COLOMER LEATHER GROUP

INCIDENT MANAGEMENT AND INTERNAL INVESTIGATION PROCEDURE

COLOMER LEATHER GROUP, S.L.

Fourth Edition

July 2023

Table of Contents

1. Introduction

As part of the culture of transparency and responsible behaviour at Colomer Leather Group, S.L. ("**CLG**" or the "**Group**") and its commitment to the highest standards of business ethics, integrity and compliance, CLG encourages its Professionals, as well as Third Parties with which CLG has a relationship, to report any potential Incidents related to the Code of Ethics, the Crime Prevention Model ("**CPM**"), any other internal regulation of CLG or applicable legislation.

It is of the utmost importance that everyone cooperates in the detection of Incidents, both to protect CLG Professionals and the Third Parties with which they interact, as well as the Group as a whole. Any CLG Professional who becomes aware of an Incident (as defined in this Procedure) by any means (even if another Professional has shared such information) must report it immediately through the Internal Reporting System (the "**Reporting System**").

As a result, the Governing Bodies of CLG have approved this Incident Management and Internal Investigation Procedure (the "**Procedure**"). Furthermore, this Procedure governs the management and investigation of and the response to Incidents, while guaranteeing the rights of those under investigation to privacy, honour, presumption of innocence and to defend themselves.

The Reporting System and this regulatory Procedure are adopted in accordance with Spanish Law 2/2023, of 20 February, which regulates the protection of persons who report violations of the law and the fight against corruption, and in accordance with the provisions of Article 31.bis of Organic Law 10/1995, of 23 November, of the Criminal Code, achieving the implementation of a set of mechanisms that ensure compliance with the Crime Prevention Model implemented by the Group, which includes all those policies, procedures and controls aimed at preventing, reducing or eliminating the risk of crimes being committed.

CLG undertakes to comply with all the obligations set out in this Procedure and will ensure compliance by adopting appropriate measures, tools and procedures.

2. Purpose

The purpose of this Procedure is to regulate the handling of Incidents by establishing the basic principles for managing and responding to the reporting of Incidents related to applicable legislation, the Code of Ethics and/or other internal regulations that make up the Crime Prevention Model.

The Procedure contains the rules and procedures to be followed from the moment a report is received until it is resolved.

The principles, processes and responsibilities established in this Procedure for the handling of reports received through the Ethics Channel shall apply *mutatis mutandis* to communications received through the other established channels or when the Compliance Committee becomes aware by any other means of Incidents that should have been raised in accordance with the provisions established in this Procedure.

3. Scope of application

This Procedure applies to all CLG Professionals (and, where appropriate, other third parties that they designate) who may be involved in the management of the Internal Reporting System or the investigation of specific Incidents.

4. Definitions

CLG or "Group"	Colomer Leather Group, S.L. and all its subsidiaries, which are currently: Adobinve, S.L.; Grupo Ledexport, S.A.; Pells de Llobregat, S.A.; Pieles Quintana, S.A. and Pieles del Segura, S.A.
Compliance Committee	A supervisory body pursuant to Article 31-bis 2 PC.
Committee Delegate	A natural person with the authority to manage the Reporting System and handle investigation files.
Accused Person	Any person who is party to an Incident raised through the Ethics Channel or other channels, where applicable.
Incident(s)	Any sign, suspicion or reasonable risk of non-compliance with the applicable laws or the internal regulations of CLG, including the Code of Ethics and other policies and procedures, that may have occurred during the course of its business activities.
Informant	Professionals and Third Parties who report an incident that has come to their attention during the course of their employment or contractual or legal relationship with CLG or, where applicable, during the selection process or pre-contractual negotiations, through any of the channels provided for such purpose in accordance with this Procedure and the Incident Reporting Policy.
Model or CPM	CLG's CPM is the organisational and management model adopted and implemented by the Governing Body, which includes appropriate monitoring and control measures to prevent crime or significantly reduce the risk of it being committed.
Procedure	This Incident Management and Internal Investigation Procedure.

Professional(s)	All employees, senior executives and members of the Governing Bodies of CLG, as well as volunteers, interns and trainees, whether remunerated or not. The following are also considered to be Professionals for the purposes of this Procedure: • persons whose employment or legal relationship has ended; and • persons whose employment relationship has not yet commenced (those in the selection process or pre-contractual negotiations).
Reporting System	CLG's Internal Reporting System.
Third Party/Parties	All third parties with which CLG interacts (i.e. suppliers, employees and customers).

