PROCEDURE FOR REPORTING VIOLATIONS (SO-CALLED 'WHISTLEBLOWING')

13 February 2025

Unipol

PROCEDURE FOR REPORTING VIOLATIONS (SO-CALLED 'WHISTLEBLOWING')

13 February 2025

Note that this document represents an English translation of the original version "PROCEDURA PER LA SEGNALAZIONE DI VIOLAZIONI (C.D. WHISTLEBLOWING) " originally issued in Italian. The accuracy and conceptual consistency of the English version of this document may not be ensured. In case of any discrepancies or doubts in the interpretation of the document, official reference must be made to the Italian-language version.

Unipol

INDEX

1. Introduction

1.1. Document Objectives

"This procedure (the '**Procedure'**) governs the system adopted by the Group to enable the internal reporting of violations of national or European Union laws that harm the public interest or the integrity of the companies falling within the scope defined in paragraph 2.2 (the 'In-**Scope Companies'**), and of which the whistleblowers have become aware in the workplace context (so-called whistleblowing)."

The Procedure specifically defines:

- the individuals who may activate the internal system for reporting violations;
- the behaviors, acts, or omissions that may be subject to violation;
- the methods for reporting potential violations and the persons responsible for receiving the violations;
- the violations management process, including the timeline, phases of the procedure, and the parties involved;
- the methods by which the whistleblower and the reported person are informed of the progress of the procedure;
- the confidentiality safeguards and protection measures against retaliatory conduct resulting from the violation.

The Procedure also provides information on external reporting and public disclosure, as additional channels available to whistleblowers.

However, the new provisions under the Whistleblowing Decree (as defined below) establish that the choice of reporting channel is not at the whistleblower's discretion, as priority must be given to the internal channel. Only if the conditions listed therein are met may other reporting channels be used.

Unless otherwise specified, references to bodies/areas/departments/functions in the Policy refer to Unipol Assicurazioni S.p.A. ("Unipol") and, where applicable, to the equivalent bodies/areas/departments/functions of the other In-Scope Companies, even if outsourced.

1.2. Approval and revision of the Procedure

The Procedure is drafted/revised with the involvement of the relevant corporate departments to ensure a clear definition and shared understanding of objectives, roles, and responsibilities. It is approved—following notification to the trade unions referred to in Article 51 of Legislative Decree No. 81 of 2015 and after review by the Group Risk Committee—by the Board of Directors of Unipol (the "**Parent Company**"), also in the exercise of its direction and coordination activities over its subsidiaries and in accordance with the Group's corporate process for the drafting and validation of company policies.

The Boards of Directors of the In-Scope Companies, as part of their responsibilities concerning governance, internal control systems, and risk management, assess and approve the Procedure, as applicable, in accordance with the relevant sector-specific regulations and their respective business models.

Companies that have adopted the organisation, management, and control model (the "**OMM**") pursuant to Legislative Decree No. 231 of 8 June 2001 (the "**Decree 231/01**") refer to this Procedure

within the OMM itself, pursuant to Article 6, paragraph 2-bis of Decree 231/01, as amended by Legislative Decree No. 24 of 10 March 2023.

The Procedure will be reviewed and, if necessary, amended whenever required by regulatory updates, interventions by Supervisory Authorities, business strategies, or contextual changes (e.g., significant changes to business processes, major structural reorganisations, significant changes to the IT platforms used, or changes to the scope of application).

The Procedure is communicated and made available by the In-Scope Companies to all personnel and other relevant stakeholders through appropriate communication channels, as further detailed in paragraph 9.

The Head of the Compliance and Group Anti-Money Laundering Function of the Parent Company ensures the drafting and updating of the Policy to be submitted for review and approval by the competent bodies.

2. Reference Context

2.1. Internal and external regulatory reference

This Procedure has been drafted in accordance with the applicable legislation and the relevant sector supervisory guidelines set out below.

European Union legislation:

- 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;
- Regulation (EU) No 596/2014 of the European Parliament and of the Council of 16 April 2014 on market abuse (Market Abuse Regulation – MAR);
- Regulation (EU) 2017/1129 of the European Parliament and of the Council of 14 June 2017 on the prospectus to be published when securities are offered to the public or admitted to trading on a regulated market (Prospectus Regulation);
- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, repealing Directive 95/46/EC (General Data Protection Regulation – GDPR).

National legislation:

- Legislative Decree No. 24 of 10 March 2023, implementing 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 on the protection of persons who report breaches of national legislation (the “Whistleblowing Decree”);
- Legislative Decree No. 231 of 8 June 2001, governing the administrative liability of legal entities, companies, and associations, including those without legal personality, as amended by the Whistleblowing Decree;
- Legislative Decree No. 231 of 21 November 2007, implementing Directive 2005/60/EC on the prevention of the use of the financial system for the purpose of money laundering and terrorist

financing and Directive 2006/70/EC laying down implementing measures (the "Decree 231/07"), as amended by Article 2 of Legislative Decree No. 90 of 25 May 2017 (implementing the Fourth Anti-Money Laundering Directive);

- Legislative Decree No. 209 of 7 September 2005, the "Private Insurance Code" ("CAP"), as amended (i) by Article 1, paragraph 2, of Legislative Decree No. 68 of 21 May 2018 (implementing Directive (EU) 2016/97 of the European Parliament and of the Council of 20 January 2016 on insurance distribution), and (ii) by Article 1, paragraph 1, of Legislative Decree No. 187 of 30 December 2020;
- Legislative Decree No. 196 of 30 June 2003, the "Personal Data Protection Code," as subsequently amended and supplemented;
- Legislative Decree No. 58 of 24 February 1998, the "Consolidated Law on Financial Intermediation" ("TUF"), as amended (i) by Article 1, paragraph 6, of Legislative Decree No. 129 of 3 August 2017 (implementing "MiFID II"), (ii) by Article 2 of Legislative Decree No. 68 of 21 May 2018 (implementing Directive (EU) 2016/97 on insurance distribution), and (iii) by Legislative Decree No. 17 of 2 February 2021 (aligning national legislation with Regulation (EU) 2017/1129 on the prospectus to be published for public offerings or admission to trading on a regulated market);
- Bank of Italy Regulation of 5 December 2019, implementing Articles 4-undecies and 6, paragraph 1, letters b) and c-bis) of the TUF, as amended by the Bank of Italy's Provision of 23 December 2022.

2.2. Scope of application

This Procedure applies—with reference to the relevant types of violations, as further specified in paragraph 4—to the Group Companies[1], which, pursuant to Article 2, paragraph 1, letter q) of the Whistleblowing Decree:

1) have employed, in the last year, an average of at least fifty employees with permanent or fixed-term employment contracts (the "**Medium and Large Companies**");

2) fall within the scope of the regulations listed in the Annex to the Whistleblowing Decree, Part I.B and Part II,[2], even if not included among those referred to in point 1) (the "**Companies operating in sensitive sectors**")

3) are different from those referred to in points 1) and 2) and have adopted an Organisation, Management and Control Model (OMM) pursuant to Legislative Decree 231/01.

The Parent Company reserves the right, based on risk-based assessments and within the limits of compatibility with specific sector regulations, to identify other companies to which this Procedure may be extended.

[1] The detailed list of the Group Companies that, at the time of approval of this Procedure, meet the requirements set out in this paragraph is provided in Annex 1.

