



WHISTLEBLOWING CHANNEL REGULATIONS

COLONIAL GROUP

Tracking of changes			
Version	Date	Supervisory body	Description
1.0	2011	RCU	Design and initial implementation of the Whistleblowing Channel as an essential element of the Compliance and Criminal Risk Prevention Model
2.0	2021	RCU	Update of the standard as per the recommendations of the Audit and Control Committee

Related regulations
Criminal Compliance Policy
Code of Ethics
Compliance and Criminal Risk Prevention Manual

Table of contents

1. Introduction and Purpose	4
2. Subjective scope of the Whistleblowing Channel	4
2.1 Who should report and who can use the Whistleblowing Channel?	5
2.2 How can I report an incident?	5
2.3 Who can be reported via the Whistleblowing Channel?	5
3. Objective scope of the Whistleblowing Channel.....	5
4. Mechanism for reporting and submitting enquiries. How should or can a report or enquiry be submitted? Who manages them?	6
5. Requirements for the acceptance of notifications.....	6
5.1. Requirements for the acceptance of an enquiry.....	6
5.2. Requirements for the acceptance of a report and causes for rejection.....	6
6. Protection of the whistleblower and the reported party. Data Protection. Guarantees of the Whistleblowing Channel	7
6.1 Non-retaliation	7
6.2 Data protection. Confidentiality and eventual anonymity of the whistleblower.....	7
6.3 Incompatibilities and/or conflict of interest	8
6.4 The whistleblower's rights and duties.....	8
6.5 The reported party's rights	8
7. Procedure for processing enquiries and reports	9
7.1 Procedure for processing enquiries	9
7.2 Procedure for processing reports. Reporting. Receipt and acceptance. Follow-up.....	9
A) Reporting	9
B) Receipt and acceptance of the report.....	9
7.3 Investigating the reported events.....	10
7.4 Motion for a resolution	11
7.5 Decision of the measures to be adopted.....	12
7.6 Implementation of the measures adopted	12
7.7 Special procedure to process mobbing and sexual or gender-based harassment reports.	12
7.8 Special procedure in the event of a report concerning a member of the RCU	12
8. Registration and Filing.....	13
9. Principles of conduct and security measures	13
Appendix I - Conducts that can be reported through the Whistleblowing Channel	14
Appendix II - Privacy Policy.	17

1. Introduction and Purpose

The need to preserve the reputation and prestige of Inmobiliaria Colonial, SOCIMI, S.A. (“**Colonial**”), as the parent company of the Colonial Group¹ (“**Group**” or “**Colonial Group**”), requires all employees and partners acting for and/or on behalf of Colonial to do so at all times abiding by and in compliance with (i) current legislation, (ii) the Code of Ethics, and (iii) any internal policies and procedures. In addition, employees and partners have the Whistleblowing Channel at their disposal, which they must use should they become aware of any behaviour breaching any of the above.

On the other hand, the cooperation of all suppliers, contractors and subcontractors in detecting possible misconduct is also of great importance. For that reason, the Whistleblowing Channel is also at their disposal.

The purpose of the Whistleblowing Channel Regulations (hereinafter, the “**Regulations**”) is to regulate the actions and steps to be taken by the Regulatory Compliance Unit (“**RCU**”) as the body in charge of managing the Whistleblowing Channel when handling the enquiries and reports received, as well as the rights and duties of those using it. In any case, the RCU will periodically report to the Audit and Control Committee.

Therefore, in line with Colonial’s ethical and compliance culture, the Channel is at our stakeholders’ (both internal² and external³) disposal for two types of notifications:

- **Reports:** these are reports of potential irregularities or non-compliance which could entail a breach of regulations, especially criminal, accounting, money laundering or workplace/sexual harassment regulations, or a breach of the Code of Ethics, its implementing provisions, or other internal Colonial regulations that may be applicable in each case.
- **Enquiries:** these are requests for clarification of specific doubts on the implementation or interpretation of internal and external regulations in force, including doubts about the operation of the Whistleblowing Channel or any other applicable regulations.

These Regulations apply to the Colonial Group in Spain, regardless of the region, and have been drawn up according to Spanish and European data protection regulations.

2. Subjective scope of the Whistleblowing Channel

The Whistleblowing Channel is a tool made available to certain groups, in accordance with the following subsection, to make enquiries or report any irregularities which they become aware of and which fall within the objective scope.

¹ Colonial Group is the set of companies of which Colonial is a majority shareholder and/or that are directly or indirectly controlled by Colonial in Spain.

² Internal stakeholders refer to all employees, interns, volunteers, directors, senior management, legal representatives and de jure or de facto directors of the Colonial Group, as well as shareholders.

³ External stakeholders are suppliers, contractors and subcontractors.

2.1 Who should report and who can use the Whistleblowing Channel?

All employees, directors, shareholders, suppliers, contractors and subcontractors can enquire and must report through the Whistleblowing Channel, without fearing retaliation, any irregularities of which they become aware and fall within the objective scope of the Regulations.

