

Limitations of the application scope of the objective scope of reports are provided. Information on reportable violations does not include **news that is manifestly unfounded, information that is already totally in the public domain, as well as information acquired only on the basis of indiscretions or rumors that are scarcely reliable** (so-called corridor talk).

To this it should be added that reports based on unfounded suspicions or rumors relating to personal facts not constituting an offense are excluded from the scope of this Procedure. This is because it is necessary both to take into account the interest of third parties who are the subject of the information reported in the report, and to avoid the Company carrying out internal inspection activities that risk being of little use and in any case expensive.

The scope of application of this Procedure does NOT include:

a) disputes, claims or requests linked to an interest of a personal nature, which relate exclusively to one's individual employment relationships, or relating to one's employment relationships with hierarchically superior figures.
b) reports of violations that are already mandatorily regulated by European Union or national acts concerning financial services, products and markets and prevention of money laundering and terrorist financing, transport safety and environmental protection or by national acts that constitute implementation of European Union acts in the same areas (details of the regulations are contained in the annex to Legislative Decree 24/2023, Part II);
c) reports of violations in matters of national security, as well as procurement relating to defense or national security aspects, unless such aspects fall within the relevant derivative law of the European Union.

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

d) classified information.
e) legal and medical professional secrecy.
f) secrecy of deliberations of judicial bodies.
g) criminal procedure matters.

Digital360 S.p.A.
Viale Bodio 37, 20158 – Milano
C.F. e P.IVA: 08053820968
REA: MI – 2000431

Camera di Commercio Milano
Monza Brianza Lodi
Capitale Sociale Versato:
€2.055.034,60
PEC: digital360@pec.it

Spain Section

The Digital360 Group considers relevant reports, for the purposes of applying this Procedure, exhaustively, behaviors, acts or omissions that **harm the public interest** or the **integrity of the entity** of which one has become aware in the work context, and which consist of:

E. violations of national and European provisions consisting of offenses regarding the following sectors [9]:

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

F. violations of European provisions consisting of:

xxxi. acts or omissions that harm the financial interests of the Union.
xxxii. acts and omissions concerning the internal market[10].
xxxiii. acts and behaviors that undermine the object or purpose of the provisions of Union acts in the sectors mentioned above.

G. violations of national provisions consisting of:

xxxiv. administrative, accounting, civil or criminal offenses.
xxxv. administrative offenses that cause economic damage to the treasury and to Social Security.

H. violations of provisions internal to the individual Company, such as:

xxxvi. Digital360 Group Code of Ethics;
xxxvii. Digital360 Group Corruption Prevention Policy;
xxxviii. Policies relating to Diversity, Inclusion and Gender Equality
xxxix. National collective agreements and, more generally, internal regulations (procedures, policies, operating instructions, etc.).

[9] These are all those offenses that fall within the scope of application of European Union or national acts indicated in national acts that constitute implementation of European Union acts indicated in the annex to Directive (EU) 2019/1937.

[10] This scope includes violations of Union rules on competition and State aid, as well as violations concerning the internal market connected to acts that violate rules on corporate taxation or mechanisms whose purpose is to obtain a tax advantage that defeats the object or purpose of the applicable legislation on corporate taxation.

Digital360 S.p.A.
Viale Bodio 37, 20158 – Milano
C.F. e P.IVA: 08053820968
REA: MI – 2000431

Camera di Commercio Milano
Monza Brianza Lodi
Capitale Sociale Versato:
€2.055.034,60
PEC: digital360@pec.it

Exclusions from the objective scope

Sono previste limitazioni del perimetro applicativo dell'ambito oggettivo delle segnalazioni.

Limitations of the application scope of the objective scope of reports are provided. Information on reportable violations does not include **news that is manifestly unfounded, information that is already totally in the public domain, as well as information acquired only on the basis of indiscretions or rumors that are scarcely reliable** (so-called corridor talk).

To this it should be added that reports based on unfounded suspicions or rumors relating to personal facts not constituting an offense are excluded from the scope of this Procedure. This is because it is necessary both to take into account the interest of third parties who are the subject of the information reported in the report, and to avoid the Company carrying out internal inspection activities that risk being of little use and in any case expensive.

The scope of application of this Procedure does NOT include:

a) disputes, claims or requests linked to an interest of a personal nature, which relate exclusively to one's individual employment relationships, or relating to one's employment relationships with hierarchically superior figures.
b) reports of violations that are already mandatorily regulated by European Union or national acts concerning financial services, products and markets and prevention of money laundering and terrorist financing, transport safety and environmental protection or by national acts that constitute implementation of European Union acts in the same areas.
c) reports of violations in matters of national security, as well as procurement relating to defense or national security aspects, unless such aspects fall within the relevant derivative law of the European Union.

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

d) classified information.
e) legal and medical professional secrecy.
f) secrecy of deliberations of judicial bodies.

Digital360 S.p.A.
Viale Bodio 37, 20158 – Milano
C.F. e P.IVA: 08053820968
REA: MI – 2000431

Camera di Commercio Milano
Monza Brianza Lodi
Capitale Sociale Versato:
€2.055.034,60
PEC: digital360@pec.it

ANNEX C – Reference Regulations

Area	Regulations
European Union	**Directive 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
	EU Regulation 679/2016 on privacy and subsequent provisions (GDPR) and national privacy regulations
Italy	**Legislative Decree 10 March 2023, n.24** containing "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 n.231/2001 containing "Regulation of the administrative liability of legal persons, companies and associations even without legal personality, pursuant to article 11 of law 29 September 2000, n.300"
	Organizational Model: Organization, Management and Control Model adopted pursuant to Legislative Decree 231/2001, aimed at preventing the commission of particular types of crimes in the business sphere.
Spain	**Law 2/2023** regulating the protection of persons who report regulatory violations and the fight against corruption.