5. Obligation to report Incidents

All CLG professionals are required to ensure compliance with the Code of Ethics, the law and other internal policies, and to report any Incidents of which they become aware through the Ethics Channel or other channels provided for this purpose (described in the Incident Reporting Policy) so that the problem can be identified and resolved.

Persons who are part of the business organisation must cooperate in the internal investigation process whenever the Compliance Committee or the natural person designated to handle reports, the Committee Delegate, requests that they do so.

Should it be proven that a person who is part of the CLG business organisation had knowledge of an Incident and did not report it, he/she may be subject to the disciplinary measures and/or sanctions set forth in the Disciplinary Procedure.

The reporting of facts in the knowledge that they are false or with reckless disregard for the truth may result in criminal or civil liability as provided for by law, as well as disciplinary measures and/or sanctions as set out in the Disciplinary Procedure.

6. Raising doubts or other questions

The Compliance Committee is also available to all CLG Professionals to raise any doubts or questions regarding the interpretation of CLG's internal rules via the email address canaletic@colomerlg.com.

If the Compliance Committee receives a question that is not related to the Code of Ethics or the Internal Rules regarding the CPM, the Compliance Committee shall refer it to the appropriate person so that it can be addressed.

7. Guidelines and safeguards for reports made via communication channels

7.1. Security measures, confidentiality and anonymity

The Ethics Channel has appropriate technical and organisational security measures in place to prevent the risk of disclosure, unavailability, loss or destruction of information.

The Committee Delegate, another member of the Compliance Committee or any other person appointed to conduct an internal investigation will maintain the absolute confidentiality of the matter, including the identity of the Informant, by sharing the information with as few people as possible and by using the most secure means of communicating with the Informant (e.g. the platform made available for the Ethics Channel).

7.2. Non-Retaliation

CLG strictly prohibits its Professionals from intimidating or discouraging other Professionals from reporting an Incident. Likewise, CLG will not tolerate any form of retaliation against an Informant who reports an Incident in good faith and in accordance with the internal rules of CLG. To this end, the Committee Delegate, any other member of the Compliance Committee or any other investigator involved in an investigation must follow up on the situation of the Informant after making his/her report, by asking questions and ensuring, both during and after the investigation, that no retaliatory action is taken against him/her.

CLG is therefore committed to preventing, investigating and taking action against any direct or indirect retaliation, threat of retaliation or attempt to retaliate against:

- the Informant, for merely reporting the Incident in accordance with the internal rules of CLG, or using an external channel, or having made a public disclosure in accordance with applicable law; or

- any other professional who assists or participates in the process (for example, as a witness or by providing information).

Acts of retaliation include, but are not limited to, discriminatory or unfavourable treatment, demotion or unfair denial of promotion, changes to working conditions or termination of contract.

CLG will take all measures it deems necessary to protect Informants from retaliation and to maintain the integrity and fairness of an investigation. Any professional who retaliates against or personally harms an Informant may be subject to disciplinary action, up to and including dismissal.

Notwithstanding the foregoing, the mere reporting of an Incident does not exempt an Informant who participated in the reported misconduct from liability, although CLG may take the reporting of the Incident into account when determining the action that will be taken.

Anyone who believes that they have been the victim of retaliation should report it immediately through the channels set out in the Incident Reporting Policy.

7.3. Data protection

CLG undertakes to at all times process the personal data received through the channels

detailed in the Incident Reporting Policy, as well as the personal data relating to any investigation, in accordance with the provisions of the applicable data protection legislation.

CLG guarantees the application of the principle of transparency in relation to the use of personal data in the Reporting System, through the information provided to data subjects and Informants.

Access to the data contained in the reports is limited exclusively to the Committee Delegate and the other member of the Compliance Committee, in addition to the Professionals or external persons involved in the management, investigation and resolution of the reports.

Personal data relating to reports of Incidents that are received and internal investigations that are conducted shall only be stored for as long as is necessary, always in accordance with the periods stipulated in the applicable legislation and the relevant internal regulations.

7.4. Presumption of innocence, right to be heard and fair procedure

The Committee Delegate and other members of the Compliance Committee, as well as any other person involved in an internal investigation, shall at all times respect the rights of the persons involved in an Incident.