Where appropriate, these groups will be referred to interchangeably as the “**Parties Concerned**”.

2.2 How can I report an incident?

- Employees and directors may report an incident either in their name or anonymously. However, they are encouraged to report in their name since confidentiality of the reporting party is guaranteed under these Regulations.
- Shareholders, suppliers, contractors, and subcontractors may report in their name, i.e., by identifying the user of the Whistleblowing Channel. However, Colonial guarantees the confidentiality of the reporting party under these Regulations.

2.3 Who can be reported via the Whistleblowing Channel?

Any Colonial Group employee or director who has committed, is committing or is about to commit an irregularity or who engages in any of the conducts that fall within the objective scope described hereunder may be reported.

3. Objective scope of the Whistleblowing Channel

The applicable objective scope of the Whistleblowing Channel includes the following conducts, which are also listed in **Appendix I**:

- Failure to comply with any external regulations in force in accordance with the applicable legislation of the country where the irregularity has allegedly been committed.
- Conducts that may be considered accounting offences, or which contravene accounting and financial regulations, as well as regulations on the prevention of money laundering and the financing of terrorism.
- Conducts defined in the Criminal Code and criminal offences under other special laws that may give rise to criminal liability, including that of Colonial, in accordance with the applicable legislation.
- Conducts contrary to the principles and rules of conduct set out in Colonial Group’s Code of Ethics and other internal regulations applicable to its Staff.

The reported events may be in the past, present or future. No evidence is required to file a report. A well-founded suspicion will suffice, provided that the report is filed in good faith.

4. Mechanism for reporting and submitting enquiries. How should or can a report or enquiry be submitted? Who manages them?

Enquiries and reports should preferably be submitted through the platform designed for this purpose and accessible on the Colonial website: <https://www.inmocolonial.com/responsabilidad-social>

The platform has been internally developed, ensuring the highest levels of confidentiality and independence, and the party concerned can rest assured that any communication received will be processed.

The RCU is the body in charge of receiving and processing the enquiries and reports through the platform in accordance with these Regulations. In addition, the RCU is in charge of processing and managing any other incidents that come to its attention via any other means, with legal advice and assistance from an external advisor if necessary. Notwithstanding the foregoing, any reports that are classified as sexual or workplace harassment will be referred to and handled by the committee created by Colonial for that purpose.

5. Requirements for the acceptance of notifications

5.1. Requirements for the acceptance of an enquiry

Enquiries must be related to the regulations, their interpretation or implementation, in accordance with the list in Section 3. In addition, enquiries must be submitted indicating the enquirer's name and will not be accepted if they don't meet these requirements or if they deal with general issues.

5.2. Requirements for the acceptance of a report and causes for rejection

Reports will be accepted provided that they meet, cumulatively, the following requirements:

- The report is submitted by the persons listed in Section 2.
- The reported party must be one of those listed in Section 2.
- The reported incident is listed in Section 3.

The following may be grounds for the rejection of a report:

- Reports submitted by or regarding groups other than those foreseen as parties concerned in the Whistleblowing Channel (e.g., Reports by clients or regarding clients will not be accepted as there is a specific channel for this purpose).
- Reports submitted by proxies (e.g., an employee reporting on behalf of another employee).
- Reporting incidents that are not reportable because they do not entail any wrongdoing or an ethical breach (e.g., "I am not happy at work", "my colleague isn't clean", etc.).

- Reports which are blatantly made in bad faith⁴.
- Reports not based on concrete or specific suspicions or indications (e.g., “I don’t trust X’s performance”).

6. Protection of the whistleblower and the reported party. Data Protection. Guarantees of the Whistleblowing Channel

6.1 Non-retaliation

Parties concerned who make an enquiry or report are protected from any form of retaliation, threat, extortion, discrimination, or penalty as a result of their reporting, provided that these are made in good faith. Colonial will sanction any form of retaliation against a party concerned who acted in good faith.

The prohibition of retaliation provided for in the preceding paragraph shall not prevent the adoption of appropriate disciplinary measures when the internal investigation establishes that the reporting is false and that the party concerned was aware of said falsity, hence having acted in bad faith.

6.2 Data protection. Confidentiality and eventual anonymity of the whistleblower

This Whistleblowing Channel is set up with full respect for the different legally established Data Protection requirements in order to duly protect the privacy of the persons involved and, in particular, to guarantee the confidentiality of whistleblowers. In this regard, the Data Protection Officer will ensure continuous compliance and may rely on external expert advice for this purpose.

Furthermore, when designing this Channel, Colonial has also taken into account specific elements of Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons who report breaches of Union law.

Accordingly, reports may be filed through this Channel either anonymously or in one’s own name, according to the type of party concerned and their relationship with Colonial. In this case, Colonial will guarantee the whistleblower’s confidentiality by ensuring, among other measures, that the exercise of the right of access by the reported party does not entail access to the whistleblower’s identity. Thus, except in expressly regulated cases, the reported party will not know the whistleblower’s identity.

