HIMOINSA GROUP ETHICAL CHANNEL MANAGEMENT PROCEDURE

Introduction

The Board of Directors of DISMUNTEL S.L. at its meeting held on September 21, 2023 ratified and adhered to the Ethical Channel Management Procedure approved by the Group's parent company, HIMOINSA, S.L., which is adapted to Law 2/2023, of February 20, regulating the protection of persons who report regulatory infringements and the fight against corruption, and whose content is set out in the following sections.

The purpose of this Procedure is to establish the rules of use, operation, principles and rules of procedure for the management of communications made through the Ethical Channel and shall be applicable to any person using the Channel.

1. Communication channels accessible through the Ethical Channel

The Ethics Channel provides two distinct types of communication channels that are easily accessible at all times:

a) A separate Inquiry Channel for each of the Himoinsa Group companies, to be accessed from the home page of each company's website, through which inquiries and/or doubts may be raised regarding the interpretation or application of the Code of Conduct, the Policies and Procedures approved and implemented by the Company.

b) An Alert Channel, also differentiated for each of the Himoinsa Group companies, which shall also be accessed from the home page of each company's website, and through which information shall be provided on the existence of risks of compliance with the Code of Ethics, the Action Policies or any other internal rules of the Company, as well as any breaches of European Union law, actions or omissions that may constitute a criminal offence or a serious or very serious administrative offence (which shall be understood to be those that imply a financial loss for the Public Treasury and Social Security)

When the communication of an Alert is sent through a channel other than this one or is delivered or communicated to members of staff not responsible for its processing, the recipient of the communication must immediately forward it to the Risk and Compliance Committee and keep the facts communicated and the identity of the informant strictly confidential.

These channels have been created with a technological communication tool designed by Lefebvre, S.A., which guarantees levels of security, privacy and data protection in accordance with legal requirements and international standards, and facilitates more secure, transparent, agile and traceable management of the communications that take place.

2. Typology of Communications

Two types of communications can be made using the access on the home page of the Corporate Website of Himoinsa and its subsidiaries (including Dismuntel, S.L.): queries and alerts on non-compliance.

Inquiries:

These are written communications that have the purpose of raising doubts about the interpretation or application of the Code of Conduct, Policies and Procedures approved and implemented by

the Company, and in which a formal and written pronouncement is requested on the scope, application or interpretation that should be given to the points consulted.

The person who raises a Consultation shall be referred to as the "Consulter".

The Communication of a Consultation will generate a file to which the Risk and Compliance Committee will assign a reference that will be different from the identification code automatically generated by the Channel's technological tool, a code that the Enquirer must keep together with the access link or URL provided by the Channel in order to access and monitor the processing of the Consultation, communicate directly with the Channel manager and provide additional information to modify or complement the initial consultation, either by adding messages or uploading files.

Alerts:

These are written communications aimed at communicating any information relating to the Himoinsa Group based on reasonable suspicions about the existence of actual or potential breaches that have occurred or may occur and about attempts to conceal such breaches in relation to any of the matters set out in Section 3.2 of the General Policy of the Ethical Channel

The person communicating the Alert shall be referred to as the "Reporting Person".

As stated in Section 4.4 of the General Policy of the Ethical Channel, at the request of the informant, the information may also be submitted by means of a face-to-face meeting with a member of the Risk and Compliance Committee, for which purpose an appointment must be requested in advance via e-mail at compliance@himoinsa.com, and the meeting must be held within a maximum period of seven (7) days. The meeting shall be recorded for complete and accurate transcription by the Secretary of the Risk and Compliance Committee; the transcript of the conversation shall be offered to the informant for verification and, if he/she agrees, acceptance by signature. Once such transcript has been signed, the recording of the conversation shall be destroyed.

If the Alert identifies the person who is considered responsible or to whom the reported facts are attributed, that person will be considered as "Investigated" for the purposes of this Procedure, provided that the Alert in question is accepted for processing.

For the purposes of this Procedure, a person shall also be treated as a person under investigation if, even though he/she has not been identified or expressly identified as such by the Reporting Person, it is reasonably inferred from the account of the events contained in the Alert admitted for processing, in the opinion of the investigator appointed by the Risk and Regulatory Compliance Committee, that he/she may have been responsible for or intervened in them.

