Document Type: *Policy*

Whistleblowing Policy

Competent Structure: Internal Audit Department

Date: July, 2023

Version 7

Internal Use Only

SUMMARY

Document Type:	Policy	
Structure Responsible for the Document:	Internal Audit Department	
Contacts	Head of Internal Audit Department: Fabio Marchesi fabio.marchesi@illimity.com	
Structures Involved in the Process of Sharing the Present Version	Compliance & AFC Officer; HR & Organization	
Recipients of the Regulation	**Parent Company**	**Other Companies**
	illimity Bank S.p.A.	n.a.
Version approved by:	Board of Directors	
Date of approval	13/07/2023	
Date of validity	14/07/2023	

VERSIONS

Name of regulation and version	Main changes	Approving body and date
Whistleblowing Policy V.1	Drafting of the Document	Board of Directors, 17 December 2018
Whistleblowing Policy V.2	Amendment of the policy previously in force in the Bank, which required a detailed revision in light of the changes in key external and internal regulations as well as the Bank's renewed organisational and business structure	Board of Directors, 18 April 2019
Whistleblowing Policy V.3	Amendment of the policy previously in force in the Bank in order to include the new physical reporting channel ("letter box") and make certain changes of a formal nature	Chief Executive Officer , 4 February 2020
Whistleblowing Policy V.4	Updating of the document incorporating the new ICT tool for reporting breaches (@Whistleblowing)	Chief Executive Officer, 23 September 2020
Whistleblowing Policy V.5	Renaming of the document and updating of the definition of "reporting" in order to include parties outside the Bank	Chief Executive Officer, 17 December 2021
Whistleblowing Policy V.6	Updating of the document renaming the "Corporate Body with a control function" and providing timeframes within which to deliver feedback to the reporting person	Chief Executive Officer, 26 January 2023
Whistleblowing Policy V.7	Updating of the document incorporating the regulatory changes introduced by Legislative Decree 24/2023 and the modification of the channels for reporting violations	Board of Directors, 13 July 2023

Contents

1 PURPOSE

The aim of this Policy is to determine the aspects of a legislative, regulatory, procedural and organisational nature of the Whistleblowing system that the Group intends to govern in accordance with the regulatory provisions of reference, detailed in paragraph 3 below.

This Policy also constitutes an implementation of the requirements of Legislative Decree no. 231/2001 (at paragraph2-bisof article 6) on reporting to the Supervisory Body.

2 GLOSSARY

Abbreviations	
ABI	Italian Banking Association
TUB	Consolidated Law on Banking
TFUE	Treaty on the Functioning of the European Union
TUF	Consolidated Law on Finance
OdV	Supervisory Board
ANAC	Anticorruption National Authority

Definitions	
DECREE	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 laying down provisions on the protection of persons who report breaches of national laws.
PUBLIC DISCLOSURE	Making information about breaches publicly available through the press or electronic media or otherwise through means of dissemination capable of reaching a large number of people.
FACILITATOR	A natural person who assists the Whistleblower in the reporting process, operating within the same work context and whose assistance must be kept confidential.
ORGANISATIONAL STRUCTURES (OR STRUCTURES)	The types of organisational structure of which illimity's Organisation Chart is composed in which the detailed responsibilities are assigned as described in the "Organisational Structure Regulation".
PERSONNEL	Pursuant to article 1, paragraph 1h-novies of the TUB, "personnel" shall mean "employees and those persons who in any case operate on the basis of relations that determine inclusion in the business organisation, also by a means other than a permanent employment contract".
RETALIATION	Any conduct, act or omission, even if only attempted or threatened, committed by reason of the report, the complaint to the judicial or accounting authorities or public disclosure and which causes or may cause the