[2] By way of example and without limitation, reference is made to the following acts: implementation of Directive 2009/138/EC (Solvency II), implementation of Directive 2016/2341/EU (IORP II), Regulation (EU) No 596/2014 (MAR), implementation of Directive 2014/65/EU (MiFID II), Regulation (EU) No 1286/2014 (PRIIPs), implementation of Directive (EU) 2016/97 (IDD), implementation of Directive (EU) 2015/849 (Fourth Anti-Money Laundering Directive).

2.3. Definitions and terminology

ACO	Antitrust Compliance Officer, pursuant to the Antitrust Organizational Procedure, if adopted by the In-Scope Company.
Personnel involved in distribution activities within the premises where the intermediary operates.	Pursuant to this Procedure, the natural person acting as an employee, collaborator, or other appointed representative of intermediaries registered in Section A of the Single Register of Insurance Intermediaries, even on an ancillary basis, as defined in letter c), paragraph 1, of Article 2 of IVASS Regulation No. 40 of 2 August 2018
Personnel engaged in distribution activities outside the premises of the intermediary for whom they operate.	Pursuant to this Procedure, the natural person acting as an employee, collaborator, or other appointed representative of intermediaries registered in Sections A and E of the Single Register of Insurance Intermediaries, even on an ancillary basis, as defined in letter b), paragraph 1, of Article 2 of IVASS Regulation No. 40 of 2 August 2018.
Agents	Pursuant to this Procedure, individual intermediaries who fall within the definitions set forth in Article 109, paragraph 2, letter a) of the Private Insurance Code (CAP) and Article 2, paragraph 1, letter d) of IVASS Regulation No. 40 of 2 August 2018, as amended.
Top Management	The Chief Executive Officer and/or the General Manager (if appointed) and, with reference to Unipol and the companies belonging to the Insurance Group headquartered in Italy, the senior management responsible for the decision-making process and implementation of strategies.
Other persons deserving of protection	Other persons connected to the whistleblower who could suffer retaliation within the workplace context, such as (i) the facilitator (as defined below); (ii) colleagues who have a habitual or recurring relationship with the person; (iii) individuals in the same workplace context who are linked to the whistleblower by a stable emotional or kinship bond up to the fourth degree; (iv) entities owned by the whistleblower or by the person for whom they work, as well as entities operating in the same workplace context as the whistleblower.
ANAC	The National Anti-Corruption Authority.
Audit	The core Audit function of Unipol, as well as the equivalent functions of the other In-Scope Companies, even if outsourced.
Risk Area	The core Risk Management function of Unipol, as well as the equivalent functions of the other In-Scope Companies, even if outsourced
Agency Collaborators	Personnel involved in distribution activities within the premises where the intermediary operates, as well as personnel engaged in distribution activities outside the premises where the intermediary operates.

Compliance	The Compliance and Group Anti-Money Laundering function of Unipol, as well as the equivalent functions of the other In-Scope Companies, even if outsourced.
Workplace context	The work or professional activities, past or present, carried out within the relationships referred to in paragraph 3, through which, regardless of the nature of such activities, a person acquires information about violations and within which they could risk suffering retaliation in the event of a violations.
Public Disclosure	The act of making information about violations public through the press, electronic media, or in any case through means of dissemination capable of reaching a large number of people
Facilitator	The natural person who assists the Whistleblower in the reporting process, operating within the same workplace context, and whose assistance must be kept confidential.
Company control functions	With reference to the Group Companies supervised by the Bank of Italy, the Audit, Risk Management, Compliance, and Anti-Money Laundering functions, in accordance with any service contracts relating to these functions.
Key Functions	With reference to the Parent Company and the other insurance undertakings of the Group, the Audit, Risk Management (or Chief Risk Officer), Compliance, and Actuarial Functions.
Insurance Group	Unipol Assicurazioni S.p.A, and the companies it controls that are registered in the Register [3]and the companies it controls that are registered in the Register of Parent Companies pursuant to Article 210-ter of the Private Insurance Code.
Unipol Group or Group	Unipol Assicurazioni S.p.A. and the companies it directly or indirectly controls, pursuant to Article 2359 of the Italian Civil Code..
Anti-Fraud Legislation	The body of European legislation for the protection of the Union's financial interests, as referred to in Article 325 of the Treaty on the Functioning of the European Union (combating fraud).[4]
Regulation aimed at safeguarding the internal market	The body of European legislation for the protection of the internal market, as referred to in Article 26, paragraph 2 of the Treaty on the Functioning of the European Union, including rules on competition, state aid, and corporate taxation[5].
Privacy Regulation	Regulation (EU) 2016/679 of 27 April 2016 (*General Data Protection Regulation* or GDPR), Legislative Decree No. 196 of 30 June 2003, as amended by Legislative Decree No. 101 of 10 August 2018, containing "*Provisions for the adaptation of national legislation to the provisions of Regulation (EU) 2016/679 of the European Parliament and of the Council of*

[3] The Register of Parent Companies can be consulted on the IVASS website in the "Registers" section. Registered in the Register are the parent company and its subsidiaries, such as (i) insurance and reinsurance undertakings, (ii) ancillary service companies, and (iii) insurance holding companies and mixed financial holding companies.

[4] See Article 2, paragraph 1, letter a), number 4) of the Whistleblowing Decree.

[5] Cf. Article 2, paragraph 1, letter a), number 5) of the Whistleblowing Decree.

	27 April 2016" (Italian Privacy Code), the Measures issued by the Italian Data Protection Authority, and, in general, all external legislation concerning the protection of natural persons with regard to the processing of personal data.
Sector-specific legislation and regulatory framework	The body of European Union or national legislation referred to in the Annex to the *Whistleblowing Decree*, or any national provisions implementing the European Union acts listed in the Annex to Directive (EU) 2019/1937, even where such provisions are not expressly mentioned in the Annex to the said Decree, insofar as applicable.[6]
SB	The supervisory body provided for under Article 6, paragraph 1, letter b) of Legislative Decree 231/01.
Decision-Making Body	Function/body responsible for defining and/or adopting the measures resulting from the Violations (see below) received, in accordance with the system of delegations and powers in force within the Companies within scope.[7]
Corporate Bodies	For the purposes of this Procedure, the term refers to the set of bodies with strategic supervision, management, and control functions. In particular, it includes the Board of Directors, the Chief Executive Officer (if appointed), and the Board of Statutory Auditors.
Whistleblowing System Officer	For the companies within the scope required to appoint this figure pursuant to the applicable whistleblowing legislation, [8] .This role ensures the correct implementation of the Procedure and, together with the Designated Structure, investigates and prepares the Report concerning Relevant Violations which, following the conducted inquiries, appear reasonably founded. Whistleblowing System Officer also maintains a dedicated Register of Violations and drafts and submits to the corporate Bodies the Report referred to in paragraph 10. Where provided, the role of Whistleblowing System Officer is carried out by the Head/Manager of the Audit function. The Whistleblowing System Officer may appoint one or more collaborators within their structure to support the management activities related to the Violations.
Retaliation	Any behavior, act, or omission, even if only attempted or threatened, carried out as a result of the Violation and which causes or may cause the Whistleblower/Reported person, directly or indirectly, an unjust harm.

[6] Cf. Article 2, paragraph 1, letter a), number 3) of the Whistleblowing Decree. It refers to acts concerning: public procurement; financial services, products and markets, and prevention of money laundering and terrorist financing; product safety and compliance; transport safety; environmental protection; radiological protection and nuclear safety; food and feed safety and animal health and welfare; public health; consumer protection; privacy and personal data protection; and security of networks and information systems.