The presumption of innocence, the right to be heard and the right to defence of the Accused Person, who may defend him/herself and present such arguments, allegations and evidence as he/she deems appropriate, shall be respected. The Accused Person shall not be subject to any disciplinary sanction until the outcome of the investigation has been determined, without prejudice to any precautionary measures (including, but not limited to, temporary suspension of employment) that may be taken to ensure the correct conduct of the investigation. Such investigation shall be proportionate to the nature and severity of the reported Incident.

The Committee Delegate and the Compliance Committee shall always conduct a thorough analysis of the Incidents to confirm their veracity, provide prompt attention and response, and evaluate the reports received independently and objectively. All decisions taken in this context shall be duly reasoned and justified.

The Accused Person has the right to know the results of the investigation in general terms, so these will be provided upon request in the form deemed most appropriate, while respecting the honour and confidentiality of the other persons involved and of CLG.

8. Compliance Committee

To ensure the effective management of reports and internal investigations, CLG has a Compliance Committee which will assume the responsibilities arising from the implementation of this Procedure.

8.1. Responsibilities

The main responsibilities of the Compliance Committee in relation to this Procedure are:

- Receiving, processing and responding to any queries regarding the Code of Ethics and other internal regulations received via email at the address canaletic@colomerlg.com.
- Deciding on the admissibility or inadmissibility of reports.
- Appointing an investigator to conduct the investigation.
- Proposing disciplinary sanctions.
- Preparing regular reports on communications received through the established communication channels.

The Compliance Committee, as the body responsible for the Reporting System, shall promptly, impartially and diligently handle all Incidents and enquiries received, regardless of the channel through which they have been submitted.

CLG shall provide the Compliance Committee with the necessary resources to perform these duties.

8.2. Conflicts of interest and recusal

The Committee Delegate and/or any other member of the Compliance Committee may be subject to a conflict of interest if he/she receives a report concerning, for example, themselves, a person he/she trusts or a person assigned to his/her department.

In such cases, or in any other circumstance where a conflict of interest may be deemed to exist, the person concerned must report such circumstance and refrain from participating in the handling of the report, including the investigation of the reported facts, the conclusions of such investigation and, if applicable, the proposed sanction. If he/she does not voluntarily withdraw, another member of the Compliance Committee shall remove him/her and inform the Group's Governing Body as soon as possible so that the member affected by the conflict can be removed and an alternative person appointed.

9. Procedure for handling reports

9.1. Receipt, registration and preliminary analysis

The Committee Delegate will be responsible for receiving reports made through the

communication channels indicated in the Incident Reporting Policy.

In the event that reports are made verbally, the Committee Delegate or alternative person, as the case may be, must document the content of the report in the manner described in Section 5 of this Procedure. Should the Informant request a face-to-face meeting with the Committee Delegate or other member of the Compliance Committee, as the case may be, they must schedule such meeting **within a maximum of seven days** and document the report in accordance with the terms set out above.

Upon receipt of the report, either directly or through referral from another recipient, the Committee Delegate will conduct an initial plausibility analysis of the alleged events. If deemed necessary, he/she will request further information (i) directly from the Informant if he/she has provided contact details; or (ii) via the platform in the event of an anonymous report submitted through the Ethics Channel.

The Committee Delegate will provide the Informant with acknowledgement of the receipt of the report within a period of **no more than seven calendar days** of receiving such report, unless doing so could potentially compromise the confidentiality of the report.

In any case, the Committee Delegate must, where appropriate, register the report in the record book (hosted on the Ethics Channel platform) if it has been made through a channel other than the Ethics Channel.

The Committee Delegate will then prepare a brief account that must be sent to the Ethics Committee within a maximum of **three working days** from the date of receipt of the report or, where appropriate, the necessary additional information requested, along with a copy of the report, identification of the Incident and the potential risks and violations reported, and his/her preliminary conclusions on the action to be taken. This account shall be sent to the other member of the Committee, unless one of them is unavailable or has a conflict of interest, in which case it shall also be sent to the relevant alternative person.

If the report concerns an Incident that could constitute a case of harassment, the Ethics Committee shall forward the report to the Human Resources Department, which shall be responsible for handling the Incident in accordance with the provisions of the Protocol against Workplace Harassment, Sexual Harassment and Discrimination. Notwithstanding the foregoing, the Committee Delegate and the other members of the Compliance Committee shall be responsible for monitoring the proper handling of Incidents in this regard.