This status shall also be attributed to the person who appears to be allegedly responsible for the facts reported, as and when the Instructor of the file carries out the internal investigation procedures.

The Communication of an Alert will generate a file to which the Risk and Compliance Committee will assign a reference that will be different from the identification code automatically generated by the Channel's technological tool, a code that the Reporting Party must keep together with the access link or URL provided by the Channel to be able to access and monitor the processing of the Alert, communicate directly with the Channel manager and be able to provide additional

information to modify or complement its additional information, either by adding messages or uploading files.

5. Ethical Channel Management

The Board of Directors of Himoinsa has appointed the Risk and Compliance Committee of the Company (hereinafter, "the Committee") as the Head of the Internal Information System, called "Ethical Channel", of the Himoinsa Group. For its part, the Board of Directors of Dismuntel, S.L. has ratified this appointment.

For the appropriate purposes, it is hereby stated that the Committee is made up of the following persons:

- The Committee is chaired by a member of the Board of Directors of Himoinsa, who also holds the position of General Power of Attorney of Himoinsa and is a member of the Board of Directors of its subsidiaries in Spain.
- The Head of Himoinsa's Finance Department.
- The Head of Himoinsa's Legal Department, who acts as Secretary of the Committee.
- The Head of Himoinsa's Human Resources Department.

The management of the Ethical Channel has been entrusted by the Committee to the person who holds its Chairmanship who, under his responsibility, may be assisted and, if necessary, delegate the investigation and processing of the investigation files of the communications to the Heads of the Legal and Human Resources Departments, or to specialized external consultants, who may act individually or jointly depending on the complexity and nature of the communications.

The receipt and acknowledgement of receipt of the communications shall be carried out, in all cases, by the Head of the Legal Department, who shall assess, together with a specialised external consultant, whether or not there is any type of conflict of interest in order to apply the measures of abstention and recusal contained in Section 7.3 of this Procedure.

6. Procedure for the Management of Consultations communicated through the Ethical Channel.

Once the inquiry has been received through the Ethical Channel, the technological tool will automatically register it and send an acknowledgement of receipt of the communication to the enquirer on the same day.

Any consultation whose content is outside the scope of the Ethical Channel or which is made in disrespectful terms or in bad faith will not be accepted.

Once the consultation has been analysed, a written response will be issued, and it will be sent to the applicant, through the Channel, within a period of no more than fifteen (15) calendar days.

7. Procedure for the Management of Alerts communicated through the Ethical Channel.

7.1 Receipt, registration and acknowledgement of receipt

Once an Alert is received through the Ethical Channel, it will be automatically registered in the technological tool, the informant will be formally acknowledged of its receipt and will be briefly informed of the procedure to be followed and the deadlines for its processing and resolution.

The acknowledgement of receipt shall be sent to the reporter as soon as possible and in any case within seven (7) calendar days of the submission of the Alert, starting on the same day.

In those cases where the reporter has acted anonymously and has not provided any contact details, the acknowledgement of receipt will be registered in the existing Communication Channel in the technological tool which the reporter can access at any time with the link and the code that was generated when sending the communication.

Exceptionally, this acknowledgement of receipt shall not be made where it is reasonably considered that such an act may compromise the protection of the identity of the informant.

7.2 Admission procedure

The Chairman of the Committee or, as the case may be, the Head of the Legal Department acting by delegation of the Chairman, shall verify whether the information contained in the Alert exposes facts or conduct that fall within the scope of application of the Channel set out in Section 3 of the Policy.

Once this preliminary analysis has been carried out, the Chairman of the Committee or, where appropriate, the Head of the Legal Department acting by delegation of the former, shall decide, within a period of no more than fifteen (15) calendar days from the date of presentation of the Alert, whether or not to admit the Alert for processing.