[7] Persons responsible for receiving, examining, and evaluating violations do not participate in the definition of any subsequent decision-making measures.

[8] Currently, the only regulatory reference is the Bank of Italy Regulation dated December 5, 2019, implementing Articles 4-undecies and 6, paragraph 1, letters b) and c-bis), of the Consolidated Finance Act (TUF).

Whistleblower	The natural person who makes the violation.
Reported Person	The subject, whether a natural person or a legal entity, mentioned in the Violation, to whom responsibility for the reported act is attributed, directly or indirectly, or who is otherwise involved in the reported violation.
Violation	Any communication, written or oral and not anonymous, of information acquired by the Whistleblower within their workplace Context, including well-founded suspicions, concerning i) violations committed or that, based on concrete elements, could be committed within the Companies in scope; and ii) conduct aimed at concealing such violations.
External Violation	Any communication, written or oral of the information about violations, submitted through the external reporting channel referred to in paragraph 11.
Relevant Violation	For the companies within the scope required to appoint the Whistleblowing System Officer pursuant to the applicable whistleblowing legislation [9], a violation having the following features : a) concerns violations involving a member of the Board of Directors, the Board of Statutory Auditors, the Supervisory Body (SB), as well as the General Manager and, if appointed, the Chief Operating Officer; b) concerns violations of criminal relevance; c) concerns violations involving personnel from multiple business units of one of the companies within the scope or personnel from multiple companies within the scope; d) concerns violations that are systematically repeated; e) concerns violations that could entail a high risk of sanctions, significant financial losses, major impacts on the financial assets situation or reputational damage.
Medium-sized companies	Group companies that, over the past year, have employed an average number of employees under permanent or fixed-term employment contracts ranging between fifty and two hundred and forty-nine.
Large-sized Companies	Group companies that, over the past year, have employed an average of at least two hundred and fifty employees under permanent or fixed-term employment contracts.
Supervised companies	The Unipol Group companies with registered offices in Italy that are subject to regulatory supervision.
Designated Structure	The individual or autonomous function, staffed with specifically trained personnel, responsible for receiving, reviewing, and assessing violations.
Primary Designated Structure	The Designated Structure identified as follows: - For Supervised Companies, the Head/Responsible Person of the

[9] The only current regulatory reference is the Bank of Italy Regulation of December 5, 2019, implementing Articles 4-undecies and 6, paragraph 1, letters b) and c-bis), of the Consolidated Law on Finance (TUF).

	established Compliance Function (including in the case of outsourcing) and any delegated personnel; - For Large Companies other than Supervised Companies, the person/function appointed or established by the respective company through a specific resolution of its administrative body, and any delegated personnel; - For the other Companies within scope, different from those mentioned above, the Head of the Compliance Function established within Unipol and any delegated personnel, pursuant to a specific outsourcing agreement
Alternative Designated Structure	The Designated Structure identified as follows: - For Supervised Companies, the Head/Responsible Person of the Audit Function (including in the case of outsourcing) and any delegated personnel - For the other Companies within scope, different from the above, the Head of Audit at Unipol and any delegated personnel, pursuant to a specific outsourcing agreement.
Antitrust Violations	Violations of European Union rules on competition and State aid, as well as violations of the Antitrust Manual and/or the Antitrust Organizational Procedure, if adopted by the Companies within scope.

3. Persons who may activate the internal reporting system for violations

The internal reporting system for violations governed by the Procedure concerns reports of violations made by:

- employees of the companies within the scope, including any seconded employees from other companies, temporary agency workers, and apprentices;
- self-employed workers, including occasional workers, collaborators, freelancers, consultants, volunteers, and interns (both paid and unpaid) who carry out their activities at the companies within the scope;
- workers and collaborators who perform their work at suppliers of goods or services, contractors, or subcontractors used by the companies within the scope;
- agents and agency collaborators (where applicable);
- shareholders.
- persons performing administrative, management, control, supervisory, or representative functions, even if such functions are exercised de facto. [10].

Violations may also be submitted when the legal relationship referred to above has not yet commenced (if the information on the violations was acquired during the selection process or other pre-contractual phases), during the probationary period, and after the termination of the legal relationship (if the information was acquired during the course of the relationship itself).

[10] Members of the Supervisory Body (SB) of the companies within the scope, where present, are also included

Anonymous violations are not included in the internal reporting system governed by the Procedure, with the clarification that such violations are considered anonymous when they lack sender information sufficient to identify the individual with reasonable certainty (e.g., full name and tax code, or date of birth, or residence). Therefore, violations in which the sender identifies themselves using pseudonyms or other generic or fictitious names that do not allow the identification of the reporting person, or refer to a person who cannot be reasonably and uniquely identified as the sender, are also considered anonymous.

If an anonymous violation contains evidence of the seriousness and credibility of the reported circumstances, it will still be handled by the competent corporate functions (see paragraph 6.1). The protective measures outlined in paragraph 7 for the reporting person also apply to anonymous violations only if the reporting person is subsequently identified and has suffered retaliation

4. Subject of the Violations

The internal reporting system for violations governed by the Procedure concerns violations relating to:

for the **Medium-sized companies and the comapnies operating in sensitive sectors:**	- unlawful acts falling within the scope of the Sectoral Legislation, including actual or potential violations of the provisions aimed at preventing money laundering and terrorist financing, pursuant to Article 48 of Legislative Decree 231/07; - acts or omissions that violate Anti-Fraud Legislation; - acts or omissions that violate legislation protecting the internal market; - Antitrust violations; - acts or conduct that undermine the purpose or objectives of the above-mentioned provisions; unlawful conduct relevant under Legislative Decree 231/01, or violations of the Organization, Management and Control Model (OMM), where adopted
for companies other than those previously mentioned and equipped with an Organization, Management and Control Mode (OMM)	- unlawful conduct relevant under Legislative Decree 231/01, or violations of the Organizational, Management and Control Model

The Procedure does not apply to complaints, claims, or requests related to a personal interest of the reporting person that concern exclusively their individual employment relationships, or their relationships with hierarchically superior figures.

Violations that are unfounded and made with willful misconduct or gross negligence, once verified—even by a first-instance judgment—entail the criminal or civil liability of the reporting person, the loss of the protective measures referred to in paragraph 7, and the application of disciplinary sanctions, in accordance with the provisions of the current Company Disciplinary Regulation, without prejudice to

any other forms of liability provided for by law.

Violations based solely on suspicions, rumors, or information already in the public domain are also excluded from the internal reporting system governed by the Procedure.

5. Reporting Channels and Transmission Methods

The internal reporting system for violations is structured to ensure that violations are received, examined, and assessed by autonomous and independent bodies with specifically trained personnel, through dedicated channels that are separate from ordinary reporting lines.

Each company within the scope activates internal reporting channels, without prejudice to the possibility of outsourcing their management to an external party, which must also be autonomous and equipped with specifically trained personnel.

The Violations may be addressed to:

- the Primary Designated Structure of the company to which the violation refers;
- the Alternative Designated Structure of the company to which the violation refers, in the event that members of the Primary Designated Structure:
    - are hierarchically or functionally subordinate to the person potentially reported;
    - are themselves the alleged perpetrators of the violation or have a potential conflict of interest related to the report, such as compromising their impartiality and independence of judgment

The Whistleblower n may choose to address their violation to the equivalent channels established by the Parent Company, i, for example, they believe this to be safer or that handling by the Parent Company may be more effective in relation to the specific case.

