EQUITER SGR

WHISTLEBLOWING POLICY

Drafting	Chief Executive Officer / Appointed Consultant
Review	Chief Executive Officer; Head of the Compliance Function
Date of approval	Board of Directors of 29/06/2022
Revision	Rev. 01 of 26/02/2025

TABLE OF CONTENTS

1. INTRODUCTION

Equiter SGR S.p.A. (hereinafter also the "SGR" or the "Company") is constantly committed to conducting its activity with honesty and integrity. However, it must be recognised that every company is subject to the risk of improper actions or unlawful conduct.

It is therefore the SGR's duty to adopt measures suitable for identifying such situations in order to remedy them. By encouraging an open and responsible culture at company level, it is also possible to help prevent such situations.

All the Company's staff are required to observe the procedures and policies adopted by the SGR and to report any conduct that fails to comply with the fundamental principles contained therein.

Every individual has the responsibility to raise any concerns about possible unlawful conduct within the work context.

2. THE REFERENCE REGULATORY FRAMEWORK

Within the framework of the provisions governing the activity carried out by intermediaries, following the entry into force of Legislative Decree No. 129 of 3 August 2017, Article 4-*undecies* "Internal systems for reporting breaches" and Article 4-*duodecies* "Procedure for reporting to the Supervisory Authorities" were introduced into Legislative Decree No. 58 of 24 February 1998 (Consolidated Law on Finance, hereinafter also "TUF"). These extended the scope of application of internal reports to the SGR (so-called whistleblowing), by staff, to acts or facts that may constitute breaches of the rules governing the activity carried out, as well as of Regulation (EU) No. 596/2017 ("Market Abuse").

The Bank of Italy and Consob adopt, according to their respective competences, the implementing provisions, having regard to the need to coordinate the supervisory functions and to minimise the burdens on the parties concerned.

In particular, with the adoption of the Provision of 5 December 2019 containing the "Bank of Italy Regulation implementing Articles 4-*undecies* and 6, paragraph 1, letters b) and c-*bis*), of the TUF" (hereinafter also the "Bank of Italy Regulation"), the Bank of Italy established that the strategic supervision bodies of SGRs must approve the internal systems for reporting breaches in accordance with Annex 4 of that Regulation.

With reference to the provisions on "Anti-Money Laundering", on 4 July 2017 Legislative Decree No. 90 of 25 May 2017 entered into force, which amended and entirely rewrote — rather than amending — the content of Legislative Decree No. 231 of 21 November 2007 (hereinafter also "Legislative Decree No. 231/2007"). Article 48 of Chapter VII ("reporting of breaches") of the new Legislative Decree No. 231/2007 provides for the introduction of a system for reporting potential or actual breaches of the provisions laid down for the prevention of money laundering and terrorist financing (so-called whistleblowing). These legal provisions aim to define the minimum requirements necessary for setting up whistleblowing systems, intended to allow staff to report acts and facts that may constitute a breach of the rules governing the fight against money laundering and terrorist financing, while at the same time guaranteeing the confidentiality and protection of the personal data of the party making the report and of the reported party.

Furthermore, Law No. 179 of 30 November 2017 (entitled "Protection of the employee or collaborator who reports unlawful acts in the private sector") intervened on Legislative Decree

No. 231/2001, inserting into Article 6 (entitled "Persons in a senior position and organisational models of the entity") a new provision that places within the organisation and management model referred to in the Decree the measures related to the submission and management of reports of unlawful conduct relevant under Legislative Decree No. 231/2001 and of breaches of the Model, as well as the related forms of protection of the reporting person.

Legislative Decree No. 24 of 10 March 2023 repealed Article 6, paragraph 2-*bis*, letter a), of Legislative Decree No. 231/2001, comprehensively regulating the discipline on whistleblowing reporting. In particular, the aforementioned Legislative Decree transposes EU Directive 2019/1937 on this point and extends the protections provided to all those who report breaches of which they become aware within their own work context — as employees or collaborators, subordinate and self-employed workers, freelance professionals and other categories such as volunteers and trainees, including unpaid ones, shareholders and persons with administrative, management, control, supervisory or representative functions. In addition, the protection measures also apply to so-called "facilitators", colleagues, relatives or stable affective relations of the person who made the report.