However, all whistleblowers are encouraged to identify themselves to obtain more information about the reported events. In any case, the identity of whistleblowers who identify themselves shall be kept strictly confidential.

Furthermore, (i) any persons who, due to the functions they perform at Colonial, have access to any reports submitted, (ii) the RCU members, or (iii) external advisors, are expressly obliged to keep the whistleblower’s identity secret as well as any other information they may be aware of within the framework of the Whistleblowing Channel.

⁴In this regard, it should be noted that, in accordance with the provisions of Article 456 et seq. of the Spanish Criminal Code, an accusation, a false report, and the simulation of crimes are considered crimes, punishable by a prison sentence of up to two years.

In any case, the specific Privacy rules applicable to this Channel are those found in the “**Privacy Policy of the Whistleblowing Channel**”, attached hereto as **Appendix II**.

6.3 Incompatibilities and/or conflict of interest

In the event that anyone involved in a report is related, by blood or marriage, to a person in charge of processing, investigating or resolving the reported case, the latter will be disqualified from intervening, in accordance with Section 7.8.

6.4 The whistleblower's rights and duties

The **whistleblower's rights** are:

- The right to non-retaliation provided that he/she is acting in good faith, as described in Section 6.1.
- The right to confidentiality and anonymity, as described in Sections 2.2 and 6.2.
- The right to be informed about the acceptance or rejection and the outcome of the investigation, if applicable.
- In addition to all the legally established rights regarding personal data found in the Privacy Policy of this Whistleblowing Channel.

On the other hand, the **whistleblower's duties** are:

- Acting in good faith.
- Providing any information and documents available relating to the events being reported.
- Duty of confidentiality: as far as possible, strict confidentiality is required when handling the report.

6.5 The reported party's rights

- The right to be informed of the report made against him/her as soon as the appropriate checks have been carried out and the case has been accepted. In the event of rejection, informing the reported party will be optional.

As a general rule, Colonial will inform reported parties whenever a report is made against them within one month of receipt. However, in exceptional cases and providing there is a just cause, informing the reported party may be delayed for a further two months (i.e., a maximum of three months in total), or the reported party may not be informed at all if doing so could seriously jeopardise the success of the investigation.

- The reported party also has the right of access to his/her personal data and to the events that have been reported, except for the whistleblower's identity and any other persons concerned by the case.

- If applicable, the right to be informed of the resolution of a report which has been admitted and investigated.
- Finally, the right to all the legally established rights regarding personal data found in the Privacy Policy of this Whistleblowing Channel.

7. Procedure for processing enquiries and reports

7.1 Procedure for processing enquiries

When an enquiry is received through the platform, the RCU will resolve it in writing within 7 business days, where possible, unless more time is necessary for justified reasons. To resolve a query, the RCU will receive the support or advice of other Colonial departments or external experts whose participation is deemed essential by the RCU to provide a rigorous and adequate response within a reasonable time.

7.2 Procedure for processing reports. Reporting. Receipt and acceptance. Follow-up

A) Reporting

The report is generated once the form has been filled out and hosted on the platform.

B) Receipt and acceptance of the report

Once the report has been registered, the RCU receives an email notification about the new report, which will have been assigned a file number, regardless of whether the report is subsequently rejected or closed.

The RCU will then access the Channel platform to perform an initial evaluation of the reported events and decide whether it initiates the corresponding investigation or rejects the report, as the case may be. The following could therefore occur:

- **Rejection of the report:** if the report does not meet the established formal requirements or if one of the grounds for rejection set out in Section 5 is met.
- **Acceptance of the report and launching of the investigation:** if the filed report meets all the established formal requirements and the reported events are relevant, the RCU will accept the report and launch the investigation.

In any case, the RCU will contact the whistleblower acknowledging receipt within **7 business days** of the reception thereof, unless more time is required for justified reasons. Should the whistleblower decide to report anonymously and not provide a mean of contact, said acknowledgement of receipt would not be possible.

In addition, any person who has been reported, except when the report is rejected, shall be informed of the following:

- receipt of the report;
- the alleged events which have raised the concern;

- the action to be taken by the RCU;
- the processing of their personal data, the purpose of said processing, and the persons who will have access to said data.

In exceptional cases, should the RCU consider that notifying the reported party may jeopardise the investigation, such notification may be postponed until such risk no longer exists. In any case, the deadline to inform the reported party shall not exceed **one month** from the report receipt, with the possibility of extending the deadline to a maximum of **three months** if there are justified reasons for doing so. This is without prejudice to the fact that the law may expressly and bindingly establish different deadlines, in which case these will prevail.

7.3 Investigating the reported events

Should the investigation be launched, the RCU will appoint one of its members (who may not be involved in the reported events, in which case, see Section 7.8) to conduct the necessary investigation to confirm the veracity of the alleged behaviour. This member may entrust an external advisor with these and other functions to ensure greater confidentiality and independence. The investigation will seek to resolve the following issues:

- What the reported conduct entails;
- To whom the conduct refers;
- When said conduct took place;
- To what extent the irregular conduct is linked to the breach of internal regulations;
- The consequences of the irregular conduct and, in particular, whether it may give rise to liability, including criminal liability, for Colonial or any of its professionals, whether Staff or Third Parties.