	Whistleblower or the person who made the report, directly or indirectly, unfair harm. By way of example, the following are forms of retaliation: • dismissal or suspension; • demotion or withholding of promotion; • transfer of duties; change of location; reduction in wages; change in working hours; • withholding of training; • imposition or administering of any disciplinary measure, reprimand or other penalty, including financial penalty; • coercion, intimidation, harassment or ostracism; • failure to renew or early termination of a temporary employment contract; • discrimination, disadvantageous or unfair treatment.
REPORTED PERSON	Person to whom the Whistleblowing breaches or public disclosure refer.
REPORTING PERSON	Person reporting a breach or a public disclosure who belongs to one of the following categories: • employees of illimity Bank S.p.A. and those persons operating on the basis of relations that determine inclusion in the business organisation, also by a means other than a permanent employment contract; • shareholders and persons with administrative, management, supervisory or representative functions.; • employees of other Group companies and those operating on the basis of relations that determine inclusion in the business organisation of these companies; • non-employee workers (e.g. freelancers and consultants) who provide goods or services to the company.
WHISTLEBLOWING	Communication made by a Whistleblower concerning a violation (including a well-founded suspicion of committing thereof) that may be submitted through the internal reporting channels adopted by the Company, through the external channel activated by the National Anticorruption Authority or publicly disclosed.

VIOLATION	Conduct attributable to: • administrative, accounting, civil or criminal offences; • offences under Legislative Decree No. 231 of 8 June 2001, or non-compliance with organisation and management models; • offences falling within the scope of Union law, relating to specific sectors (by way of example: financial services, products and markets and prevention of money laundering and financing of terrorism; environmental protection; protection of privacy and personal data; security of networks and information systems); • acts or omissions affecting the financial interests of the European Union; • acts or omissions concerning (Art. 26 section 2 TFEU) the free movement of goods, persons, services and capital in the internal market, including violations of European Union competition rules, State aid, corporate taxation; • acts or conduct that frustrate the object or purpose of European Union provisions.

3 LEGISLATIVE AND REGULATORY REFERENCES

Legislative Decree No. 24 of 10 March 2023 in implementation of Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 brings together in a single legal text the entire discipline of how to report (Whistleblowing), including the related protections, violations of national or European Union regulatory provisions that harm the public interest or the integrity of the public administration or private entity, of which the Whistleblower has become aware in a public or private employment context. In addition, on the same subject, reference should be made to Consob Resolution no. 20249 of 28 December 2017[1], Bank of Italy Circular No. 285 "Supervisory Provisions for Banks" (Part I, Title IV, Chapter 3, Section VIII), as well as Articles 52 bis and 52 ter of the Consolidated Banking Act (TUB) and subsequent provisions issued on the subject.

Concerning the role of the corporate bodies connected with the situations of Whistleblowing procedures reference should also be made to the ABI Guidelines of 28 October 2015 on “Detailed analyses for setting up an internal Whistleblowing system”.

As far as the Administrative Responsibility of Legal Persons is concerned, it should be noted that the aforementioned Decree stipulates that an entity’s Organisation Model must provide for one or more channels that enable to submit, as protection of the integrity of the entity itself, a detailed report on unlawful conduct relevant pursuant to Legislative Decree no. 231/2001 based on precise and concordant factual items or breaches of the Organisation Model adopted by the entity.

[1] Regulation on provisions implementing Legislative Decree no. 58 of 24 February 1998 on market matters (article 60-bis).

4 SCOPE OF APPLICATION

This Policy, concerning the internal system for reporting breaches, is applicable to all Group companies, which must incorporate the provisions of this Policy into their internal rules and regulations and make an appropriate distribution of these provisions to all of their staff.

4.1 Objective scope of application

Pursuant to Legislative Decree No. 24/2023, the report must relate to any breach attributable mainly to:

- administrative, accounting, civil or criminal offences;
- relevant offences pursuant to Legislative Decree no. 231 of 8 June 2001, or violations of organisation and management models;
- national and/or European regulations applicable to the Bank's activities, such as acts and omissions relating to consumer protection, competition, State aid, personal data protection, and network and information system security.

Pursuant to article 52-bis, paragraph 1 of the TUB, the report may also regard any action or fact that constitutes a breach of the laws and regulations governing banking activity.

A number of examples (not comprehensive) of areas to which said laws and regulations relate, which are accordingly susceptible to reporting, are set below in order to provide practical details of the scope of application of this Policy:

- breaches of internal and external regulations that govern the activity of illimity Bank S.p.A. or other Group companies, including those contained in the Bank's Organisation, Management and Control Model, as well as the principles and rules of conduct contained in its Code of Ethics (illimity way);
- unlawful or fraudulent conduct, carried out by employees, members of the corporate bodies or third parties (suppliers, consultants, collaborators, financial promoters or Group companies) that may, directly or indirectly, cause damage to the Group's results or net assets and/or to its image;
- criminal offences committed by employees, members of the corporate bodies or third parties (suppliers, consultants, collaborators, financial promoters or Group companies) to the detriment of the Bank or which may lead to a liability for the Bank;
- any conduct that gives rise to conflicts of interest, adopted without full compliance with the rules and procedures of control envisaged for such situations (such as for example the conflict of interest of an employee in a lending transaction in which he or she has a personal interest).