Violations may be submitted, either in written or oral form, through a dedicated IT platform (the “Platform”), accessible to all reporting persons via the web, upon registration. The access link to the Platform and the instructions for its use, as described in a dedicated manual, are published together with the Procedure as provided in paragraph 9. The Platform has undergone a data protection impact assessment—in accordance with Article 13, paragraph 6, of the Whistleblowing Decree—which will be reviewed and updated whenever process changes may affect the risk to the rights and freedoms of the data subjects.

Written reports are submitted by completing the form available on the Platform, including all elements necessary to enable appropriate verification and checks to assess the validity of the reported facts. The whistleblower is also required to declare whether they have a personal interest related to the violation. Additionally, the reporting person may attach any documentation deemed relevant for the assessment of the violation.

Oral violations are submitted by recording a voice message using the specific functionality of the Platform.

The reporting person may also request, via the Platform, a direct meeting with members of the Designated Structure, to be scheduled in accordance with the guidelines set out in paragraph 5.1.

If a person other than the members of the Primary/Alternative Designated Structure receives a communication potentially falling within the scope of this Procedure:

- observe the confidentiality measures set out in paragraph 7.1,
- forward it within seven days to the Primary Designated Structure or – if the members of the Primary Designated Structure are hierarchically or functionally subordinate to the person potentially reported, are themselves the alleged perpetrators of the violation, or have a potential conflict of interest related to the violation– to the Alternative Designated Structure[11].
- simultaneously inform the whistleblower of the transmission

In this case, the confidentiality of the reporting person is guaranteed—according to the standards of the Platform referred to in paragraph 7.1—only from the moment the violation is taken over by the competent Designated Structure (see below). Similar measures apply in cases where communication is received through means other than the Platform.

5.1. Guidelines for the arrangement of the meetings with the Whistleblowers

Direct meetings are scheduled within fifteen working days from the date the Whistleblower's request is received, at the premises of the relevant Company, in company facilities that ensure maximum confidentiality in accordance with paragraph 7.1. Alternatively, if the requester consents, the meeting may be held via videoconference, provided that it also guarantees the utmost confidentiality of the conversation and is attended only by authorized individuals.

The meetings may also be attended, at the Whistleblower's request, by any Facilitators. One or more members of the Designated Structure of the relevant Company will participate and document the conversation as provided in paragraph 8.

The members of the Primary/Alternative Designated Structure are responsible for promptly entering the violations thus received into the Platform.

6. The violations management process

The violations management process is divided into the following phases, which are detailed in the subsequent paragraphs

- receipt and preliminary analysis of violations;
- review and assessment of Reports and Relevant Violations;
- adoption of decision-making measures;
- monitoring of corrective actions.

6.1. Receipt and preliminary analysis of violations

Upon receipt of a violation, the members of the Primary/Alternative Designated Structure carry out a preliminary assessment to determine whether it meets the criteria to be classified as a violation under this Procedure. In particular, they verify that the report:

- is not anonymous;
- is submitted by an individual falling within the categories referred to in paragraph 3;
- concerns behaviors, acts, or omissions that are not already public knowledge and that may constitute a violation as defined in paragraph 4.

[11] The members of the Primary/Alternative Designated Structure are responsible for promptly entering the violations received in this manner into the Platform

If any of the above elements are missing, the violation shall be considered outside the scope of this Procedure. [12] Although the communication does not qualify as a violation under the legislation governing whistleblowing management, it must still be handled within the framework of company procedures. Therefore, where appropriate, the violation shall be forwarded—together with a brief explanatory note—to the competent structure (as identified below), with simultaneous notification to the whistleblower, so that it may be processed in accordance with the applicable regulations. By way of example, but not limited to:

- violations that can be classified as "complaints," pursuant to the "Complaint Management Policy" in force (where adopted) for the specific Company within scope, shall be forwarded to the structure responsible for complaints, in accordance with said Policy;
- violations concerning behaviors that are contrary to the Code of Ethics shall be forwarded to the Group Ethics Officer, in accordance with the provisions of the Code of Ethics;
- violations that present disciplinary aspects not specifically related to this Procedure shall be forwarded to the Unipol Human Resources Area or to the equivalent function of the other Companies within scope (where applicable);
- violations concerning Antitrust Violations that (i) are based on information acquired outside of the individual's workplace context, (ii) are already public knowledge, or (iii) are anonymous, shall be forwarded to the ACO of the relevant Company and managed in accordance with the procedures set out in the Antitrust Organizational Procedure, where adopted;
- for Companies not equipped with an Organizational, Management and Control Model (OMM), violations concerning corrupt practices shall be forwarded to the email addresses indicated in the Group's current Anti-Corruption Guidelines.

If, on the other hand, the violation falls within the scope of this Procedure, the Designated Structure shall proceed with the activities described in the following paragraphs. [13] As further specified below, in cases where a violation concerns an Antitrust Violation, such activities shall be carried out in coordination with the ACO, who shall perform their duties also in accordance with the provisions of the Antitrust Organizational Procedure.

6.2. Review and Assessment of Violations and Relevant Violations

The Whistleblower shall be informed—via the Platform—of the receipt of the violation within seven working days from the date it was received, as well as of the possibility of being contacted again to provide any additional information useful for the investigation phase.

The Designated Structure shall first assess whether the violation contains the minimum elements and requirements necessary to initiate the appropriate inquiries; if not, it shall promptly request the Whistleblower to provide the additional information deemed necessary. If the violation concerns Antitrust Violations, the above activities shall be carried out in coordination with the ACO. [14]

---

[12] In this case, the Primary/Alternative Designated Structure is not required to enter the violation received through a direct meeting or other means into the Platform.

[13] In the presence of the elements referred to in the relevant paragraph, a report concerning violations already reported to the judicial or accounting authority shall also qualify as a violation under this Procedure. In such cases, the Designated Structure, in compliance with the confidentiality measures set out in paragraph 7.1, shall involve Unipol's Legal Area (or an equivalent function) to assess the most appropriate actions and to monitor the outcomes of any ongoing proceedings.

[14] Except in cases where the ACO is the alleged perpetrator of the violation or has a potential conflict of interest related to the violation.

If, within 15 working days from the request, such additional information is not provided or is provided in an incomplete and/or otherwise insufficient manner for a proper assessment of the violation, the Designated Structure shall proceed with the archiving of the violation promptly informing both the Whistleblower and the Whistleblowing System Officer [15] and to the ACO (if the violation concerns Antitrust Violations), within 30 working days from the receipt of the violation or from the receipt of any additional information. This is without prejudice to any independent decisions made by the ACO in accordance with the Antitrust Organizational Procedure. If, even following the additional information provided by the Whistleblower, the violation does not appear to be manifestly unfounded, the Designated Structure shall take charge of the violation t and initiate the investigation phase.
If the violation t concerns unlawful conduct relevant under Legislative Decree 231/01 or violations of the OMM, the Designated Structure, in compliance with the confidentiality measures set out in paragraph 7.1, shall promptly inform the Supervisory Body (SB) of the relevant company about the violation received and the intention to proceed with the investigation phase, in order to gather any input from the SB. The Designated Structure shall keep the SB of the relevant company constantly updated on the progress of the case. Such notifications to the SB shall be managed through specific features of the Platform, to which the members of the SB are individually authorized.