In this sense, the report processing procedure, regardless of its nature, shall be governed by the following principles, which must be observed and respected at all times by the RCU, as well as by any external person involved in the investigation:

- Ensure the reliability of the evidence and compliance with current legislation, in particular, respect for the reported party's rights.
- Ensure confidentiality and protection of the privacy and dignity of the persons concerned, guaranteeing, in any case, the preservation of the whistleblower's identity and personal circumstances.
- If necessary, prioritise and urgently process the report.
- Comprehensive investigation of the events, which should be led, if necessary, by expert professionals.
- Ensure action is taken, by adopting the necessary measures, including, where appropriate, disciplinary measures, against the person or persons whose irregular conduct is proven, specifically harassment, as well as anyone who makes a false accusation or report in bad faith.
- Protection against retaliation, ensuring that whistleblowers do not suffer any adverse or negative treatment as a result of reporting an incident to initiate this procedure (without prejudice to any disciplinary action that may be taken in the event of false reporting).
- Ensure that the victim of harassment can continue working under the same conditions if they so wish.

In any case, anyone involved in the investigation is obliged to keep professional secrecy regarding the information to which they may have access while processing the case. Failure to comply with this obligation may result in penalties.

In compliance with the principles and guarantees listed, the RCU will conduct the necessary investigation to confirm the veracity of the reported conduct. To this end, it may, with due regard for the rights of the persons concerned, use any means necessary, and in particular the following:

- Meeting with the whistleblower: whenever possible, for non-anonymous reports, it is advisable to meet with the whistleblower in a private place to explain the investigation process and, in particular, the prohibition of retaliation for any reporting made in good faith. The minutes of each meeting shall be drafted and must be signed by all the attendees.
- Meeting with the reported party: must be held as soon as possible after gathering the necessary information from other sources. The minutes of each meeting shall be drafted and must be signed by all the attendees.
- Meeting with witnesses: anyone who may have reliable information regarding the events under investigation. The minutes of each meeting shall be drafted and must be signed by all the attendees.
- Electronic documents and records: including emails, diaries, and files, provided they are found on corporate electronic media owned by Colonial and provided to employees for work-related purposes (e.g., corporate email, corporate telephone, etc.), in accordance with the applicable ICT systems and media policy.
- Hard copies: must be numbered with a unique number and stored securely, either physically or electronically. These can include: corporate policies and procedures, invoices, reports, expense settlements, performance appraisal, etc. If these documents are kept at the workplace premises for the exclusive use of the reported party (such as lockers, personal belongings, etc.), they shall be searched during working hours and in the presence of an employees' legal representative or, failing that, another employee.
- Security system records: such as video surveillance recordings, in accordance with the ICT systems and media policy and, in particular, policies regarding video surveillance in the workplace.

7.4 Motion for a resolution

Upon conclusion of the investigation, within a maximum period of 30 calendar days, the RCU member in charge of the investigation shall inform the other members of the outcome, and they will then proceed to vote on the closure of the proceedings, or failing that, the measures to be adopted in each case. A favourable vote of the majority of the RCU members is required and will then be put forward to the Audit and Control Committee for a final decision. The motion for a resolution must be drafted within 15 calendar days from the conclusion of the investigation.

The RCU shall resolve to close the proceedings and the actions undertaken when the reported events have not been sufficiently proven, or should a breach not exist, as described in the objective scope of the Whistleblowing Channel.

On the other hand, should the RCU consider the reported events to have been sufficiently proven, it shall issue a reasoned decision indicating the legal measures, of any kind, to be adopted (including, among others, disciplinary proceedings and improvements to the system to prevent similar situations in the future).

At any point during the procedure, the RCU may receive legal advice and assistance from an external adviser to assist in aspects related to the investigation (e.g., the initial description of the events, their classification, the investigation and enquiries to be conducted, or the adoption of the most appropriate disciplinary measures in each case).

7.5 Decision of the measures to be adopted

In order to ensure the objectivity and independence of the decision, the decision-making power shall in all cases rest with Colonial's Audit and Control Committee, which shall be duly informed by the RCU of the breach, the investigation outcome, and the motion for a resolution, whether it is a minor, serious, or very serious breach, as stated in the previous section.

In the event of the reporting of a minor breach, the RCU, in coordination with Human Resources, shall decide on the measures to be adopted.

7.6 Implementation of the measures adopted

The penalties or disciplinary measures adopted shall be implemented by Human Resources, and the RCU shall keep evidence of the implementation of such measures.

7.7 Special procedure to process mobbing and sexual or gender-based harassment reports.

When a harassment event of any kind is reported, it shall be submitted to Colonial's Harassment Committee for resolution in accordance with Colonial's Harassment Protocol, which is available on the corporate intranet.