Any reporting based on interpersonal questions which follows the traditional channels (for example line supervisor, the human resources function) is excluded from the admissible cases.

In addition, pursuant to Legislative Decree no. 231/2001, reporting must regard unlawful conduct or breaches of the Bank's Organisation Management and Control Model that are detailed and based on precise and concordant items.

4.2 Subjective scope of application

Reports and/or public disclosure may be made by:

- the employees of illimity Bank S.p.A. and those who work on the basis of relationships that determine their inclusion in the company organisation, even in a form other than an employment relationship;
- shareholders and those who perform functions of administration, management, control, supervision or representation of illimity Bank S.p.A;
- workers employed by other companies of the Group and those who work on the basis of relationships that determine their inclusion in the corporate organisation of these companies;
- non-employee workers (e.g. freelance professionals and consultants) who provide goods or services in favour of the Company.

5 THE ROLE OF THE CORPORATE BODIES AND STRUCTURES INVOLVED

5.1 The corporate body responsible for strategic supervision

The corporate body responsible for strategic supervision:

- establishes and approves the internal system designed to enable actions and facts that may constitute a breach of the norms governing banking activity to be reported;
- after obtaining the opinion of the corporate body responsible for control, appoints the Head of the internal system for reporting breaches;
- after obtaining the opinion of the corporate body responsible for control, receives and approves the annual report containing aggregate information on the results of the work performed by the Head of the internal system for reporting breaches as a consequence of the reporting received;
- encourages the use of internal reporting systems and fosters the dissemination of a legality culture by delegating the Head of the internal system for reporting breaches to arrange training and the provision of information for personnel.

5.2 The corporate body with a control function

The corporate body with a control function:

- oversees the proper functioning of the internal system for reporting breaches;
- obtains periodic information from the Head of the internal system for reporting breaches on any reporting of breaches received;
- expresses its opinion to the corporate body responsible for strategic supervision on the appointment of the Head of the internal system for reporting breaches;
- expresses its opinion to the corporate body responsible for strategic supervision on the annual report containing aggregate information on the results of the work performed by the Head of the internal system for reporting breaches as a consequence of the reporting received.

5.3 Head of the internal system for reporting breaches

The Head of the internal system for reporting breaches (hereinafter also the “Head of Whistleblowing”) is appointed by the body with a strategic supervision function on the basis of the following characteristics:

- he is not hierarchically or functionally subordinate and accordingly reports directly to the corporate bodies;
- he does not perform operational duties;
- he does not participate in the adoption of any decision-making provisions resulting from the reported breaches, which are remitted to the competent corporate functions or bodies.

The Head of the internal system for reporting breaches:

- examines and assesses the reports of breaches received;
- ensures the procedure for reporting breaches has been correctly followed;
- where relevant reports the information reported to the corporate bodies directly and without delay;
- guarantees the confidentiality of the information received;
- ensures the confidentiality of the reporting person and the person alleged to be responsible for the breach, without prejudice to the rules governing investigations or proceedings initiated by the judicial authorities in relation to the facts to which the reporting relates;
- provides suitable protection for the reporting person against retaliatory, discriminatory or in any case unfair conduct as a result of the reporting;

- in accordance with legislation on personal data protection draws up an annual report on the proper functioning of the internal reporting system containing aggregate information on the results of the work performed as a consequence of the reporting received, which is approved by the corporate bodies and made available to the Bank's staff;
- is continuously trained in relation to the management of the reporting channel and takes care of the training of the Bank's staff, describing in a clear, precise and complete manner the internal procedure for reporting adopted, indicating the controls put in place to ensure the confidentiality of the reporting person's personal data; looks after the maintenance of the ICT reporting tool (called "@Whistleblowing") provided by BDO Italia S.p.A. and on a regular basis checks that it continues to function properly.