9.2. Admissibility of the report

Based on the information received from the preliminary analysis, the Compliance Committee will decide to:

a) Accept the report and initiate an investigation; or

b) Dismiss the report without further action for one or more of the following reasons:

a. There is no clear evidence that the Incident is in breach of internal regulations and/or the law.

b. The report does not meet the minimum requirements set out in the Incident Reporting Policy and the Informant has not corrected the errors after being requested to do so.

c. The nature of the report is such that the responsibility for dealing with it lies with another area or department. In such a case, the Compliance Committee will (i) notify the Informant as to which area or department is responsible; and (ii) refer the file to the appropriate area or department.

d. The reports have been made to a judicial or administrative authority that is in the process of investigating or preparing a decision, or such decision has already been made.

The deadline for notifying the Informant of the admissibility or inadmissibility of the report is **20 working days** from the date of receipt of the communication.

All information on reports received shall be accessible only to the Committee Delegate and the Compliance Committee and shall be kept in a protected and secure area that is accessible only to the aforementioned members.

10. Investigation Procedure

10.1. Initiation of the investigation

The purpose of the internal investigation is to clarify the events that have taken place, identify those responsible and determine whether irregular, unlawful or criminal conduct has occurred. The investigation shall be based on the principles of legality, validity, the admissibility of evidence obtained, accountability and transparency, subject to a strict regime of confidentiality to respect the rights of the Informant.

In any event, the internal investigation shall be conducted in such a way as to allow the gathering of evidence that is legally valid and admissible in any potential legal proceedings brought against the Accused Person.

10.2. Methodology

The Compliance Committee shall, upon receipt of the report, determine the following aspects of the investigation:

- The scope of the internal investigation;
- The adoption of any urgent precautionary measures deemed necessary to preserve relevant evidence, and whether any of these measures conflict with the fundamental rights of the persons concerned;
- The means of acquiring the evidence necessary to determine the veracity of the reported events, including, but not limited to; (i) intercepting the IT devices and/or communications of the persons under investigation; (ii) reviewing documentation of any kind and in any medium; (iii) requesting information from external sources; and (iv) conducting interviews with the Informant, witnesses and/or the person under investigation;[1]

[1] To this end, the Compliance Committee shall request the necessary expert advice, including the input of the

- Whether it is necessary to involve any department of the Group in any of the phases of the investigation, if it has knowledge of the alleged events or if this is advisable due to its specialisation in the area under investigation;

- Whether all or part of the internal investigation file needs to be outsourced. All cooperation with the investigation shall be subject to a duty of confidentiality on the part of those involved;

- The appointment of an investigator to conduct the investigation, whether this is from the members of the Compliance Committee, another CLG professional or an external third party.

If the circumstances of the case so require, the internal investigation file may be outsourced in whole or in part.

In any case, in all investigation procedures the applicable legal provisions shall be respected, including those contained, where appropriate, in the applicable collective bargaining agreement. The rights of the Informant to privacy, defence and the presumption of innocence shall also be guaranteed.

10.3. Communication to the persons being investigated

As a general rule, the investigator is required to inform the Accused Person as soon as possible of:

- The acts that he/she is accused of;
- The opportunity that such Accused Person has to present his/her version of events and to present any evidence in support of his/her defence as he/she deems appropriate;
- Which departments within the Group or other third parties may have access to the information contained in the report; and
- How to exercise his/her rights in relation to his/her personal data.

All individuals involved in an Incident should be informed of how their personal data will be processed as soon as possible. Affected persons may include Informants, witnesses, third parties and Accused Persons. Depending on the case, informing all third parties mentioned in the allegations is not necessary if this would entail a disproportionate effort.

At all stages of the investigation, the rights to defence of the Accused Person shall be respected. The investigator shall therefore, if necessary, give the Accused Person a hearing. At such a hearing, the facts will be presented and the Accused Person shall be given the opportunity to present his/her version of events, always in compliance with the principle of presumption of innocence and the provisions of the applicable laws and agreements.[2]

However, in the event that a risk exists that such a notification would jeopardise the ability

Data Protection Officer, in order to ensure that such access is performed in such a way as to comply with the necessary guarantees of protection of personal data. Furthermore, in all cases, the joint authorisation of the two members of the Compliance Committee shall be required in order to proceed with the interception of the IT devices and/or communications of the persons under investigation.