7.8 Special procedure in the event of a report concerning a member of the RCU

If it is concluded, after reading the report or its preliminary analysis, that an RCU member is concerned in any way, either as a participant or collaborator, in the events being reported, as well as in the cases referred to in Section 6.3, the special procedure shall be activated. This procedure differs from the ordinary procedure only in terms of who participates in the processing of the report:

- **If the report concerns an RCU member:** that member shall refrain from taking part in the investigation and will be denied access to the Whistleblowing Channel regarding that specific report throughout the entire investigation, and another RCU member shall take charge of the investigation.
- **If the report concerns all RCU members:** the report will be immediately referred to the Human Resources Management, who shall be in charge of processing the report with the advice of an external and impartial third party.

Thereafter, the procedure will be the same as for reports that do not involve a member of the RCU, as outlined above.

8. Registration and Filing

All notifications (enquiries and reports), responses and related documentation received shall be duly registered and filed. The aforementioned documentation shall be kept for a minimum of 10 years to respond to any possible claims that may be made or to comply with any legal obligations that the Colonial Group may be required to fulfil. In any case, the preservation, blocking of personal data, and the applicable technical measures must comply with Colonial's internal regulations and the provisions of the Privacy Policy of the Whistleblowing Channel.

The RCU shall collect said documentation and keep it in its systems, always in compliance with personal data protection regulations and security measures in accordance with the internal regulations and the Privacy Policy of the Whistleblowing Channel.

9. Principles of conduct and security measures

The actions of the RCU and of those departments and persons involved in the investigation shall conform to the following constitutional principles and rights:

- The Right to Effective Judicial Protection
- The Principle of Presumption of Innocence
- The right to due process

The RCU will be responsible for the custody and filing of any reports received and shall ensure the implementation of all the necessary technical and organisational measures to safeguard the confidentiality and security of the data collected and to protect them from unauthorised disclosure or access, in accordance with the provisions of Title VIII of the Regulations implementing the Organic Law on Data Protection.

Appendix I - Conducts that can be reported through the Whistleblowing Channel

- a) Supplier-related conducts: breach of company procedures related to the selection, negotiation or monitoring of suppliers.
- b) Workplace and/or sexual harassment: any verbal or physical behaviour of a sexual or non-sexual nature that violates a person's dignity, creates an intimidating, degrading, or offensive environment.
- c) Misappropriation and diversion of resources: misappropriation of company-owned goods or services for private use or with intent to profit (directly or indirectly) from them.
- d) Money laundering: acquisition, possession, use, or transfer of assets, knowing that they originate from criminal activity.
- e) Financing of terrorism: making available assets or securities of any kind, intentionally, or knowing that they will be used to commit terrorist offences.
- f) Bribery: offering, promising, making gifts, doing favours, or providing compensation to authorities or public officials so that they may carry out, in the exercise of their duties, an act that is contrary to their duties and/or that will unlawfully benefit us. This also includes the reverse situation, namely, accepting an unlawful act by an official or authority because it apparently benefits us in exchange for a favour, compensation, gift, or benefit of any kind.
- g) Influence peddling: influencing by taking advantage of any situation arising from a personal relationship to achieve a decision that may directly or indirectly generate an economic benefit for the company.
- h) Illegal financing of political parties: providing donations or contributions to a political party, federation, coalition or group of voters contravening the provisions of Organic Law 8/2007 of 4 July on the financing of political parties (making donations to finance political parties in excess of €50,000).
- i) Embezzlement: causing damage to the assets of a Public Administration by infringing or exceeding the powers of administration over those assets.
- j) Corruption between private individuals: accepting, promising, offering or conceding directors, employees or collaborators of a corporation, company, association, foundation or organisation, an unjustified or unlawful benefit or advantage of any nature in exchange for an act that, apparently, favours us.
- k) Falsification of economic-financial information in brochures: falsification of the economic-financial information contained in brochures for the issue of any financial instruments or the information that the company is required to publish and disseminate in accordance with the securities market legislation.
- l) Accounting and auditing aspects: systematic recording and analysis of business and financial transactions that differ from generally accepted accounting practices (e.g., incorrect recording of income, expenses or assets, incorrect application of generally accepted accounting principles, illegal transactions, etc.).