5.4 The Supervisory Body

The Supervisory Body has a complete view of any reporting through the @Whistleblowing tool and can decide whether to initiate an assessment procedure or dismiss the case, documenting the reasons for the decision in the minutes of the meeting at which the report is discussed.
If the Supervisory Body decides to carry out an assessment or go into further detail, it minutes whether the assessment activities will be performed with the support of certain specific business functions or instead by using the services of external resources (for example consultants, forensic analysts, technicians, private investigators).
On completion of the assessment or after going into further detail, and on the basis of the results of such work, the Supervisory Body:

a. dismisses the case if the reporting turns out to be unfounded;
b. calls for further work to be done;
c. provides the functions concerned with its recommendations;
d. assesses, together with the competent business functions, the need for any disciplinary measures to be taken against the persons involved and any steps required to protect the Group's interests.

6 PROCEDURE FOR REPORTING BREACHES

6.1 Reporting through internal channels

The person reporting the alleged breach must forward his report – either anonymously or bearing his name – by the following means:

- using the ICT tool @Whistleblowing (accessible via web at the address **https://digitalroom.bdo.it/illimitybank**), through which he receives an immediately confirmation of report's receipt and a unique code required for monitoring the state of progress of the report processing. The Head of Whistleblowing views the reports received on the dashboard included in the tool to which the members of Audit and Internal Control Committee and Supervisory Body of the reporting person's reference company have access (in reading mode only). If the report regards the Head of Whistleblowing, an "alternative" operating process is envisaged under which the report is visible (in reading/writing mode) to the Chairman of the Audit and Internal Control Committee and (in reading mode only) to the other members of the Committee as well as to the members of the Supervisory Body. In this case, the activities for which the Head of Whistleblowing is usually responsible must be performed by the Chairman of the Audit and Internal Control Committee;
- by way of sending a paper letter addressed to the Whistleblowing Officer, which must also contain a non-company email reference in order to send confirmation of receipt of the report and to allow monitoring of its processing status. The Whistleblowing Manager then proceeds, within seven days of receipt of the report, to census the report in a special section of the @Whistleblowing IT tool, including the email reference provided by the Whistleblower. At the end of the census, the tool will automatically send confirmation of receipt of the report as well as the unique code needed to monitor the progress of the report processing;
- by calling the telephone number (+39) 0282849697 (not subject to a registration procedure) manned

by the Whistleblowing Manager, who transcribes the report and, within seven days of the telephone call, sends it to the Whistleblower by email to the address provided by himself so that he may verify, correct and confirm the content. After confirming the content, the Whistleblowing Manager proceeds to record the report in a special section of the @Whistleblowing IT tool, including the email reference provided by the Whistleblower in order to allow the automatic sending of a unique code necessary to monitor the progress of its processing.

Any reports received in written form by other offices of the Bank must be forwarded by them to the Whistleblowing Officer within three days of their receipt. In such a case, the Whistleblowing Officer tracks the report in the same way as for the handling of paper reports.

The report must contain a detailed description of the facts and the conduct considered in breach of the regulations, also indicating, where possible, the documents, the rules that are considered to have been breached and other items useful for making a determination of the disputed facts. In addition, the reporting person is required to state whether he has a personal interest in making the report.

The @Whistleblowing tool ensures that it is impossible to hide or eliminate a report that has been sent, and its content constitutes the register of reports.

The Head of the internal system for reporting breaches, the corporate body with a control function and the Supervisory Body are jointly involved in guaranteeing:

- retention of the documentation regarding the reports and the relative checks as well as the provisions on any decisions taken by the competent functions in appropriate hard copy/ICT files, ensuring suitable levels of security/confidentiality;
- storage of the data concerning the reports for a period of time not exceeding five years, starting from the date of the communication of the final outcome of the reporting procedure, and the use of such data in accordance with the purposes for which the data were originally collected and subsequently processed, and in any case in compliance with applicable personal data protection laws and regulations[2].

The Bank reserves the right to inflict specific penalties on the reporting person, where possible, if the related reports are made with wilful misconduct or gross negligence or if they should turn out to be false, unfounded, with defamatory content or in any case carried out with the sole purpose of harming the Bank, the reported person or other parties affected by the report. The Bank may additionally take the appropriate initiatives in a court of law. Excluding cases of responsibility for libel and defamation, or for the same pursuant to article 2043 of the Italian Civil Code, the existence of a report as part of the procedure referred to in paragraph 1 does not constitute a breach of the obligations deriving from an employment relationship[3].