If the relevant company has an ACO and the Report concerns Antitrust Violations, regardless of how the violation is classified by the Whistleblower on the Platform, the Designated Structure, in coordination with the ACO and in compliance with the confidentiality measures set out in paragraph 7.1, shall proceed with the investigation phase. The involvement of the ACO in the investigation process is managed through specific features of the Platform, to which the ACO is authorized.

The Designated Structure may, if deemed appropriate, make use of the support of the Audit function or other company departments to carry out the necessary checks, including at the premises of the relevant departments or with the individuals involved, always in compliance with the confidentiality measures set out in paragraph 7.1.

The Reported Person may be heard, or, upon their request, shall be heard, including through a written procedure by submitting written observations and documents, always in compliance with the confidentiality measures set out in paragraph 7.1.

Once the investigation phase is concluded and all elements useful for assessing the violation have been collected, the Designated Structure, in coordination with the ACO (if the violation concerns Antitrust Violations), shall prepare an explanatory note detailing the analyses carried out and the findings that emerged (the “Note”), accompanied by any proposals regarding the adoption of necessary corrective actions on the areas and business processes affected by the violation. These actions are identified to improve/strengthen the internal control and risk management system, also involving the relevant Key Functions/Control Functions (the “Corrective Actions”), and the Note shall be forwarded to the competent Decision-Making Body.[16]. Any independent decisions made by the ACO pursuant to the Antitrust Organizational Procedure remain unaffected.

If the violation is classified as a Relevant violation, the Designated Structure shall initiate the investigation phase jointly with the Whistleblowing System Officer [17], as well as with the ACO (in the

[15] Except in cases where the Whistleblowing System Officer is the alleged perpetrator of the violation or has a potential conflict of interest related to the violation.
[16] In the case of a collegial body, the Designated Structure shall request the secretary of said body to include the review of the Note in the agenda of the next available meeting, or—if necessary—to convene an extraordinary meeting.
[17] Except in cases where the Whistleblowing System Officer is the alleged perpetrator of the violation or has a potential conflict of interest related to the Violation

case of a Relevant Violation concerning Antitrust Violations). If, following the investigations carried out, the Relevant Violation appears to be unfounded, the Designated Structure shall share with the Whistleblowing System Officer a reasoned proposal for archiving, which shall be communicated to the Chair of the Board of Directors of the relevant Company. The Whistleblower shall also be informed of the archiving. Any independent decisions made by the ACO pursuant to the Antitrust Organizational Procedure remain unaffected.

If, on the other hand, the Relevant violation appears reasonably well-founded following the investigations, the Designated Structure and the Whistleblowing System Officer, in coordination with the ACO (in the case of a Relevant violation concerning Antitrust Violations), shall forward the Note, along with their assessments, to the competent Decision-Making Body[18], also informing the Board of Statutory Auditors.

6.3. Adoption of Decision-Making Measures

The competent Decision-Making Body, upon receiving the Note, shall decide on the appropriate actions to be taken based on the applicable internal and external regulatory framework, unless it deems further investigation necessary. In such cases, it shall request the Designated Structure and/or the Whistleblowing System Officer, as applicable according to the previous paragraph, to carry out the additional inquiries.

If the violation constitutes grounds for the possible initiation of disciplinary proceedings against the Reported Person, and if the allegations are based, in whole or in part, on the violation (and not on separate and additional findings resulting from independent investigations carried out by the Company, even following the violation), and the identity of the Whistleblower is essential for the defense of the Reported Person, the violation may only be used for disciplinary purposes with the Whistleblower's consent to the disclosure of their identity.

If the Whistleblower is jointly responsible for the violations, any disciplinary measures imposed on them shall be modulated, taking into account the contribution they provided to the discovery or prevention of violations, and in accordance with the applicable regulations.

The Decision-Making Body informs the Designated Structure/ Whistleblowing System Officer, where present, of the actions taken following the violation it received, including any decision to close the case. The Designated Structure, in turn, is responsible for informing the structures in charge of implementing the Corrective Actions, as well as the ACO (if the Corrective Actions are relevant to its areas of responsibility[19]) and the SB, if the violation concerns unlawful conduct relevant under Legislative Decree 231/01 or violations of the Company's Organizational, Management and Control Model (OMM), of the Company to which the violation refers.

If the violation is deemed Significant, the Designated Structure/ Whistleblowing System Officer shall inform about the actions taken by the Decision-Making Body / the defined Corrective Actions: i) the structures responsible for implementing the Corrective Actions and the SB (Supervisory Body), if the violation concerns unlawful conduct relevant under Legislative Decree 231/01 or violations of the Organizational, Management and Control Model (OMM) of the Company to which the violationt refers; ii) the corporate bodies of the Company to which the violation refers, if they have not already been

[18] In the case of a collegial body, the Whistleblowing System Officer shall request the secretary of the body to include the review of the Note on the agenda of the next available meeting, or – if necessary – to convene an extraordinary meeting

[19] By way of example and not exhaustively, this includes cases where Corrective Actions involve changes to the organizational structure of the areas/companies affected by the Report (provided such changes concern in-scope Companies that have an Antitrust Organizational Procedure in place).

involved.

The Whistleblower has the possibility, through access to the Platform, to check at any time the status of the reported violation as well as the outcome of the procedure (including the possible closure of the violation). In any case, the Designated Structure, within three months from the date of acknowledgment of receipt of the violation or, in the absence of such acknowledgment, within three months from the expiry of the seven-day period following the submission of the violation, shall provide a written response via the Platform[20] - regarding the outcome of the procedure or any further responses to be expected.

6.4. Monitoring of Corrective Actions

The Designated Structure ensures the monitoring of the implementation of the defined Corrective Actions and provides adequate reporting—at least annually—to the Whistleblowing System Officer, where present, to the ACO (for Violations concerning Antitrust Violations), to the SB (Supervisory Body), if the violation concerns unlawful conduct relevant under Legislative Decree 231/01 or violations of the OMM, and to the corporate bodies (in the case of a Significant Violation), regarding the progress and completion status of such actions.

7. Protection Measures for the Whistleblower and the Reported Person

7.1. Confidentiality

Violations may not be used beyond what is necessary to appropriately follow them up.

Throughout the entire process of violations management—from receipt to investigation and conclusion—maximum confidentiality is ensured regarding the identity of both the Whistleblower and the Reported Person, as well as the content of the violation and the related documentation.

Individuals who receive, examine, and assess violations, the Whistleblowing System Officer (where present), the ACO, the members of the Supervisory Body (SB), and any other parties involved in the Procedure are required to ensure that the information received is kept strictly confidential and that the identity of the Whistleblower is not disclosed, except under specific conditions outlined in paragraph 7.2.

The Whistleblower is not punishable for disclosing information about violations covered by confidentiality obligations—excluding obligations related to classified information, legal or medical professional secrecy, or the confidentiality of judicial deliberations—or for disclosing information concerning copyright protection or personal data protection, or information that may harm the reputation of the person involved, when, at the time of disclosure, there were reasonable grounds to believe that such disclosure was necessary to reveal the violation and the violarion was made in accordance with the Procedure. In such cases, any further liability, including civil or administrative, is also excluded.

In any case, criminal liability and any other liability, including civil or administrative, is not excluded for actions, conduct, or omissions unrelated to the violation or not strictly necessary to disclose the violation.