Under Decree 24/2023, the companies concerned (i.e. those with more than 50 employees, or that have adopted a Model 231, or that fall within the application of the rules referred to in Parts I.B and II of the Annex to Decree 24/2023) must set up internal reporting channels capable of guaranteeing the highest level of confidentiality. In companies with fewer than fifty employees, only internal reporting is permitted, excluding the possibility of resorting to the external channel and to public disclosure.

Among its binding contents, the directive — fully transposed by the implementing Decree and by the SGR's Model 231 — provides that protection is granted even in the case of reports or disclosures that subsequently prove to be unfounded, where the reporting person had reasonable grounds to believe that the breaches were true. Protection ceases, however, where the unfounded reports were made with intent (dolo) or gross negligence (colpa grave).

The possibility of external reports (via the A.N.A.C. channels) is also provided for, on condition that the internal channel has first been used and, in particular cases, public disclosure.

3. SCOPE OF APPLICATION

The purpose of this Policy is to identify suitable organisational solutions on whistleblowing, in accordance with the aforementioned legal provisions and proportionately to the SGR's size profile and operational complexity.

As reported above, the primary legislation applicable to the SGR circumscribes the objective perimeter of whistleblowing to:

- ☐ "acts or facts that may constitute a breach of the rules governing the activity carried out, as well as of Regulation (EU) No. 596/2014";
- ☐ "the provisions laid down for the prevention of money laundering and terrorist financing";
- ☐ administrative, accounting, civil or criminal offences, unlawful conduct relevant under Legislative Decree No. 231/2001, and breaches of Model 231.

In addition, the SGR considers it appropriate to include within the perimeter of whistleblowing also what is defined within the Code of Ethics and Conduct.

Apart from cases of liability for slander (calunnia) or defamation, or on the same basis pursuant to Article 2043 of the Civil Code, the submission of a report does not constitute a breach of the obligations arising from the employment relationship.

Reports may be made by all the SGR's staff, as defined in Article 1, paragraph 2, letter cc), of Legislative Decree No. 231/2007 (as well as by Article 1, paragraph 1, letter i-*ter*), of the TUF), namely "employees and those who in any case operate on the basis of relationships that entail their inclusion in the organisation of the obliged party, including in a form other than a subordinate employment relationship — including financial advisors authorised for off-premises offer referred to in Article 31, paragraph 2, of the TUF, as well as direct producers and intermediation staff referred to in Article 109, paragraph 2, letters c) and e), of the Private Insurance Code (CAP)". Furthermore, in compliance with the provisions of Legislative Decree No. 24/2023, reports may be made by: self-employed workers, freelance professionals and consultants who carry out their work activity at the company; workers or collaborators of the undertakings supplying goods or services; volunteers and trainees, whether paid or unpaid; shareholders and persons with administrative, management, control, supervisory or representative functions, even where such functions are exercised on a purely de facto basis.

Reports may be made in the following cases:

- when the legal relationship is ongoing;
- when the legal relationship has not yet begun, if the information on the breaches was acquired during the selection process or in other pre-contractual phases;
- during the probationary period;
- after the termination of the legal relationship, if the information on the breaches was acquired during the relationship itself.

The SGR is required to provide the aforementioned Policy and its subsequent updates to all employees, as well as to publish it on its website.

The Board of Directors approves the internal systems for reporting breaches.

4. APPOINTMENT OF THE HEAD OF THE INTERNAL REPORTING SYSTEMS

In accordance with Article 4, paragraph 2, of Legislative Decree No. 24/2023, the SGR designates a Head of the Internal Reporting Systems (hereinafter also "RSIS"), with the task of:

- ensuring the correct functioning of the procedures;
- examining and assessing the reports received;
- reporting directly and without delay to the Board of Statutory Auditors the information that is the subject of a report, where relevant;
- drawing up — in compliance with the personal-data-protection rules — an annual report on the correct functioning of the internal reporting system, containing aggregate information on the results of the activity carried out following the reports received. This report is submitted annually to the attention of the Board of Directors.