The report is acquired by the Head of the internal system for reporting breaches, who immediately initiates an analysis procedure, also using the collaboration of Internal Audit resources and other departments within the Bank as well as external resources (e.g. consultants, forensic analysts, technicians, private investigators). All investigations must be conducted on a timely basis, without continuing for longer than is reasonably necessary given the subject of the report. The investigation must be conducted with impartiality and independence. No person with a conflict of interest may be involved in the enquiries or decision-making process, nor anyone who might be responsible for the failure to adopt measures designed to prevent or detect the alleged breaches. Current or potential conflicts of interest must be promptly reported by any persons involved in the investigations to the Head of Whistleblowing or to the Chairman of the Management Control Committee if the Head of Whistleblowing finds himself in a situation of conflict of interest. The outcome of the investigation will be communicated to the reporting person within a period not exceeding three months from the acknowledgment of receipt.

The investigations are performed with the utmost confidentiality at all levels, from the receipt of the report to the completion of the procedure. Confidentiality applies to the facts under investigation, to the person(s) involved or mentioned, to the subject of the report, to the procedure being followed, to the materials and information gathered and to the results of the procedure. The persons involved in the investigations must not disseminate information to anyone not directly involved in such investigations.

[2] Legislative Decree no. 196 of 30 June 2003, as amended by Legislative Decree no. 101 of 10 August 2018; Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (articles 5, 15 and 23).
[3] Article 4-undecies of the TUF.

The procedure adopted by the company ensures the confidentiality of the personal data of the reporting person and the person allegedly responsible for the breach, in accordance with the requirements of privacy laws and regulations, without prejudice to the rules governing any investigations or proceedings initiated by the judicial authorities in respect of the facts contained in the reporting. The parties receiving, examining and assessing the reports, the Head of the internal system for reporting breaches and any other person involved in the process are required to ensure the confidentiality of the information received, also with respect to the identity of the reporting person who, in any case, must be suitably protected from retaliatory, discriminatory or in any case unfair conduct as a result of the reporting.

If, subsequent to further detailed analysis, the report turns out to be unfounded, it will be filed and no further action of any kind will be taken. On the other hand, if a breach is discovered, the Head of the internal system for reporting breaches immediately informs the corporate body with a control function, the corporate body responsible for strategic supervision, the Supervisory Body and any organisational unit involved about this, as well as informing the reporting person and possibly also the reported parties, also for the purpose of identifying and deciding on the most appropriate measures to be taken, in accordance with the requirements of the company's disciplinary system in force at the time, and to inform the authorities if there is a legal requirement in that sense. In either case, at the end of the procedure the reporting person is informed that the procedure has been concluded.

The above-mentioned systems are structured in such a way as to ensure that reports are received, examined and assessed by way of specific, autonomous and independent channels that are separate from ordinary lines of reporting. To this end, due to the way they are configured (ICT channel, paper and oral channel), the internal reporting systems ensure the availability of an alternative channel for the reporting person, guaranteeing that the person in charge of receiving, examining and assessing the report is not hierarchically or functionally subordinate to any reported person, is not the person allegedly responsible for the breach and does not have a potential interest linked to the reporting that may compromise the impartiality and independence of his judgement. If the reporting person is jointly responsible for the breaches, it would be better if he were to receive privileged treatment compared to the other jointly responsible persons, compatible with the applicable discipline.

In any event, Circular no. 285 of the Bank of Italy of 17 December 2013 requires that the persons responsible for receiving, examining and assessing the reports should not participate in the adoption of any decision-making provisions, which are remitted to the competent corporate functions or bodies.

6.2 Reporting through external channels

In accordance with the legislation in force, the Whistleblower may make an external report to the National Anti-Corruption Authority (ANAC) if:

- he/she has already made an internal report that was not followed up;
- there are reasonable grounds for believing that, if he/she made an internal report, it would not be effectively followed up or that he/she might be subject to retaliation;
- has reasonable grounds to believe that the breach may constitute an imminent or obvious danger to the public interest.