The use of the Platform referred to in paragraph 5 allows:

- encryption of elements related to the violation, including the Whistleblower’s identifying data,

[20] In the case of a violation submitted through a direct meeting, the written response is sent to the contact provided by the Whistleblower during the interview.

already at the time of receipt;

- storage of all violations and related documentation in a 'secure environment' accessible only to members of the Designated Structure, the Responsible SIS (where present), the ACO (if the violations concern Antitrust Violations), or the members of the Supervisory Body (SB) (if the violation concerns unlawful conduct relevant under Legislative Decree 231/01 or violations of the OMM);
- prevention of communications or circulation of documents outside this environment, except where strictly necessary for managing the violation.

Access rights to the Platform for the purpose of managing violations are defined according to criteria that ensure access is limited to only those users strictly necessary for the effective management of the process. The decryption of the Whistleblower's identity may only take place with prior authorization from the Responsible SIS, for Companies where such a role has been appointed[21] or by the Head of the Designated Structure that received the violation for the other in-scope Companies, and only under the conditions specified in paragraph 7.2.

The following measures shall also be observed:

- any paper or electronic documents containing information related to the violation must be marked as 'Confidential' and must never be left unattended; they must be stored in physically controlled-access areas or in dedicated archives protected by appropriate security systems;
- when the transmission/storage of information related to the violation is carried out via electronic files, these must, where possible, be protected by specific passwords;
- printing or copying of documents must be done only when strictly necessary and, in any case, in secure environments, avoiding sending print jobs or leaving copies unattended at printers or photocopiers located in hallways or other unsupervised areas;
- the transfer of paper documents should be avoided; if necessary, it must be tracked by completing the specific confidential document transmission form referred to in Annex 3.
- anyone who becomes aware that information related to the violation has come into the possession of individuals not involved in the violation management process must report this circumstance to the Primary/Alternative Designated Structure.

The breach of the confidentiality obligation constitutes grounds for disciplinary liability, in accordance with the provisions of the current Corporate Disciplinary Regulation, without prejudice to any other forms of liability provided for by law.

7.2. Cases in which the identity of the Whistleblower may be disclosed and information provided to the Reported Person

Outside the cases expressly provided for by the legislation in force from time to time.[22], the identity of the Whistleblower and any other information from which their identity can be directly or indirectly inferred may not be disclosed without their express consent to persons other than those authorized to receive or follow up on the violations , and who are expressly authorized to process such data in accordance with Privacy Regulations.

---

[21] This provision does not include any collaborators of the Whistleblowing System Officer. If the Whistleblowing System Officer is the alleged perpetrator of the violation or has a potential conflict of interest related to the Report, the authorization must be granted by the Head of the Primary Designated Structure.

[22] The law provides for the possibility of disclosing the identity of the Whistleblower when it is absolutely necessary for the defense of the Reported Person (see, by way of example and not limitation, TUF, Article 4-undecies, paragraph 2(a)).

In the context of disciplinary proceedings, in particular, no information is provided to the Reported Person regarding the Violation made against them, nor regarding the identity of the Whistleblower:

- whether disciplinary proceedings are initiated against the Reported Person;
- or whether the violation is dismissed.

As indicated in paragraph 6.3, if the allegation is based, in whole or in part, on the violation (and not on findings from separate and additional investigations carried out by the Company, even following the violation), it may only be used if the Whistleblower consents to the disclosure of their identity. In such a case, the identity of the Whistleblower may be disclosed to the Reported Person if it is essential for their defense. The Designated Structure shall notify the Whistleblower in writing of the reasons for the disclosure of the confidential data.

7.3. Prohibition of Retaliation

Whistleblowers must not be subject to any Retaliation.

Dismissal, reassignment of duties pursuant to Article 2103 of the Italian Civil Code, as well as any other retaliatory or discriminatory measure against the Whistleblower[23]shall be null and void if adopted for reasons directly or indirectly connected to the violation[24].

The submission of a violation does not constitute a breach of the obligations arising from the contractual relationship between the Whistleblower and the Company concerned.

It is understood, however, that if the Whistleblower is found criminally liable — even by first-instance judgment — for the offenses of defamation or false accusation, or found civilly liable in cases of willful misconduct or gross negligence, a disciplinary sanction may be imposed.

The above protection measures also apply to Other Persons deserving of protection. Entities and individuals who believe they have suffered Retaliation may act in the manner and form provided for by Article 19 of the Whistleblowing Decree. [25]

7.4. Protection of Reported Person

The Reported Person is protected (i) from negative consequences resulting from the Violation, in cases where the violation management process does not reveal any elements justifying the adoption of measures against them, and (ii) from any negative effects other than those provided for by any measures that may be adopted.

8. Provisions on Personal Data Protection and Traceability of the Violation Management Process

Pursuant to the applicable Privacy Regulations[26], the Data Controller for the personal data collected in the management of violations is the Company within the perimeter to which the violations refers.

---

[23] Pursuant to Article 17, paragraph 4 of the Whistleblowing Decree, retaliation includes, by way of example and not limited to: suspensions, transfers, demotions or missed promotions, non-renewal or early termination of a fixed-term employment contract, failure to convert a fixed-term contract into a permanent one where the worker had a legitimate expectation of such conversion, cancellation of leave or time off, negative evaluations or references, early termination or cancellation of contracts for the supply of goods or services

[24] In the event of disputes, it is the employer's responsibility to prove that such measures are based on reasons unrelated to the violation itself.

[25] Article 19 of the Whistleblowing Decree provides for the possibility of reporting any retaliation to ANAC. In such cases, ANAC informs the National Labour Inspectorate, which is responsible for taking the appropriate measures within its competence.

[26] See Article 4, paragraph 1, point 7 of the GDPR.

Annex 2 provides the privacy notice for Whistleblowers regarding the processing of personal data for the purpose of receiving and managing the Violations made available together with the Procedure as set out in paragraph 9.
When the Whistleblower submits a Violations—either through the Platform or via a direct meeting—they must confirm that they have read the privacy notice on the processing of personal data.

Individuals involved in the report management process, in various capacities, act as Authorized Persons for the related processing of personal data acquired during the management of violations . With regard to the processing of such data, and in addition to (i) the provisions of the Group Unipol's Policy on the protection and enhancement of personal data and (ii) the designation act as Authorized Data Processor provided to all employees in accordance with Group Internal Provision No. 231 of 12 June 2018, it is specified that each Authorized Person involved in the management process of violation is previously authorized under this Procedure and—based on the specific authentication credentials assigned to them—is enabled to access the Platform solely for the purpose of carrying out the operations strictly necessary for the proper execution of the activities provided for by the Procedure.

The Designated Structure keeps a register of all received violations (including anonymous ones[27])and their related management, ensuring the storage of the reports and all supporting documentation in appropriate paper or digital archives, in compliance with the confidentiality measures set out in paragraph 7.1.

When information on violations is communicated orally—either by recording a voice message or, at the Whistleblower's request, during a direct meeting with members of the Designated Structure—the violation, with the Whistleblower's prior consent, is documented by the Designated Structure either by recording it on a device suitable for storage and playback, or in writing through a detailed transcript of the conversation.