The communication shall be rejected as inadmissible if any of the following applies:

a) The facts reported do not relate to the scope of application of the Channel as set out in Section 3 of the Policy.

b) The facts reported relate to any of the matters expressly excluded from the objective scope of the Channel in accordance with Section 3.2 of the Policy

c) The facts reported do not constitute, in a notorious and obvious manner, any irregularity or infringement within the objective scope of the Channel (Section 3.2 of the Policy).

d) The reporter has not respected the principles governing the Ethical Channel (Section 4 of the Policy) in his/her communication; in particular, the alert will be rejected if it contains personal data of persons who have no connection with the facts or if personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, as well as biometric data, data concerning health or data concerning the sex life or sexual orientations of the informant, the person under investigation or any other natural persons are communicated.

e) The whistleblower has made a public disclosure of facts without first going through the Company's Ethical Channel.

f) When the false or malicious nature of the communication is clearly and manifestly established.

g) When the communication is manifestly unfounded or there are reasonable grounds to believe that the information has been obtained through the commission of an offence; in Versión 08/05/2023 5 the latter case, in addition to the inadmissibility, a detailed account of the facts deemed to constitute an offence shall be sent to the Public Prosecutor's Office

h) When the Alert communicated refers to facts that are already being investigated in another ongoing File, without prejudice to the possibility of joining the Alert that is inadmissible to that File when it contains additional information relevant to the facts under investigation there.

i) When the Alert does not contain significant new information on infringements as compared to a previous communication in respect of which investigations have been completed.

j) When the Alert suffers from a total lack of definition or lack of specificity with regard to the facts and alleged non-compliances reported, which have not been rectified by the informant after the appropriate request for complementary information or clarifications.

k) The Alert does not provide or facilitate the slightest evidentiary support to corroborate, even indirectly or indirectly, the plausibility, veracity or credibility of what is stated in the communication.

The non-admission will be communicated to the informant within seven (7) calendar days following the decision taken in this regard, unless it was anonymous and the informant has not provided any contact details, in which case the non-admission will be reported through the Communication Channel of the technological tool.

If none of the above cases of inadmissibility apply, the Alert will be accepted for processing. The informant shall be notified of the admission for processing within seven (7) calendar days of the decision taken in this regard.

In the event that the facts reported in the Alert could be indicative of a criminal offence, the information received shall be immediately forwarded to the Public Prosecutor's Office or to the European Public Prosecutor's Office (if the facts affect the financial interests of the European Union), provided that such forwarding does not affect the rights and guarantees recognised in the criminal proceedings of the legal person.

7.3 Grounds for abstention and recusation

In the event that the information contained in an Alert affects a member of the Committee who is to be involved in the processing, investigation or resolution of the relevant file, he/she must abstain from participating in the process.

Likewise, the following are causes for abstention and recusation that will prevent the participation of a member of the Committee in the processing of an investigation file and/or of the Instructor of the file:

a) Existence of a family relationship with the informant or the person under investigation.

b) Having submitted a previous Alert against him/her.

c) Having a direct or indirect interest in the facts reported.

d) Being part of the Area or Department affected by the information reported.

e) To have a manifest and known enmity with the informant or with the person under investigation.

f) Being or having been in a situation of direct hierarchical dependence on the informant or the person under investigation.

g) Any other circumstance that hinders or prevents the Committee member from acting independently, impartially and objectively

The concurrence of any of these causes for abstention and recusation in a member of the Committee shall be evaluated by a specialised external consultant who shall communicate his opinion to the Committee, which shall decide on the concurrence or not of a cause for abstention and recusation by agreement adopted by a simple majority of its members of those who are not involved in said cause. In the event of a tied vote, the Chairman of the Committee shall have a casting vote.

7.4 Opening of the investigation and conduct of the investigation

7.4.1 Starting the investigation

In order to proceed with the opening of an internal investigation and, consequently, to process the corresponding file, the person(s) designated by the Chairman of the Committee (hereinafter "the investigator") shall first carry out a preliminary analysis of the irregular conduct reported or detected in order to assess the credibility and relevance of the alleged facts.

In any case, efforts shall be made to ensure that the preliminary analysis does not take longer than seven (7) calendar days.

7.4.2. Information

The person or Area involved shall be informed of the basic content of the communication received and the conduct imputed, without in any case communicating the identity of the informant, who shall have the guarantee of confidentiality provided for in Section 7.5.1 below.

However, in cases where there is a reasonable risk that such notification may compromise the proper conduct of the investigation or the taking of necessary evidence, the notification to the investigated person may be delayed for as long as such risk exists. In any event, this period shall not exceed two (2) months.

Likewise, during the processing of the investigation, the investigator will maintain communication with the informant to inform him/her briefly of the formal evolution of the processing and, if necessary, to request additional information, if required.