The reporting procedures are defined by ANAC and published on its website.
The Whistleblower may also report, pursuant to Article 52 - ter of the Consolidated Banking Act (TUB), possible Regulatory violations or alleged management irregularities concerning banking activities through the external reporting channel activated by the Bank of Italy in accordance with the procedures published on its website.
Finally, the Whistleblower has the option of making the report through public disclosure, benefiting from the protection provided by the Decree if one of the conditions set out therein is met.

7 MEASURES TO PROTECT THE PERSONS INVOLVED

7.1 Confidentiality of the personal data

The Bank puts suitable controls in place to ensure the confidentiality of the personal data of the reporting person and of the person allegedly responsible for the breach.

The information and any other item of personal data acquired in applying these rules are processed in full compliance with Legislative Decree no. 196 of 30 June 2003, Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and any subsequent measures on the subject

("Privacy Legislation").

More specifically personal data processed for the purpose of these rules must be:

- restricted to data strictly and objectively necessary for checking the validity of the reporting and for managing this;
- processed lawfully and properly;
- retained for a period not exceeding five years from the date of communication of the final outcome of the reporting procedure, unless requested by the Judicial Authority

It should be noted that personal data which are clearly not useful for processing a specific alert are not collected or, if accidentally collected, are deleted immediately.

The @Whistleblowing platform, as well as in the appropriate section of the website which is available to the reporting and reported person, contains information on the protection of the personal data processed in application of these rules.

The identity of the reporting person is not applicable and that this can only be revealed with their consent and when the knowledge is essential for defending the reported person; in this case, the reporter receives a written communication containing the reasons for the disclosure of the data.

The reported person must in any case be informed with a reasoned communication – unless the communication may jeopardise the purpose of the limitation – that the exercising of his rights may, in any case, be delayed, restricted[4] or excluded for the time period and to the extent that this constitutes a necessary and proportionate measure, given his basic rights and legitimate interests, in order to safeguard the interests of the reporting person and the investigation procedure itself. The data and documentation relating to Whistleblowing, also acquired during investigations, are stored in the @Whistleblowing tool provided by the company BDO, which has been appointed as data controller pursuant to EU Regulation 2016/679 on the protection of personal data. In particular, the supplier has adopted appropriate technical and organisational measures to guarantee the confidentiality of the processed data certified according to the ISO/IEC 27001 standard, including the use of encryption tools and the performance of vulnerability & penetration testing activities aimed at identifying any weaknesses in the tool that could be exploited by attackers.

7.2 Protecting the reporting person

The Bank provides appropriate protection for the reporting person "against retaliatory, discriminatory and in any case unfair conduct as a result of the reporting", in a climate of respecting the dignity of such.

illimity Bank safeguards reporting persons against any form of retaliation, discrimination and penalisation and in all cases ensures full and complete confidentiality of their identity, excluding any legal obligations. Pursuant to Legislative Decree no. 24/2023:

- direct or indirect retaliatory or discriminatory action taken against the reporting person for reasons connected directly or indirectly with the reporting is forbidden. Retaliatory dismissal and organisational measures having direct or indirect negative effects on working conditions are null and void, unless it can be shown that they are not of a retaliatory nature and are based on reasons not connected with the reporting;
- any adoption of discriminatory measures can be reported to the national labour inspectorate;
- the internal disciplinary system envisaged by Legislative Decree no. 231/2001 is applicable in the event of:
    - breach confidentiality rules on the identity of the reporting person or the prohibition of discriminatory or retaliatory action;
    - the sending of a report is obstructed;
    - analysis and verification of the received reports are not carried out.

[4] The limitation of the exercise of rights is governed by Article 2-undecies of Legislative Decree No. 196 of 30 June 2003

The protection of the Whistleblower also applies if the report or public disclosure is made when the legal relationship has not yet started or after its termination.

Facilitators and persons working in the same employment context who have a habitual or family relationship with the Whistleblower also benefit from the aforementioned protections.

8 ANNEXES

8.1 ANNEX 1: RELATED LEGISLATION AND REGULATIONS

INTERNAL RELATED REGULATIONS

Organisation, Management and Control Model
illimity Way

EXTERNAL RELATED LEGISLATION AND REGULATIONS

Legislative Decree no. 24 of 10 March 2023
Legislative Decree no. 231 of 8 June 2001
Circular no. 285/2013 of the Bank of Italy
Regulations on the implementation of Legislative Decree No. 58 of 24 February 1998 on markets