The Whistleblower's consent to the documentation of the violation is expressly recorded at the beginning of the recording or the written transcript through a full transcription. In the case of a transcript, the Whistleblower may review, correct, and confirm its content by signing it. The Group has defined the retention periods for personal data processed in the context of violation management, in accordance with the provisions of the applicable Privacy Regulations and the Group's Internal Provisions relating to (i) the rules for determining the retention periods of personal data contained in documents and electronic archives, and (ii) the retention periods of personal data contained in company paper archives.
In particular, personal data are processed for the time strictly and technically necessary for the proper management and completion of the procedure; thereafter, they are retained for a maximum of five years from the date of communication of the final outcome of the violation and, once this period has elapsed, they are deleted, except in cases where the violation leads to the initiation of disputes, proceedings, or complaints, in which case the data must be retained until the final resolution of such matters.
Personal data that are not relevant for the management of the violation are not collected or, if collected accidentally, are immediately deleted.

9. Dissemination and Publication of the Document

[27] Thus making it possible to trace them, in the event that the whistleblower informs ANAC that they have suffered retaliatory measures as a result of that anonymous violation or disclosure.

To encourage the use of the internal reporting system and to promote a culture of legality, this Procedure:

- is published in the "The Group – Whistleblowing" section of the Group Futur@ corporate Intranet and in the "Regulations and Manuals – Compliance and Regulations – Relationship with the Company – Whistleblowing" section of the DAILY portal dedicated to Agents, which is also accessible to Agency Collaborators;
- is published by the Companies within the scope in one or more dedicated sections [28] of their respective websites;
- is made available in paper format at the premises of the Companies within the scope that do not have a website and whose personnel may not have access to the Group corporate Intranet, by posting it on the designated bulletin boards.

10. Reporting

For the Companies within the scope that are subject to specific obligations under the applicable whistleblowing legislation[29], the Board of Directors and the Board of Statutory Auditors receive an annual report from the SIS Manager on the proper functioning of the internal reporting system (the "Report"), containing aggregated information on the outcomes of the activities carried out following the violations received. The Report, approved by the Board of Directors and, where required by the applicable whistleblowing legislation[30],by the Board of Statutory Auditors, is made available to personnel.

If violations have been received concerning unlawful conduct relevant under Legislative Decree 231/01 or violations of the Organizational, Management and Control Model (OMM), the Supervisory Body (SB) of the relevant company is informed by the Designated Structure at the first available meeting, in compliance with the confidentiality measures set out in paragraph 7.1.

11. External Violation and Public Disclosure

The Whistleblower – except in the cases referred to in paragraph 2.2 no. 3 – may submit an external violation to ANAC if, at the time of submission, one of the following conditions is met:

- the internal reporting channel is not mandatory in the workplace context, or, if required, it has not been activated or, even if activated, it does not comply with the provisions of Article 4 of the Whistleblowing Decree;
- the Whistleblower has already submitted an internal violation under this Procedure and it has not been followed up;
- the Whistleblower has reasonable grounds to believe that, if they were to submit an internal violation , it would not be effectively followed up or could lead to a risk of Retaliation;
- the Whistleblower has reasonable grounds to believe that the violation may constitute an imminent or manifest danger to the public interest.

Such external Violations may be submitted through the channels established pursuant to Article 7 of

[28] Easily accessible and whose name includes the term "whistleblowing".

[29] Currently, the only regulatory reference is the Bank of Italy Regulation of 5 December 2019 implementing Articles 4-undecies and 6, paragraph 1, letters b) and c-bis), of the Consolidated Law on Finance (TUF).

[30] Currently, the only regulatory reference is the Bank of Italy Regulation of 5 December 2019 implementing Articles 4-undecies and 6, paragraph 1, letters b) and c-bis), of the Consolidated Law on Finance (TUF).

the Whistleblowing Decree, in accordance with the procedures indicated on the ANAC website.[31].

The Whistleblower who makes a public disclosure is entitled to the protection provided by the Whistleblowing Decree if, at the time of the disclosure, one of the following conditions is met:

- They have previously made an internal and external violation, or have made an external violation directly, and no response has been provided within the prescribed time limits;
- They have reasonable grounds to believe that the violation may pose an imminent or manifest danger to the public interest;
- They have reasonable grounds to believe that the external violation may entail a risk of retaliation or may not be effectively followed up due to the specific circumstances of the case, such as situations where evidence may be concealed or destroyed, or where there is a well-founded fear that the person receiving the violation may be colluding with the perpetrator of the violation or involved in the violation itself.

[31] *https://www.anticorruzione.it/-/whistleblowing*

Annex 1 – Companies of the Group falling within the Scope of application

Companies[32]	1) **Medium and Large-sized Companies**	2) **Company operatng in sensitive sectors**	3)**Companies equipped with OMM**[33]
Unipol Assicurazioni[34]	x	x	x
Gruppo UNA	x		x
UniSalute	x	x	x
UnipolRental	x		x
Società e Salute	x		x
Compagnia Assicuratrice Linear	x	x	x
UnipolAssistance	x		x
Arca Assicurazioni	x	x	x
Arca Vita[35]	x	x	x
Casa di Cura Villa Donatello	x		x
Siat Società Italiana Assicurazioni e Riassicurazioni	x	x	x
Irma	x	x	
UnipolTech	x		
Leithà	x		
Tenute del Cerro	x		x
SiSalute	x		x
UnipolService	x		x
Arca Inlinea	x		x
Arca Sistemi			x
I.Car	x		
UnipolPay		x	
Marina di Loano			x
Unipol Motor Partner		x	
BeRebel		x	
UniAssiTeam		x	
Florence Centro di Chirurgia Ambulatoriale			x
Bim Vita[36]		x	x
Unipol Investimenti SGR		x	x
Arca Direct Assicurazioni		x	x
Unipol Finance		x	
LinearNext		x	
UnipolReC		x	x

[32] The Companies are listed in order of average workforce as of 31/12/2024; seconded personnel from other Group Companies is not included in the calculation. Companies classified as Large under this Procedure are shown in bold.

[33] Companies already included under points 1) and 2) are shown in grey.

[34] Also in its capacity as an entity that has established and manages supplementary pension schemes (Open Pension Fund and Individual Pension Plans).

[35] Also in its capacity as an entity that has established and manages supplementary pension schemes (Individual Pension Plan).

[36] Also in its capacity as an entity that has established and manages supplementary pension schemes (Open Pension Fund).

Annex 2 – Privacy Notice to the Data Subject pursuant to Articles 13 and 14 of Regulation (EU) 2016/679

USA_Info_Whis_01 – Ed. 01.01.2025

Privacy Notice to the Data Subject pursuant to Articles 13 and 14 of Regulation (EU) 2016/679 – General Data Protection Regulation (hereinafter also referred to as the "Regulation")

We hereby inform you of the following.

Unipol Assicurazioni S.p.A. and the companies belonging to the Unipol Group that are subject to Legislative Decree No. 24 of March 10, 2023, as listed below, have implemented an internal system to ensure the protection of individuals who report violations of legal provisions that may harm the integrity of the aforementioned companies and that they have become aware of in a workplace context (so-called whistleblowing).
To enable the activation of the internal reporting system, the "Procedure for Reporting Violations (so-called Whistleblowing)" (hereinafter, the "Procedure") has been adopted.
According to this Procedure, violations may be submitted in writing or orally through a dedicated IT platform (the "Platform"), accessible via the web after registration.