In those cases in which the informant has acted anonymously and has not provided any contact details, this information on the status of processing or requests for additional information will be recorded in the existing Communication Channel in the technological tool, which the informant can access at any time with the link and the code generated when sending the communication.

7.4.3 Planning of the research

In order to clarify the events that took place and to identify those responsible, the designated investigator will plan the investigation procedure, which will be set out in a document called "Investigation Process".

This "Investigation Process" document shall specify at least: the identity of the Investigator of the investigation, the facts to be investigated, the alleged perpetrators, the main evidence or measures to be taken, the time initially planned for the duration of the investigation, as well as any precautionary measures.

Precautionary measures shall be taken within the framework of legality and shall be of a provisional nature for as long as necessary, including: suspension of access rights to computer equipment, systems, etc.; auditing of computer equipment and systems; securing of electronic evidence; suspension of employment, etc.

In planning the investigation, the investigator shall primarily take into account the seriousness, the possible scope of the facts, the values or principles or rules infringed, the persons involved, the possible damages, as well as the possible consequences and liabilities for the Company.

The task of the investigator shall be to conduct the investigation procedure in all its phases, carrying out, by himself or with the support of third parties, the necessary diligences and actions to clarify the facts.

The decision to outsource the function of Instructor to a third party expert shall be evaluated in each case, depending on the complexity of the investigation, ensuring the independence, objectivity, confidentiality and technical knowledge of the third party expert. The performance of certain procedures or measures to be carried out as part of the investigation may also be outsourced to a third party.

7.5. Development of the research

7.5.1. Principles and safeguards that govern the conduct of the investigation

Internal investigations shall be conducted regardless of the position, title, type and duration of the relationship of the persons under investigation with the Company.

The rights of the subjects involved in the investigation must be respected at all times, and in particular the right to confidentiality and the protection of personal data, privacy, honour, the presumption of innocence and the right not to retaliate against both the informant in good faith and the person under investigation and the persons who have given testimony in the internal investigation process.

Guarantee of confidentiality

Confidentiality of the identity of the informant and of any third party mentioned in the Alert is guaranteed in any case.

The identity of the informant shall not be disclosed to the person under investigation, except with the prior express written consent of the informant.

Access to the informant's personal data shall be restricted (i) to the members of the Committee, being the body designated as the Internal Information System Controller, (ii) to any data processors that may be appointed (which shall include external third parties that may be contracted to support the instructor) and, where appropriate, (iii) to the data protection officer.

For further information on the processing of personal data, this Procedure refers to the Channel's Privacy Policy.

Guarantee of non-retaliation

Retaliation, including threats of retaliation and attempted retaliation against persons who report in good faith any violation within the material scope of the Ethical Channel General Policy is expressly prohibited.

For further information, see Section 4.7 of the Policy.

Other rights and guarantees of the investigation procedure

Effective guardianship: The exhaustive analysis and resolution of any Alert submitted through the Ethical Channel, as well as of any data, information or document provided, is guaranteed.

Necessity and proportionality: The collection and gathering of data and information during the processing of the Alerts' investigations (i) will be limited to what is strictly and objectively necessary for their proper processing, as well as to verify the reality of the facts reported; (ii) will be processed at all times in accordance with the applicable personal data protection regulations, for legitimate and specific purposes, without being used for purposes incompatible with said aim; and (iii) will be adequate and not excessive in relation to the aforementioned ends.

Impartiality: Alerts will always be handled fairly, impartially, with integrity, objectivity, independence and honesty.

7.5.2 Rights of the persons under investigation

The person under investigation shall have the right to:

a) Be informed of the existence of the opening of a case and the reasons for it: The Instructor shall contact the person(s) under investigation as soon as possible, identifying himself to them as the person responsible for the investigation and making it clear that under no circumstances does he act as legal advisor to the person under investigation.

The person under investigation shall be informed of the facts attributed to him or her, but in no case shall the identity of the informant be communicated to him or her unless the written consent of the informant has been obtained in advance.