The Board of Directors of 26 February 2025 appointed the Supervisory Body (OdV), excluding its internal member, as the RSIS. Consistently with the legal provisions and with its own organisational and operational model — in light of the principle of proportionality — the SGR considered it appropriate to attribute to the RSIS also the activities of receiving, as well as of

examining and assessing, the reports. This examination and assessment activity may also be carried out by the RSIS with the support, if necessary, of qualified personnel, including external, in compliance with confidentiality obligations and personal-data-protection obligations.

Where the RSIS is presumed to be responsible for the breach or has a potential interest related to the report such as to compromise impartiality of judgment, the activities of receiving, examining and assessing the reports will be carried out by the holder of the "Reserve Function", identified by the Board of Directors of 9 December 2024 in the person of Mr Roberto Giribaldi, head of the Internal Audit Function.

5. CONTENT AND METHODS OF REPORTING

5.1 Internal reports of breaches

The reporting person (falling within the definition of "SGR staff" under the law and as further specified in the preceding paragraph 3) must provide, as far as possible, the elements useful for reconstructing the fact and for ascertaining the merits of what is reported. The report must contain the following elements:

- the identity of the reporting person, indicating their job classification and professional qualification, place of work and contact details;
- the place and date/period in which the fact that is the subject of the report occurred;
- a clear and complete description of the facts that are the subject of the report and that may constitute a breach as specified in the preceding paragraph 3;
- the identity or other elements enabling the identification of the party or parties who carried out the reported facts;
- any other parties who can report on the facts that are the subject of the report, and any documents that can confirm the merits of such facts;
- any other information that may provide useful corroboration of the existence of the reported facts;
- a declaration by the reporting person as to the absence or existence of a private interest connected to the report.

For the purposes of the report, the reporting person is required to use the form attached to this Policy (Annex A – Form for the internal reporting of breaches).

It is in any event indispensable that the facts be of the reporting person's direct knowledge and not reported by other parties.

The report is sent by the reporting person to the RSIS by one of the following methods:

- by sending it to the dedicated certified email (PEC) address: segnalazioni@equitersgr.it attributable to the party responsible for receiving the report; where that party is the presumed person responsible for the breach or has a potential interest related to the report such as to compromise impartiality of judgment, via the email address rgiribaldi@regulatoryconsulting.it referring to the "Reserve Function" as identified above;
- by ordinary post to the address: Piazza San Carlo 156, Turin, for the attention of the "Head of the Internal Reporting Systems"; where that party is the presumed person responsible for the breach or has a potential interest connected to the report such as to compromise

impartiality of judgment, to the same address indicated above but for the attention of the "Reserve Function" as identified above. In order to guarantee the confidentiality of the reporting person, the report must be placed in three sealed envelopes: the first containing the form with the reporting person's identifying data; the second containing the form with the report, so as to separate the identifying data from the report; both envelopes must then be placed in a third sealed envelope bearing on the outside the wording "Confidential – To the Head of the Internal Reporting Systems" or, in the cases indicated above, "Confidential – For the attention of the Reserve Function".

In any event, the confidentiality of the personal data of the reporting person and of the presumed person responsible for the breach must be guaranteed, without prejudice to the rules governing investigations or proceedings initiated by the judicial authority in relation to the facts that are the subject of the report. In order to protect the confidentiality of the reporting person and the very purpose of the investigation, the information on their identity may be withheld even from the exercise of the rights provided for by the personal-data-protection legislation (in particular Articles 15–22 of the European Regulation 2016/679 – GDPR) for all phases of the procedure, save with their consent or where knowledge is indispensable for the defence of the reported party. In any event, even where the identity of the reporting person should be revealed — for example because it is essential for the defence of the reported party — adequate protection of the reporting person against retaliatory, discriminatory or otherwise unfair conduct following the report must always be guaranteed, in accordance with Legislative Decree No. 24/2023.