- m) Disclosure of trade secrets: seizure, by any means, of data, written or electronic documents, software or other related objects to disclose a trade secret.
- n) Insider trading: breach or infringement of legal regulations relating to the securities markets and of Colonial's internal regulations regarding the securities market. Unauthorised use of corporate, client or supplier information.
- o) Conflict of interest: a situation in which an individual has sufficient personal interest that may condition the objective exercise of his/her professional duties (e.g., inappropriate relationships with vendors, corruption, inappropriate relationships with clients, selecting suppliers for subjective reasons, etc.).
- p) Against personal and family privacy: seizure, use, modification or disclosure of third-party personal data found in hard copies or electronic documents, or any other document or personal belongings, as well as unauthorised access to data contained in computer systems.
- q) Commitments to third parties (clients/suppliers): breach of agreements entered into with third parties or cheating to secure an agreement.
- r) Misleading advertising: offering or advertising services or products by making false claims or stating untrue characteristics thereof in a way that may cause serious and evident damages to consumers/clients.
- s) Falsification of contracts, reports or records: the alteration, invention or falsification of a document, contract or record, in whole or in part, to obtain some form of benefit or alter the content of the document, contract or record.
- t) Urban planning: carrying out unauthorised development, construction or building works on land intended for roads, green areas or public property, or on land which has legally or officially been recognised as having a landscape, ecological, artistic, historical or cultural value, or which has been considered to have special protection for one of those reasons.
- u) Environmental protection: breach of internal or external regulations regarding the environment.
- v) Obstruction of inspections: refusal to cooperate with the market inspecting authorities subject to administrative supervision.
- w) Retaliation: discriminatory actions by the company against anyone who reports possible irregularities in good faith.
- x) Safety: breach of requirements to safely perform the activity.

- y) Others: when the abovementioned definitions fail to describe the situation that you wish to report due to breaching an internal or external rule or Colonial Group's Ethical Code. Therefore, different types of reportable offences have been included as an example without limitation. However, whenever unlawful behaviour occurs or may occur, it is the staff's duty to report it to the RCU.

Appendix II - Privacy Policy.

Basic legal information (1st layer)

The personal data collected within the framework of this Whistleblowing Channel will be processed by Inmobiliaria Colonial, SOCIMI, S.A., as the legally liable company, for public interest reasons to avoid any possible irregularities or unlawful activities from being committed.

Except when required by law, this data will not be shared with third parties outside the Company or with anyone within the Company who is unauthorised to see or access it.

The parties involved in the reports or enquiries received may exercise the Privacy rights to which they are legally entitled and know in due detail all additional legal information by contacting dpo@inmocolonial.com or through this Policy.

Basic legal information (2nd layer)

Privacy Policy

1. PURPOSE

The purpose of this Privacy Policy is to inform of the legal conditions under which the personal data collected as a result of the reports or enquiries submitted through Colonial's Whistleblowing Channel will be processed.

In order to design and set up this Whistleblowing Channel, Colonial fully complies with the applicable Personal Data Protection regulations, in particular:

- (i) 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 (hereinafter, "*General Data Protection Regulation*"),
- (ii) Organic Law 3/2018, of 5 December, on Personal Data Protection, and
- (iii) other applicable implementing regulations.

Although not yet transposed into national law, Colonial has also taken into account some of the issues set out in 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.

2. DATA CONTROLLER

The data controller of any data collected within the framework of the Whistleblowing Channel is the company Inmobiliaria Colonial, SOCIMI, S.A. (hereinafter, interchangeably "Colonial" or the "Company").

The data controller's contact details are:

Company Name: Inmobiliaria Colonial, SOCIMI, S.A.

Registered office: Castellana 52, 28046, Madrid

Contact Information: Avenida Diagonal 532, 08006, Barcelona; Telephone: +34 93 404 79 00; Email: infocolonial@inmocolonial.com

Registry Information: Listed in the Madrid Commercial Registry in Volume 36660, Sheet 87, Page M-30822, Entry 276.

TAX IDENTIFICATION NUMBER: A28027399

3. ORIGIN OF THE PROCESSED PERSONAL DATA

In this Whistleblowing Channel, the data of both the whistleblower and the reported party may be processed, as well as the data of third parties if they have been involved in the events that are being reported or enquired about (e.g., possible witnesses). Colonial may receive this data:

- a) directly from the party concerned (by providing it when submitting the report or enquiry, when making possible allegations, or at any other time during the investigation); and,
- b) indirectly, by any natural or legal persons involved in the investigation, or by the Colonial Group companies, when the person works for or provides services to any one of those companies. In cases where personal data is indirectly received from a party concerned, he/she will be immediately informed, as a sign of transparency, in particular of the origin of the data and the category of the information received.

4. PURPOSE AND LEGAL STANDING

Pursuant to the European General Data Protection Regulation, it is hereby stated that the Whistleblowing Channel seeks to fulfil a threefold purpose, each with its corresponding legal standing:

a) Prevention of criminal risks in the Public Interest

Firstly, the personal data collected via the Whistleblowing Channel will be processed for the purpose of (a) processing and managing the enquiries and reports received; (b) where appropriate, investigating the events that are the object of the report; (c) clarifying and obtaining evidence of what occurred so that legal action can be taken if necessary; (d) providing the whistleblower with the necessary protection to prevent possible retaliation. This data processing will be carried out to fulfil a purpose in the public interest, such as the prevention, detection and discovery of possible risks and breaches of criminal law that may occur within the company, and which may give rise to criminal liability for Colonial as a legal entity.

b) As evidence of the correct functioning of the Criminal Risk Prevention Model in Colonial's Legitimate Interest

In addition, personal data may be processed within the framework of the Whistleblowing Channel to provide Colonial with proof of the correct functioning of its Criminal Risk Prevention Model.