The personal data you provide, necessary to identify you and allow you to proceed with the violation , will be processed by the company to which the report refers (hereinafter, the "Company"), in its capacity as Data Controller, for the purposes and on the legal bases indicated below:

(F1) – Platform Registration: the processing is carried out to enable registration on the Platform through which you can submit violations. If, after registering on the Platform, you do not submit a violation within 10 days from the registration date, your account will be automatically deleted and your data erased (without prejudice to the possibility of registering again for a new violation).

(F2) – Reporting: the processing is carried out to allow you to submit a violation, either in writing or orally, through the Platform.

The legal basis for the processing, for both purposes listed above, lies in the need to comply with legal obligations and in the legitimate interest of the Company to which the violation refers, in preventing unlawful conduct within its organization.

We also specify the following:

1. Processing will also be carried out using electronic or otherwise automated means, through logic and methods strictly related to the purposes indicated, and always in a way that ensures the security and confidentiality of personal data. Personal data will be stored in full compliance with the security measures provided by data protection legislation and will be retained for the time necessary for the proper management of the report and, in any case, no longer than five (5) years from the date of communication of the final outcome of the reporting procedure, except in cases where the report leads to disputes, proceedings, or complaints, in which case the data must be retained until their full resolution. Personal data not relevant to the management of the violation will be immediately deleted.
2. The provision of the requested personal data is essential to proceed with the violation; refusal to provide such data would prevent the Company from processing your violation.
3. Your data may be disclosed only to those who receive, examine, and assess the violations, to

the SIS Manager, where applicable, and to any other party involved in the Procedure, as well as to public authorities such as the Judicial Authority or Supervisory Authorities in compliance with specific legal obligations and/or to fulfill requests made in connection with ongoing investigations and legal proceedings. Data may also be disclosed to third parties if necessary to pursue the legitimate interests of the Company to which the violation refers (e.g., to assert or defend a right in court). Personal data will not be disseminated.

4. Privacy legislation (Articles 15–22 of the Regulation) guarantees data subjects the right to access their data at any time, as well as to request its rectification and/or integration if inaccurate or incomplete, its erasure or restriction of processing where applicable, to object to processing for reasons related to their particular situation, and to data portability for data provided and processed by automated means, within the limits set by the Regulation (Article 20). Please note that the exercise of the above rights may be delayed, limited, or excluded pursuant to Article 2-undecies, paragraph 1, letter f) and paragraph 3, of Legislative Decree 196/2003 (the "Privacy Code") and may not in any case compromise the confidentiality of the identity of the whistleblower.
5. The Data Controller is the Company to which the violation refers.
6. The "Data Protection Officer" is available to data subjects at the Company to which the violation refers, at the addresses listed in the table below.
7. Each data subject retains the right to lodge a complaint with the Italian Authority, the Garante Privacy, if deemed necessary to protect their personal data and rights, or, in cases expressly provided for by Article 2-undecies of the Privacy Code, to exercise their rights through the Garante, in accordance with Article 160 of the Code.

Company Name	**Contact Details (Registered Office – e-mail)**
Arca Assicurazioni S.p.A.	Via del Fante n. 21, 37122, Verona - privacy@arcassicura.it
Arca Direct Assicurazioni s.r.l.	Via del Fante n. 21, 37122, Verona - privacy@arcassicura.it
Arca Inlinea Scarl	Via del Fante n. 21, 37122, Verona - privacy@arcassicura.it
Arca Sistemi Scarl	Via del Fante n. 21, 37122, Verona - privacy@arcassicura.it
Arca Vita S.p.A.	Via del Fante n. 21, 37122, Verona - privacy@arcassicura.it
BeRebel S.p.A.	Via Stalingrado n. 37, 40128, Bologna - privacy@berebel.it
Bim Vita S.p.A.	Via San Dalmazzo n. 15, 10122, Torino - privacy.bim-vita@unipol.it
Casa di Cura Villa Donatello S.p.A.	Viale G. Matteotti, n. 4, 50132, Firenze - privacy@villadonatello.it
Compagnia Assicuratrice Linear S.p.A.	Via Larga n. 8, 40138, Bologna - privacy@linear.it
Florence Centro di Chirurgia Ambulatoriale S.r.l.	Viale G. Matteotti, n. 4, 50132, Firenze - privacy@centroflorence.it
Gruppo UNA S.p.A.	Via Gioacchino Murat n. 23, 20159, Milano - privacy@gruppouna.it

Company Name	**Contact Details (Registered Office – e-mail)**
I.CAR S.r.l.	Via Tevere n. 18, 40069, Zola Predosa (BO) - privacy@icar-web.it
IRMA S.r.l.	Via Larga n. 4A, 40138, Bologna - privacy.irma@unipol.it
Leithà S.r.l.	Via Stalingrado n. 53, 40128, Bologna - privacy@leitha.eu
Linear Next s.r.l.	Via Larga n. 8, 40138, Bologna - privacy@linearnext.it
Marina di Loano S.p.A.	Lungomare Nazario Sauro n. 12/1, 17025, Loano - privacy@marinadiloano.it,
SIAT Società Italiana di Assicurazioni e Riassicurazioni p.A.	Via V Dicembre n. 3, 16121, Genova - privacy.siat@unipol.it
SiSalute S.r.l.	Via Larga n. 8, 40138, Bologna - privacy@si-salute.it
Società e Salute S.p.A.	Via Temperanza n. 6, 20127, Milano
Tenute del Cerro S.p.A.	Via Grazianella n. 5, 53045, Montepulciano, - privacy@tenutedelcerro.it
UniAssiTeam S.r.l.	Via Stalingrado n. 45, 40128, Bologna - privacy.uniassiteam@unipol.it
Unipol Assicurazioni S.p.A.	Via Stalingrado n. 45, 40128, Bologna - privacy@unipol.it
UnipolAssistance S.c.r.l.	Via Carlo Marenco n. 25, 10126, Torino - privacy.unipolassistance@unipol.it
UnipolPay S.p.A.	Via Stalingrado n. 37, 40128, Bologna - privacy@unipolpay.it
UnipolReC S.p.A.	Piazza Sergio Vieira de Mello n. 6, 40128, Bologna - privacy@unipolrec.it
UnipolRental S.p.A.	Via G.B. Vico n. 10/C, 42124, Reggio Emilia - privacy@unipolrental.it
Unipol Finance S.p.A.	Via Stalingrado n. 45, 40128, Bologna
Unipol Investimenti SGR	Via Carlo Marenco n. 25, 10126, Torino - privacy.UnipolInvestimenti@unipol.it
Unipol Motor Partner S.r.l.	Via Tevere n. 18, 40069, Zola Predosa (BO) - privacy@unipolbo.it
UnipolService S.p.A.	Via C. Marenco n. 25, 10126, Torino - privacy@unipolservice.it
UnipolTech S.p.A.	Via Stalingrado n. 37, 40128, Bologna - privacy@unipoltech.it
UniSalute S.p.A.	Via Larga n. 8, 40138, Bologna - privacy@unisalute.it

Annex 3 - Module for the submission of confidential documents

Confidential Document

Company	
Document Title	
Last update Date	

Sender

Name	
Surname	
E-mail adress	
Company Function	
Group Company of Affiliation	

Signature of the Sender

_____

Recipient

Name	
Surname	
E-mail adress	
Company Function	
Group Company of Affiliation	

Recipient's Signature for Receipt of Confidential Documents

_____

Unipol S.p.A.
Sede Legale
Via Stalingrado, 45
40128 Bologna

unipol.com
unipol.it