2 This hearing shall be deemed to conclude the prior consultation procedure under the contradictory procedure provided for, where applicable, by the applicable legislation or collective agreement.

of the panel to effectively investigate the alleged events or gather the necessary evidence, notification of the Accused Person may be delayed for as long as such risk exists. Any delay shall be determined on a case-by-case basis. In any event, the delay shall not exceed **one month from the date of receipt** of the report.

Furthermore, the Accused Person will not be informed of the identity of the Informant, except as required by law or other legitimate interests and as permitted by applicable data protection and employment laws.

Should the events reported potentially be indicative of a criminal offence, the investigator will inform the Compliance Committee, which will immediately inform the Public Prosecution Service and, where appropriate, an internal investigation may be conducted in parallel with the relevant judicial proceedings, provided this does not interfere with said proceedings, in which case it must be suspended.

10.4. Conclusion and sanctions

The investigator shall complete the investigation as soon as possible and without undue delay, and in any event **within three months** of the date of the acknowledgement of the receipt of the report. If the investigation is particularly complex, the investigation period may be extended **by a further three months**.

The investigation process shall be fully documented in writing. The investigator shall describe the actions taken and statements made, including the following:

i. The nature of the potential Incident: to the extent possible, the parties involved (and their level of involvement or responsibility); the nature of the alleged events; the circumstances alleged to have occurred and the date and place of such occurrence; as well as the legal requirements and/or internal policies alleged to have been violated should be identified.

ii. The identity of the person in charge of the investigation and list of actions taken: the person in charge of the investigation will be identified, as well as any other CLG or external Professionals who may have been involved in the investigation. Furthermore, the main actions carried out during the investigation and the information obtained shall be detailed.

iii. The chronology of relevant events: a precise chronology of relevant events should be included.

iv. The conclusions and assessment of the events: the conclusions drawn and whether the reported events are truthful and constitute a breach of internal regulations or applicable law shall be detailed.

Upon completion of the investigation, the Compliance Committee will issue a final report outlining the key findings, which will be forwarded to the appropriate Governing Body of the Group for appropriate action.

The Compliance Committee will notify the Informant of the outcome of the investigation conducted, unless there are circumstances that make it appropriate to maintain the confidentiality of the conclusions. The conclusion reached by the Compliance Committee will, where appropriate, be communicated to the Accused Person.

Should the events reported be confirmed in whole or in part, the investigation report will include a proposal for appropriate sanctions, depending on the seriousness of the conduct that has been identified and based on the provisions of CLG's Disciplinary and Sanctioning Procedure, and will serve to notify the Informant of the actions taken.

10.5. Other relevant findings of the investigation

Based on the results of the investigations, the Compliance Committee will determine whether corrective or remedial action should be taken with respect to any required controls or elements of CLG's CPM. Where appropriate, the Compliance Committee will inform the relevant Governing Body of the Group of any resulting action plans or recommendations to improve CLG's existing processes and policies.

10.6. Principles applicable to the disciplinary system

With the aim of discouraging behaviour that is contrary to internal regulations and/or the law, while ensuring effective compliance with the CPM, appropriate disciplinary action will be taken not only against those who actively and directly perpetrate an Incident, but also against those who:

- prevent or attempt to prevent the submission of reports;
- help to prevent or hinder the detection of Incidents;
- encourage or induce third parties to participate in and/or commit Incidents;
- fail to comply with the duty to report (through the Ethics Channel or other channels) the existence of Incidents;
- take or threaten to take any retaliatory action against the Informant;
- breach the duty to maintain the confidentiality of the Informant's identity; and
- make flagrant malicious use of the Ethics Channel or any other channels.

Any conduct that violates the obligations arising from the Code of Ethics, the CPM or this Procedure will be sanctioned, and the fact that the offender was following the orders of a hierarchical superior will not be considered as a valid justification.

In the event that, as a result of the investigation carried out in accordance with this

Procedure, a breach of the aforementioned obligations by a CLG Professional has been proven, the Human Resources Department shall communicate the conclusions reached to the offender, informing him/her of the resulting consequences via any means that allows for proof of receipt, within the corresponding legal deadline.

In any case, the imposition of disciplinary measures shall be in accordance with the grading of offences and sanctions established by the general legal provisions and the collective agreement in force. Penalties shall be graded according to the seriousness of the acts committed and may take into account circumstances such as recidivism, the damage or harm caused or the circumstances of the victims.