5.2 Reports to the Supervisory Authorities

Since 3 January 2018, pursuant to Article 4-*duodecies* of the TUF, the staff of the parties indicated in Article 4-*undecies* thereof may also transmit reports directly to the Supervisory Authorities in accordance with operating rules defined by them.

In this regard, the Bank of Italy and Consob:

a) receive, each in the matters within its competence, from the staff of the parties indicated in paragraph 2 of this Policy, reports that refer to breaches of the rules of the TUF, as well as of European Union acts directly applicable in the same matters;

b) may establish conditions, limits and procedures for receiving reports, taking into account: the confidentiality of the personal data of the reporting person and of the presumed person responsible for the breach, without prejudice to the rules governing investigations or proceedings initiated by the judicial authority in relation to the facts that are the subject of the report — the identity of the reporting person is withheld from the application of Article 15, paragraph 1, letter g), of the GDPR, and may not be revealed for all phases of the procedure, save with their consent or where knowledge is indispensable for the defence of the reported party; and the adequate protection of the reporting person against retaliatory, discriminatory or otherwise unfair conduct following the report;

c) make use of the information contained in the reports, where relevant, exclusively in the exercise of supervisory functions;

d) provide, by means of a memorandum of understanding, the appropriate coordination measures in carrying out the activities within their respective competences — including the

application of the related sanctions — so as to coordinate the exercise of the supervisory functions and to minimise the burdens on the supervised parties.

The documents relating to the reports are withheld from the access provided for by Articles 22 et seq. of Law No. 241 of 7 August 1990 ("New rules on administrative procedure and on the right of access to administrative documents"), as subsequently amended.

As at the date of approval of this policy, the following may be consulted:

- on the Consob website, the dedicated section, at the following address: http://www.consob.it/web/area-pubblica/whistleblowing;
- on the Bank of Italy website, the dedicated section, at the following address: https://www.bancaditalia.it/compiti/vigilanza/whistleblowing/.

In that section, the operating methods that all the SGR's staff must follow to transmit directly to Consob or the Bank of Italy reports relating to alleged breaches or offences of the rules of the TUF, as well as of European Union acts directly applicable in the same matters, are indicated.

5.3 Reports to A.N.A.C.

Under Article 6 of Legislative Decree No. 24/2023, the reporting person may make an external report to A.N.A.C. (the National Anti-Corruption Authority) if, at the time of submission, one of the following conditions is met:

- they have already made an internal report and it has not been followed up;
- they have reasonable grounds to believe that, if they made an internal report, it would not be effectively followed up, or that the report itself could give rise to a risk of retaliation;
- they have reasonable grounds to believe that the breach may constitute an imminent or manifest danger to the public interest.

The external report is addressed to the National Anti-Corruption Authority (A.N.A.C.) via the channels it has activated (https://www.anticorruzione.it/-/whistleblowing).

External reports to the Supervisory Authorities for breaches of the rules of the TUF, as well as of Union acts directly applicable in the same matters, may be made regardless of whether the conditions listed above are met, in accordance with the methods indicated in paragraph 5.2.

External reports may be made:

- in writing, via the IT platform; or
- orally, through telephone lines or voice-messaging systems or — at the request of the reporting person — by means of a direct meeting arranged within a reasonable time.

An external report submitted to a party other than A.N.A.C. is transmitted to the latter within seven days of the date of its receipt, giving simultaneous notice of the transmission to the reporting person.