Digital360 S.p.A.
Viale Bodio 37, 20158 – Milano
C.F. e P.IVA: 08053820968
REA: MI – 2000431

Camera di Commercio Milano
Monza Brianza Lodi
Capitale Sociale Versato:
€2.055.034,60
PEC: digital360@pec.it

ANNEX D – Commitment declaration of the investigator

The undersigned, (name/surname) _____ (hereinafter: "**Person informed of the report**"), under his/her exclusive responsibility

DECLARES

A. to have been made aware of the existence of a report concerning information on unlawful conduct (report id code: _____) for the purpose of carrying out specific investigation acts.
B. to have been informed and to undertake to maintain the confidentiality obligation to which the undersigned is bound in carrying out the mandate, both regarding the identity of the reporting person and of any other subject involved, as well as the facts that are the subject of the report;
C. to have been informed and to undertake to guarantee the prohibition of carrying out retaliatory acts against the reporting subject or any other subject who has even just facilitated the report, or who is connected to the Reporter by an employment relationship or by an affective/kinship relationship.
D. to be aware of having assumed the role of Person informed of the report and that, as such, the violation of the obligation of confidentiality and retaliation constitute grounds for the application of sanctions both by the Company and, where provided, by the national Authorities of the States where the Digital360 Group Companies are based, as reported in the Procedure adopted by the Company for the management of unlawful conduct reports (paragraph 9 "Sanctions").
E. to have read, know and accept the content of the Procedure adopted by the Company for the management of unlawful conduct reports (*Procedure for the management of Whistleblowing reports*).

(*place*), (*date*)

(signature)

_____

Digital360 S.p.A.
Viale Bodio 37, 20158 – Milano
C.F. e P.IVA: 08053820968
REA: MI – 2000431

Camera di Commercio Milano
Monza Brianza Lodi
Capitale Sociale Versato:
€2.055.034,60
PEC: digital360@pec.it

APPENDIX E – External reports

Italy section

Italian legislation provides for the possibility of making external reports to the Digital360 Group. **The external report can be made when one of the following conditions occurs**:

- the internal channel, although mandatory, is not active or is not compliant with what is prescribed by law.
- the Reporter has already made an internal report and it has not been followed up.
- the Reporter has well-founded reasons to believe that the Organization would not effectively follow up on the internal report or sees a concrete risk of retaliation in case of internal report
- the reporting person has well-founded reason to believe that the violation may constitute an imminent or manifest danger to the public interest.

It is noted that reports of unlawful conduct relevant under Legislative Decree 231/2001 or violations of the Organization, Management and Control Model adopted by the Company cannot be the subject of external reports. Information on such violations can only be shared through the internal channel referred to in the previous chapter 6.

The use of external reporting is, therefore, residual, compared to internal reporting and can be made only where the violation that is intended to be reported is included *in Appendix B-Reports relevant for the purposes of the procedure*, Italy Section under letters A) and B).

It is the reporting person's responsibility to evaluate the occurrence of one of the situations listed above before proceeding to make an external report.

External reports are made by the Reporter directly to ANAC, through specially prepared channels. These are:

- IT platform, which can be accessed through the ANAC services portal at the following url: https://whistleblowing.anticorruzione.it/#/
- Oral reports
- Direct meetings scheduled within a reasonable time

Furthermore, should the Reporter who believes to have suffered retaliation has the right to transmit the communication to the National Anti-Corruption Authority (ANAC), competent for the investigations that the law attributes to the Authority, through the IT platform form available on the ANAC institutional website. It is important, therefore, that those who have suffered retaliation do not transmit the communication to subjects other than ANAC in order not to nullify the protections that the legislation guarantees, first of all, confidentiality.

On the ANAC institutional website, by clicking the link to the dedicated page, one accesses the service dedicated to "*whistleblowing*" (**https://whistleblowing.anticorruzione.it/#/**), where clear and easily accessible indications are found relating to the channel, to the competent subjects to whom the management of reports is entrusted, as well as to the procedures.

Digital360 S.p.A.
Viale Bodio 37, 20158 – Milano
C.F. e P.IVA: 08053820968
REA: MI – 2000431

Camera di Commercio Milano
Monza Brianza Lodi
Capitale Sociale Versato:
€2.055.034,60
PEC: digital360@pec.it

Spain section

Spanish legislation provides for the possibility of making external reports to the Digital360 Group. External reports are made by the reporter directly to the Autoridad Independiente de Protección del Informante (A.A.I.) and to the competent bodies of the autonomous communities through specifically designated channels.

Digital360 S.p.A.
Viale Bodio 37, 20158 – Milano
C.F. e P.IVA: 08053820968
REA: MI – 2000431

Camera di Commercio Milano
Monza Brianza Lodi
Capitale Sociale Versato:
€2.055.034,60
PEC: digital360@pec.it

ANNEX F - Guidelines for sending internal reports through the platform

The Guidelines can be consulted through the company intranet "*Digital360Workspace*" or other IT bulletin board shared with personnel and in the *Legal&Compliance* section https://www.digital360.it/legal-compliance/ for all interested parties.

Digital360 S.p.A.
Viale Bodio 37, 20158 – Milano
C.F. e P.IVA: 08053820968
REA: MI – 2000431

Camera di Commercio Milano
Monza Brianza Lodi
Capitale Sociale Versato:
€2.055.034,60
PEC: digital360@pec.it