Should such measures affect the Compliance Committee, the results of the investigation, along with all available information, will be reported to the relevant Governing Body of the Group.

In the event that the violations have been committed by Professionals of whom CLG is not the employer, this fact shall be brought to the attention of their employer. Without prejudice to the exercise of the employer's disciplinary powers, CLG shall consider the suitability of taking appropriate action within the framework of its contractual relationship with the employer and/or bringing the reported events to the attention of the relevant authorities.

11. Register of reports

The register of reports should include the following information, as appropriate, for internal and statistical control purposes:

- The date of receipt of the report and the acknowledgement of receipt.
- The company to which the Accused Person belongs.
- A description of the alleged events.
- Whether the report of the Incident has been accepted for processing or filed.
- The department or person responsible for conducting the investigation.
- The date the internal investigation was initiated.
- The history of the measures taken since the Incident was reported, including the actions and decisions taken at each stage of the process and the reasons for them, as well as any means and resources used for the purpose of the investigation.
- The resolution of the Incident.

The register shall comply with applicable data protection legislation and be accurate, detailed and up to date regardless of the channel used.

12. Annual Report and Review

The Compliance Committee shall inform the relevant Governing Body of the Group about the reports received and the investigations carried out in accordance with the provisions of this Procedure.

Specifically, the Compliance Committee shall prepare an annual report on the functioning of the Ethics Channel, detailing the activities carried out while performing its role of monitoring the effectiveness of the internal controls of CLG and the CPM to prevent, detect and respond to potential Incidents, irregular conduct and/or non-compliance. The Compliance Committee shall monitor the proper functioning of the Ethics Channel and the Internal Investigation Procedure. In this regard, the report that will be prepared annually by the Compliance Committee and sent to the Governing Bodies of CLG and the compliance

function of the MDM shall include at least the following information:

- The number of consultations and reports received.
- The origin of the consultations and reports received (internal/external).
- The nature of the consultations and reports received.
- The number and type of reports filed.
- The number and type of reports investigated.
- The outcome of the investigations into reports and the legal proceedings initiated as a result.
- The disciplinary measures taken.
- Regulatory changes that may affect the Ethics Channel and other communication channels and the Internal Investigation Procedure.

Both in the aforementioned annual report and in the register used to document the investigative actions, all references that would allow the Informant and the Accused Person to be identified shall be avoided.

13. Data protection

13.1. The Data Controller

In accordance with the provisions of the legislation on the protection of personal data, the data provided through the Ethics Channel or other channels and those derived from the investigations and enquiries conducted will be included in a personal data file under the responsibility of the Colomer Leather Group, S.L. (hereinafter "**CLG**"), with registered address at C/Figueres, 12 08500 Vic (Barcelona) and the email address privacy@colomerlg.com.

13.2. Purpose and legal basis for the processing of personal data

CLG undertakes to at all times process the personal data received through the Ethics Channel or other channels in a confidential manner and in accordance with the purposes set out in this regulation and to adopt the necessary technical and organisational measures to guarantee the security of the data and to prevent their unauthorised alteration, loss, processing or access, taking into account the state of the art, the nature of the data stored and the risks to which they are exposed. In accordance with the applicable regulations, the legal basis for the processing of personal data is the public interest, or the processing of personal data may be based on compliance with a legal obligation of the Group, in which case the data subject must provide his/her personal data in order for CLG to comply with the applicable legislation.

13.3. Access to personal data

Access to the data contained in the Ethics Channel is restricted exclusively to the Compliance Committee, as the body responsible for CLG's internal control and compliance duties, and to those persons within CLG and/or external persons who assist CLG with managing, investigating and resolving reports. However, access may also be granted when

necessary for the purposes of disciplinary action or legal proceedings. Access will only be granted to staff with human resources management and control duties in the event that disciplinary action may be taken against an employee.

13.4. Informing the Accused Person

As a general rule, the Compliance Committee will notify the Accused Person as soon as possible regarding:

- The alleged events;
- The person responsible for managing the Ethics Channel; and
- The departments within CLG or other third parties which may have access to the information reported.

However, should such notification present a risk of jeopardising the ability of CLG to effectively investigate the alleged events or gather the necessary evidence, notification of the Accused Person may be delayed for as long as such risk exists. In any event, such delay shall not exceed one month from the receipt of the notice.