A.N.A.C. carries out the following activities:

a) provides any interested person with information on the use of the external reporting channel and the internal reporting channel, as well as on the protection measures provided for whistleblowing by Legislative Decree No. 24/2023;

b) gives notice to the reporting person of receipt of the external report within seven days of the date of its receipt, save on the reporting person's explicit request to the contrary or where it considers that the notice would prejudice the protection of the confidentiality of the reporting person's identity;

c) maintains communications with the reporting person and requests supplementary information from them, if necessary;

d) diligently follows up the report received;

e) carries out the investigation necessary to follow up the report, including through hearings and the acquisition of documents;

f) responds to the reporting person within three months or, where justified and substantiated reasons exist, six months from the date of the notice of receipt of the external report or, in the absence of such notice, from the expiry of the seven days from receipt;

g) communicates to the reporting person the final outcome, which may also consist of dismissal, transmission to the competent authorities, a recommendation or an administrative sanction.

A.N.A.C. also arranges for the transmission of reports concerning information on breaches that do not fall within its competence to the competent administrative or judicial authority — including the institutions, bodies or offices of the European Union — and gives simultaneous notice to the reporting person of the referral. The competent administrative authority carries out the activities referred to in the preceding letters c), d), e), f) and g), and guarantees — including through the use of encryption tools — the confidentiality of the identity of the reporting person, of the person involved and of the person mentioned in the report, as well as of the content of the report and the related documentation.

A.N.A.C. may decline to follow up reports concerning breaches of minor significance and proceed to dismiss them.

5.4 Public disclosure

To make a public disclosure means making information on breaches available in the public domain through the press or electronic means, or in any case through means of dissemination capable of reaching a large number of people.

The reporting person who makes a public disclosure benefits from the protection provided for by Legislative Decree No. 24/2023 if, at the time of the public disclosure, one of the following conditions is met:

- they have first made an internal and external report, or have made an external report directly, and no response has been given within the established time limits regarding the measures envisaged or adopted to follow up the reports;
- they have reasonable grounds to believe that the breach may constitute an imminent or manifest danger to the public interest;
- they have reasonable grounds to believe that the external report may entail a risk of retaliation or may not be effectively followed up, in view of the specific circumstances of

the actual case — such as those in which evidence may be concealed or destroyed, or in which there is a reasonable fear that the person who received the report may be in collusion with the perpetrator of the breach or involved in the breach itself.

6. INTERNAL REPORTING PROCEDURE

In accordance with Article 5 of Legislative Decree No. 24/2023, upon receiving the report, the RSIS (or the "Reserve Function", where the conditions are met) communicates to the reporting person, within 7 days (using the same method by which the report was received), the initiation of the examination procedure, and begins to verify whether or not the report is well-founded. The investigations following the report are carried out in compliance with the principles of minimisation and purpose limitation under the GDPR, as well as in compliance with Article 13 of Legislative Decree No. 24/2023, and may entail carrying out targeted investigations, including on the tools used to perform work duties such as, for example, computers, the internet network, mobile phones, and also through the viewing of cameras.

The reported party is informed of the start of the investigations against them (Annex B), unless such information would compromise the outcome of the investigation. It is advisable to document such assessments, for which the opinion of the Head of the Compliance Function may be requested.

Where it is considered that the reported party cannot be informed before the investigation, the latter is in any event informed at the outcome of the verification.

The notice referred to in Annex B will be given to all those who are involved in the investigation following the report.

In any event, at the outcome of that verification:

- in the case of unfoundedness, the RSIS communicates to the reporting person (using the same method by which the report was received) the reasoned outcome and the conclusion of the procedure;
- where, from the outcome of the verification, the report proves to be well-founded, the RSIS proceeds to inform (i) the reporting person of the positive outcome of the investigations, (ii) the reported party via separate communication, (iii) the Board of Statutory Auditors via dedicated communication.

During the process of analysing the report, the RSIS assesses the report in terms of its relevance and seriousness and proceeds to inform the reporting person (using the same method by which the report was received) and the reported party (via separate communication) of the results of that assessment. Where serious breaches have occurred, the RSIS promptly informs the Board of Directors and the Board of Statutory Auditors so that they may assess the possible adoption of decision-making and disciplinary measures within their respective competences.