This will be performed in Colonial's legitimate interest and does not harm or affect the Privacy of the parties concerned. Likewise, it is also in the latter's interest, since they have a legitimate

interest in the Company for which they work or to which they provide their services having and applying an appropriate and effective Criminal Risk Prevention Model.

c) Other possible uses that may become legally binding

In some cases, personal data may also be processed to comply with certain legal obligations applicable to Colonial, specifically regulations applicable to listed companies, and in particular, Circular 1/2020 of the Spanish National Securities Market Commission (CNMV).

The corresponding cases and applicable regulations will be announced where possible.

5. RETENTION PERIOD FOR COLLECTED PERSONAL DATA

Personal data of the whistleblower, the reported party, and third parties that may be mentioned in the report or that participate in the investigation (e.g., clients or other employees) will be processed by Colonial:

- a) For the necessary time to decide whether to open an investigation into the reported events. Three months after the data have been input, Colonial will delete them from the reporting system unless they need to be kept as proof of the functioning of the crime prevention model.
- b) When appropriate, during the course of the corresponding investigation.
- c) Throughout the exercise of the corresponding legal actions.
- d) In the case of enquiries, for the time necessary to manage, process and respond to the enquiries.

Following that, Colonial will keep the data (i) duly blocked and exclusively (ii) to comply with possible applicable legal obligations, as well as (iii) to respond to possible claims and liabilities, keeping them blocked for the periods set by law and at the disposal of the Mossos d'Esquadra (Catalan police), Law Enforcement Authorities, Courts, and possible competent Public Administrations.

6. WHO WILL BE THE RECIPIENTS OF THE COLLECTED PERSONAL DATA?

As a general rule, Colonial will not share any of the data collected through the Whistleblowing Channel with third parties. The data will only be accessed by Colonial staff who are duly authorised to do so as a result of their roles, responsibilities and duties within the Company.

However, there are some exceptions to this general rule. These are as follows:

- a) Data may be shared with third parties with whom Colonial is legally required to share it, for example, Courts, Mossos d'Esquadra (Catalan police), Law Enforcement Authorities, or any competent Public Body.
- b) If, as a result of an investigation carried out, it is decided to take legal action against a **Colonial Group employee**, the information strictly necessary for the correct execution of the relevant measures will be provided to the corresponding company.
- c) Colonial may also collaborate with **third-party service providers**, who may access and process the personal data in their name and on their own behalf.

Accordingly, it is hereby stated that Colonial, in accordance with Article 28 of the GDPR, **follows strict criteria for selecting suppliers in order to comply with its data protection obligations**. Therefore, in order to regulate the Privacy conditions under which these

potential third-party suppliers will act, Colonial agrees to sign the corresponding data processing agreement with them, which will impose the following obligations, among others: to apply appropriate technical and organisational measures; to process personal data for the agreed purposes and exclusively in accordance with Colonial's documented instructions; and to delete or return the data once the provision of services has been completed.

The previous statement is made since Colonial may contract third parties that provide services in, including but not limited to, the following sectors: legal counselling, multidisciplinary professional services networks, and technological or computer services.

When a third-party supplier is involved, the following obligations shall be expressly stated in the agreement entered into with said supplier:

- The supplier, as the data controller, will rigorously and strictly follow Colonial's instructions.
- The data controller will not use said data for any other purpose.
- The data controller will install technical and organisational security measures to ensure the confidentiality of the information to which it has access.
- The data controller will refrain from disclosing to third parties any data collected within the Whistleblowing Channel management framework, including for storage purposes.

The aforementioned actions will not entail the transfer of personal data outside the European Economic Area, and therefore, no international transfer of data will take place. Notwithstanding the foregoing, in exceptional circumstances, if it is necessary to carry out any actions that could entail an international transfer of data, Colonial will at all times strictly and duly comply with the legal and information obligations established by the law in force at any given time to safeguard the privacy of individuals.

7. RIGHTS

The persons whose personal data may be processed within the Whistleblowing Channel's context and framework shall have the following rights:

- a) The right to obtain confirmation as to whether their personal data is being processed (within the Channel's management framework) and to access, rectify, or restrict the use of their data, or, where appropriate, request their erasure, under the terms established by law.
- b) In certain circumstances, the right to object to the processing of their personal data.
- c) They are also entitled to lodge a complaint with the Data Protection Agency (as the competent Data Protection Supervisory Authority), especially if they are not satisfied with the exercise of their rights:
 - in writing to the Data Protection Agency, C/ Jorge Juan, 6, 28001-Madrid,
 - or via the website <https://www.aepd.es>

The interested party may also lodge a complaint with any other National Supervisory Authority within the European Union in the event that they are not a Spanish resident or in any other case and for any reason whatsoever. Click [here](#) to see the locations and contact details of these National Authorities (see Section "Making a Complaint").