Except as required by law or in the case of reckless disclosure, the identity of the Informant will not be disclosed to the Accused Person.

13.5. Data retention

The personal data of the person making the report and of the Professionals and third parties will be stored in the Ethics Channel for the time required to decide whether to initiate an investigation into the reported events. CLG will delete the data from the Ethics Channel three months after they have been entered unless (i) the investigation is extended by three months due to its complexity, and/or (ii) the purpose of storing the data is to have evidence of the functioning of CLG's Crime Prevention Model. In the event that there is no follow-up on the report, the data may only be stored in an anonymised form.

Notwithstanding the foregoing, the entities and persons referred to in Section 13.1. may continue to process the personal data for the purpose of investigating the reported events and not store them in the Ethics Channel system.

13.6. International transfers

In general, CLG does not intend to transfer personal data to third countries or international organisations.

13.7. Principle of data quality and rights

By using the Ethics Channel, Informants declare that the information provided is truthful, accurate, complete and current to the best of their knowledge and belief.

Users of the Ethics Channel may exercise their rights of access, rectification and erasure of their personal data, their rights to object to and restrict the processing of said data, as well as their right to data portability, in accordance with current legislation. Such rights can be exercised by sending a written communication to CLG's registered office, stating the specific right to be exercised. You also have the right to lodge a complaint with the

Spanish Data Protection Agency, located at C/ Jorge Juan, 6 (28001) Madrid (www.aepd.es).

14. Final provisions

14.1. Approval and modification of the Procedure

This Procedure has been approved by the Governing Bodies of CLG which has been taken note of. Any amendment to this Procedure must be approved by the Governing Bodies of CLG.

14.2. Questions and incidents

It is the responsibility of the Committee Delegate to resolve any doubts or discrepancies that may arise regarding the interpretation and application of the content of this Procedure.

Similarly, any CLG Professional and/or third party who suspects the existence of a breach of this Procedure must report it immediately using the communication channels detailed in the Incident Reporting Policy.

14.3. Communication and training activities

This Procedure shall be made available to all Professionals and third parties on the CLG website. Similarly, the senior executives and members of the governing bodies of CLG, in conjunction with the Committee Delegate, shall raise awareness of and promote strict compliance with this Procedure among the CLG Professionals under their supervision and shall take appropriate measures to monitor compliance with this Procedure by those under their authority.

At the beginning of their professional relationship with CLG, each Professional shall be informed of the existence of the Internal Reporting System and this Procedure as part of their initial training.

In addition, managers and executives will be trained on how to identify and manage reports of Incidents and on their roles and responsibilities within the Internal Reporting System.

14.4. Non-compliance with this Procedure

All CLG professionals are responsible for complying with this Procedure. Failure to comply with this Procedure may result in appropriate disciplinary action up to and including dismissal or termination of contract, depending on the circumstances. Third parties who violate the law or this Procedure may be subject to lawful termination of the business relationship by CLG, without the possibility of any compensation or other recourse as a result of such termination.

14.5. Related documents

a) CLG Code of Ethics

b) Incident Reporting Policy

15. SOLE ANNEX

15.1. Data protection notice (window opens with the following information)

FIRST LEVEL

Data controller	COLOMER LEATHER GROUP, S.L. (hereinafter referred to as **"CLG"**)
Purposes	• The processing and evaluating of reports submitted through the Ethics Channel or other communication channels, in order to conduct any necessary investigations into the reported conduct. • Compliance with applicable requirements under relevant laws and regulations to which CLG is subject.
Legal basis	(a) Legitimate interest. (b) Compliance with applicable legal or regulatory requirements.
Recipients	• Companies within the CLG Group to the extent necessary to process complaints and conduct any necessary investigations. • Third party service providers. • Law enforcement agencies, courts, regulatory bodies, government agencies or other third parties with full authority.
Rights	You have the right to access, rectify or erase your personal data, to restrict further processing and to data portability. You may also object at any time to the processing of your personal data for reasons relating to your particular situation, if the processing is based on legitimate interest.