At any stage of the procedure — and without waiting for the outcome of the assessment — the RSIS reports directly and without delay the relevant information that is the subject of the report to the Corporate Bodies, which proceed to adopt the related measures, including on an urgent basis where necessary, including, where applicable, a notice to the Head of the Anti-Money Laundering Function should the conditions exist for the preparation of a suspicious transaction report. Where

the subject of the report is the RSIS itself and the report is deemed well-founded and relevant, the prompt notice to the Corporate Bodies must be provided directly by the Reserve Function.

Where the reporting person is co-responsible for the breach that is the subject of the report, the Company may provide for privileged treatment of that person compared to the other co-responsible parties, save in cases where the reporting person's conduct is of particular seriousness.

The process described above must be concluded in the shortest possible time, according to criteria that take into account the seriousness of the breach, in order to prevent the continuation of the breaches from producing further aggravation for the SGR. In any event, the procedure must be concluded within 2 months of receipt of the report, save in exceptional and duly substantiated cases in which the examination and assessment of the report may extend to 3 months, subject to communication to the Board of Statutory Auditors.

7. FORMS OF PROTECTION OF THE REPORTING PERSON

7.1 Protection of anonymity

In order to prevent the fear of suffering prejudicial consequences from inducing a person not to report breaches, the identity of the reporting person may not be revealed, save with their express and free consent, and all those involved in managing the report are required to protect the confidentiality of that information.

An exception is made for the cases in which the reporting person may be liable for slander (calunnia) and defamation under the provisions of the Criminal Code or under Article 2043 of the Civil Code, as well as the cases in which anonymity cannot be invoked by law.

The reporting person's anonymity is also guaranteed in the context of disciplinary proceedings when the charge against the reported party is based on findings that are separate from and additional to the report. The identity of the reporting person may, however, be revealed to the reported party, with the consent of the reporting person, or when the charge is based principally on the report and therefore knowledge of the identity is absolutely indispensable for the defence of the reported party.

Breaches of the confidentiality obligation — including the disclosure of information on the basis of which the reporting person's identity may be inferred — are considered a breach of this policy and a source of disciplinary liability, without prejudice to further forms of liability provided for by the legal system.

7.2 Prohibition of discrimination

Staff who make a report under this policy may not be sanctioned, dismissed (save in cases of ascertained co-responsibility) or subjected to any discriminatory measure having effects on working conditions for reasons connected to the report (without prejudice to the provisions of the following paragraph 8). The retaliatory or discriminatory dismissal of the reporting person is null and void, and likewise null and void are the change of duties pursuant to Article 2103 of the Civil Code and any other retaliatory or discriminatory measure adopted against the reporting person. Discriminatory measures means unjustified disciplinary actions — even merely attempted or threatened — harassment in the workplace, and any other form of retaliation that causes or may

cause the reporting person, or the person who filed the complaint, directly or indirectly, unjust harm.

It is the employer's burden, in the event of disputes related to the imposition of disciplinary sanctions, demotions, dismissals, transfers or the subjection of the reporting person to another organisational measure having negative effects — direct or indirect — on working conditions, subsequent to the submission of the report, to demonstrate that such measures are based on reasons unrelated to the report itself.

The adoption of discriminatory measures against those who make reports may be denounced to the National Labour Inspectorate, for the measures within its competence, by the reporting person as well as by the trade-union organisation designated by the reporting person.

In the more serious cases, and where possible, the SGR may consider ordering the transfer of the reporting person for reasons of environmental incompatibility, subject to the latter's consent.

Staff who consider that they have suffered discrimination give detailed notice thereof to the RSIS, which — having ascertained the merits — reports the case to the competent Corporate Bodies, so that the measures necessary to restore the situation and/or remedy the negative effects of the discrimination may be adopted.

Likewise prohibited is any form of retaliation or discrimination having effects on the working conditions of those who cooperate in the activities to verify the merits of the report.

The same protection measures also apply to:

- the facilitator;
- persons in the same work context as the reporting person who are linked to them by a stable affective bond or by kinship up to the fourth degree;
- work colleagues of the reporting person who work in the same work context and who have a habitual and current relationship with that person;
- the entities owned by the reporting person or for which those persons work, as well as the entities operating in the same work context as the aforementioned persons;
- in the case of an anonymous report, if the reporting person is subsequently identified.