8. RESTRICTION OF ACCESS TO DATA

Access to the data contained in the Whistleblowing Channel will be exclusively limited to the RCU, Human Resources, the Audit Committee, or to any other departments that are strictly necessary for the investigation of the reported events, all within the strict scope of their competency, in accordance with Colonial's Criminal Risk Prevention Model.

Furthermore, as indicated above, this data may also be accessed by third-party professionals to whom Colonial entrusts the provision of certain services related to the management of the Whistleblowing Channel.

9. PRINCIPLE OF PROPORTIONALITY AND DATA MINIMISATION

The personal data gathered in the framework of the Whistleblowing Channel:

- Shall be limited to the data that is **strictly and objectively necessary** to process the reports and, if applicable, to verify the veracity of the reported events;
- Shall be processed at all times in compliance with the applicable data protection regulations, **for legitimate and specific purposes** related to the investigation that may arise as a result of the report; and
- Shall be **adequate and not excessive**. Personal data shall not be collected where it is manifestly irrelevant to deal with a specific report.

10. SECURITY AND CONFIDENTIALITY MEASURES. EVENTUAL ANONYMITY OF THE WHISTLEBLOWER

Colonial shall ensure that all necessary technical and organisational measures are taken to preserve the security of the data collected in order to protect them from unauthorised access or disclosure.

In this regard, whistleblowers may decide to share their identity or remain anonymous when reporting an event. However, all whistleblowers are encouraged to identify themselves to obtain more information about the reported events. In any case, the identity of whistleblowers who identify themselves shall be kept strictly confidential.

Furthermore, as a measure to ensure the whistleblower's confidentiality, it is hereby expressly stated that the reported party's right of access does not automatically entail access to the whistleblower's identity.

However, as an exception to the foregoing, provided that there is sufficient and justified reason and it is essential to safeguard the right of defence of the affected party, or when required by law, the whistleblower's identity (as well as any other information from which the whistleblower's identity may directly or indirectly be deduced) may be disclosed to the reported party.

Disclosures made under the exception provided for in the previous paragraph will be subject to the appropriate safeguards. In particular, in addition to other measures that may be taken, the whistleblower will be informed before disclosure, unless said information could jeopardise the investigation or court proceedings, and shall be provided with a written explanation of the reasons for disclosure.

It should be noted that the whistleblower's identity will only be known to the RCU, the Audit Committee and the Directors of those departments that are strictly competent and involved in the investigation and resolution of the reports made. Their identity may also be known by external experts.

In this regard, it should be noted that anyone who, by reason of his/her duties, has access to the reports made is obliged to keep the whistleblower's identity secret.

11. DUTY TO INFORM THE INVOLVED PARTIES

The parties involved in the enquiries or reports received will be duly informed of the privacy terms and conditions under which their personal data will be processed. In order to carry out the above, Colonial's RCU:

1. Will provide the necessary mechanisms to guarantee that the recipients of this Channel know and have at their disposal the Privacy rules contained in this Policy in a simple, accessible, comprehensible, and free manner, and, in any case, prior to making any enquiry or report.

2. In addition, whenever a report or enquiry is made, the RCU will inform the people concerned individually. However, the manner in which this is done will be handled on an individual basis. In this regard, regardless of the fact that this Policy is accessible on Colonial's employee portal, the following measures will be taken to reinforce and ensure compliance with this duty to inform (depending on whether it is the whistleblower, the reported party or a third party):
 - **The whistleblower:** When reporting, whistleblowers will be informed of the processing of their data in the email sent to acknowledge receipt of the submission of their report or enquiry, with a link to this Privacy Policy if not reporting anonymously. This will be carried out within 7 business days from receipt of the report.
 - **The reported party:** In the case of the reported party, it will be necessary to assess, on a case-by-case basis, whether informing them of the report made against them could jeopardise the proper conduct and successful outcome of the investigation. In this regard, if it is decided not to inform the person concerned in the initial stage of the investigation, this decision will be duly recorded and justified.

As a general rule, the reported party will be informed whenever a report is made against them within one month of receipt thereof.

However, in exceptional cases and providing there is a just cause, informing the reported party may be delayed for a further two months (therefore, a total of three months), or the reported party may not be informed at all if doing so could seriously jeopardise the success of the investigation, notwithstanding their eventual involvement as a result of challenging the process followed.
 - **Any other party concerned with the report or enquiry:** Third parties involved in the report or enquiry made shall be informed prior to their participation in the process, for example, a potential witness prior to his/her interview or statement being taken.

12. DATA PROTECTION OFFICER

Colonial has appointed a person to ensure, among other aspects, that the Whistleblowing Channel operates in compliance with all the legal requirements of Spanish and European data protection regulations.

This person is the Data Protection Officer, who is responsible for managing any queries or complaints submitted as a result of and in relation to the processing of your personal data within the Whistleblowing Channel. The Data Protection Officer's contact email address is dpo@colonial.com