	The above rights may be exercised by sending a request, along with a copy of your national identity card or equivalent identification document, via email to privacy@colomerlg.com.
Additional information	Please contact the following email address for further information: privacy@colomerlg.com

SECOND LEVEL

In order to receive and process your complaint, COLOMER LEATHER GROUP, S.L. (hereinafter referred to as "**CLG**") will collect certain information about you, which will be considered "personal data" within the scope of the applicable data protection legislation. Specifically, the personal data provided through this Ethics Channel will be included in a database whose Data Controller is CLG, with registered offices at Calle Figueres (PLA ST dels Pradals),12, piso 2, Desp 8, 08500 Vic and the email address privacy@colomerlg.com.

Please note that the personal data collected through this Ethics Channel, as well as any subsequent communication between you and CLG in relation to the relevant complaint, are essential to determine the validity of such complaint and also to ensure an appropriate investigation of the reported misconduct.

CLG will collect and further process the personal data you provide through the Ethics Channel for the following purposes, including the legal basis thereof:

(i) To process and assess the complaint and any subsequent related communication submitted through the Ethics Channel and to conduct such investigations as CLG deems appropriate in relation to the reported conduct, taking into account the legitimate interests of CLG. Further information regarding this analysis is available upon request.

(ii) To ensure optimal compliance with the applicable requirements of the relevant laws and regulations to which CLG is subject, including but not limited to employment, social security, tax and criminal law, and to facilitate cooperation with regulators and law enforcement agencies where necessary to respond to requests from authorities and public bodies with decision-making powers.

In furtherance of the purposes described above, CLG may not disclose or otherwise provide access to personal data to parties other than the following:

(i) CLG entities, when necessary and only to the extent required to determine the validity of the complaint, to request information from certain internal roles where necessary, and alternatively to assist in the investigation of potential improper conduct, including disclosure of the outcome of the investigation to interested parties.

(ii) Third party advisory, legal and consulting service providers, such as external consultants, law firms, auditors, forensic experts, IT managers, translators, investigators

and, where necessary, government agencies, who provide certain services and other business support to CLG and who will be granted access to personal data to the extent necessary to perform the data processing operations in providing such services or activities as described in this notice.

(iii) Law enforcement agencies, courts, regulatory bodies, governmental authorities or other duly authorised third parties that CLG deems necessary to comply with applicable requirements established by applicable laws and regulations or to otherwise protect its own rights or the rights of third parties.

CLG must provide adequate safeguards to ensure that your personal data are processed with the same level of protection as would be afforded to you in your own jurisdiction, such as the standard contractual clauses approved by the European Commission. You can access these documents or obtain a copy of the relevant decisions at the links below: 2004/915/EC (standard contractual clauses for the transfer of personal data from the Community to third countries (transfer between processors)) and 2010/87/EU (standard contractual clauses for the transfer of personal data to processors established in third countries) or by contacting us at the email address indicated at the end of this document.

CLG will store and process your personal data on servers located in Spain and will retain it for the duration of any ongoing investigation and for at least two months (i) following the conclusion of any investigation or (ii) for any complaint in respect of which CLG determines that there is insufficient evidence. Please note that these retention periods are in addition to any other relevant statutory retention periods that CLG is required to comply with under applicable laws.

You have the right to obtain confirmation from CLG as to whether or not your personal data are being processed and, if this is the case, to request access to the personal data as well as certain information about the processing of your personal data (the purposes, categories and recipients of the personal data being processed, etc.) (right of access). You also have the right to request the rectification of inaccurate personal data (right of rectification) and the erasure of personal data if, inter alia, it is no longer necessary for the purposes for which it was collected (right to be forgotten). In certain cases, for example, if the data subject has doubts as to the accuracy of the personal data, he/she may, pending verification, request a restriction of the processing of the personal data, which may only be processed for the purpose of lodging a complaint or objecting to processing (right to restriction of processing). Finally, you may also exercise the right to data portability, i.e. to receive personal data in a structured, commonly used and machine-readable form, and the right to transfer them to another controller without being prevented from doing so by the controller to which you provided them, where you are legally entitled to do so (right to data portability).

In addition to the above rights, you have the right to object at any time to the processing of your personal data on grounds relating to your particular situation, when the processing is based on legitimate interest.

You can exercise your rights by sending a request, along with a copy of your national identity card or equivalent identification document, via email to privacy@colomerlg.com.

You also have the right to lodge a complaint with the local data protection authority, particularly if you believe that the exercise of your rights has not been satisfactorily fulfilled.

CLG is committed to protecting your personal data as described in this notice and as required by applicable laws. If you have any questions or would like more information on how to exercise your rights, please contact us at privacy@colomerlg.com.