8. LIABILITY OF THE REPORTING PERSON

This Policy leaves unaffected the criminal and disciplinary liability of the reporting person in the event of a slanderous and defamatory report under the Criminal Code or under Article 2043 of the Civil Code.

Without prejudice to the specific limitations of liability provided for by Article 20 of Legislative Decree No. 24/2023, the following are also a source of liability, in disciplinary and other competent fora: any forms of abuse of this Policy, such as manifestly opportunistic reports and/or reports made for the sole purpose of harming the reported party and/or other parties, and any other instance of improper use or intentional instrumentalisation of the mechanism that is the subject of this Policy.

9. DATA PROTECTION AND DOCUMENT ARCHIVING

In order to ensure the reconstruction of the various phases of the reporting process, it is the RSIS's responsibility (or the Reserve Function's, for the reports received by it) to guarantee:

- the traceability of the reports and the related investigative activities;
- the preservation of the documentation relating to the reports and the related verification activities, in dedicated archives (paper/electronic);
- the retention of the documentation and the reports for a period of time no longer than that necessary for the purposes for which the data was collected or subsequently processed, and in any case in compliance with the privacy procedures in force.

The competent functions archive the documentation relating to the sanctioning and disciplinary process.

The processing of the personal data of the persons involved in and/or mentioned in the reports is protected in accordance with the legislation in force and the corporate privacy procedures.

10. UPDATING OF THE POLICY

The SGR reviews the entire content of this policy whenever a significant change occurs in the Company's operations or in the system for reporting breaches. The revision and updating of this policy is carried out by the Compliance Function and submitted for approval to the competent corporate bodies.

ANNEX A – Form for the internal reporting of breaches

Name and surname of the reporting person	
Job classification and professional qualification	
Place of work	
Contact details	
Place where the fact occurred	
Description of the facts that are the subject of the report	
Name(s) and surname(s) of the reported party/parties	
Name(s) and surname(s) of the party/parties aware of the facts that are the subject of the report (optional)	
Further information that may provide useful corroboration of the existence of the facts that are the subject of the report (optional)	
Relevant attachments (optional)	

ANNEX B – Notice for the employee subject to an internal investigation

[Date], [Place]

Subject: privacy notice for the carrying out of an internal investigation

Dear […],

In the context of an investigation relating to [brief description of the case], the Company needs to carry out checks and examine — and, where appropriate, extract a copy of — [indicate subject of the investigation].

The Company intends to carry out a comprehensive examination of the material collected in order to assess [indicate the purpose of the investigation] for the defence of its rights. The controller of the data collected through the investigation is the Company. Your data will be used only for the purposes mentioned and may be processed with or without the aid of electronic or automated means. The parties who will have sight of your data are the Company's Supervisory Body (OdV), as well as the Company's Chief Executive Officer and/or those instructed by the latter to follow any judicial proceedings that may arise from it. The provision of your data does not require your consent, as the data is collected for the purpose of protecting the Company's rights. Any refusal on your part would be unlawful, and in that case the Company would be obliged to adopt the most appropriate measures to achieve the purposes indicated, which could also give rise to consequences at the disciplinary level. The data may be shared with the Company's external consultants, exclusively for the purposes indicated above. The data and information will be retained for the time strictly necessary for conducting the checks and for any protection of the Company's right of defence, as well as for any further period during which there is a legitimate interest in retaining the information and data — including the interest in defence in judicial proceedings — after which they will be deleted or made anonymous. You have the rights provided for by Articles 15 et seq. of the GDPR. To exercise your rights, you may contact us by written communication or by email, writing to […].

We remind you that, should you consider the processing of personal data to be unlawful, you may lodge a complaint with the Data Protection Authority (Garante per la Protezione dei Dati Personali).

We thank you in advance for your cooperation and send you our kind regards.