Such communication to the investigative target may only be delayed if it is considered that there is a reasonable risk that it would compromise the proper conduct of the investigation, in particular the company's ability to investigate effectively or to gather relevant evidence in order to establish what has happened.

b) Presumption of innocence: All persons are innocent with respect to any information communicated through an Alert until proven guilty after the investigation and its termination.

c) Consultation of the file: the person under investigation shall have access to the information in the file and the documents of the investigation, as soon as possible, ensuring that this right does not conflict with the guarantee of confidentiality of the informant who has made the communication, which must be preserved in any case, nor with the proper conduct of the investigation.

d) Right to contradiction: the possibility for the person under investigation to provide all the information he/she deems necessary and to make allegations must be guaranteed, while at all times respecting the right to defence and, in particular, the principle of contradiction and to be heard at any time, which shall take place at the time and in the manner deemed appropriate to ensure the proper conduct of the investigation.

e) Non-declaration and/or silence and non-confession of facts: the person under investigation has the right not to declare and/or remain silent on all or some of the matters from which an assumption of responsibility may arise, and not to confess responsibility for the facts under

investigation. Any person under investigation shall be informed that the acknowledgement of the facts will not exonerate him/her from possible responsibilities, although it may mean the mitigation of such responsibilities.

f) Data protection rights: the data subject shall be informed of his or her data protection rights and shall be provided with a copy of the Channel's Privacy Policy

g) Legal assistance: the person under investigation may appoint a lawyer of his or her confidence to accompany and advise him or her in investigations where the facts could constitute a criminal offence.

h) Counselling: during the investigation procedure, the person under investigation may be counselled by the Workers' Representatives.

7.5.3. Obligations of employees and managers

Any employee and manager of the Himoinsa Group has the obligation to collaborate with the Committee for the correct and adequate processing of the investigation, and to this end they shall have the following obligations:

a) Duty to cooperate: in order to facilitate the investigation, all Company staff must cooperate with the Instructor, who may request cooperation, information, documentation and technical support from them.

b) Duty of diligence: all questions posed to Company personnel in the context of their obligation to cooperate with the investigation must be answered diligently, truthfully and completely, and silence or evasive answers shall be considered as non-diligent information.

c) Confidentiality: Company employees who collaborate in the investigation must preserve the confidentiality of all data, documents, information and actions of which they have knowledge, directly or indirectly, as a result of their participation in the investigation. Likewise, they shall comply with the personal data protection requirements of the regulations in force.

7.5.4. Investigative measures

By way of an illustrative, non-exhaustive list, some of the steps that can be taken in the investigation are detailed, which must at all times comply with the principles, requirements and fundamental rights regarding the gathering of evidence in order to avoid its possible unlawfulness:

a) Interviews with the informant, the investigated and witnesses:

The investigator shall interview the informant, the person under investigation and, where appropriate, the witnesses whose testimony is considered relevant to the knowledge of the alleged facts (hereinafter "interviewee(s)").

These interviews may be in person, by videoconference or even by telephone, depending on the circumstances and the geographical location of the parties involved, at the discretion of the investigator of the case. It will only be compulsory to conduct the interview in person when expressly requested by the informant or the person under investigation.

As a general rule, the interview with the informant, the person under investigation and, where appropriate, with witnesses is compulsory during the course of the investigation, with the investigator being empowered to specify the most suitable time for it, being able to postpone it whenever it is reasonably considered that it may compromise the success and effectiveness of

the internal investigation in progress, hinder the collection and analysis of necessary evidence or prevent the effective execution of the measures that may be agreed by the investigator.

All interviews shall be recorded, subject to the consent of the interviewee, who shall be provided verbally at the beginning of the interview or in writing with information on the processing of their personal data, to be subsequently transcribed completely and accurately by the instructor; the transcript of the conversation shall be offered to the interviewees so that they may check it and, if they are in agreement, accept it by signing it. Once the transcript has been signed, the recording of the conversation shall be destroyed.

In the event that the interviewee refuses to have the interview recorded (which shall be expressly stated orally at the beginning of the recording or at an earlier time in writing), the instructor shall draw up a record of the meeting, which shall subsequently be sent to the interviewee by any means (preferably by e-mail) for reading and review. In the event that the interviewee raises objections, nuances, comments or points out errors, the trainer shall decide whether to accept them by amending the minutes where appropriate. In the event that the Instructor does not accept all or any of the interviewee's indications, he/she will note this at the end of the record by means of the appropriate "Record of the Interviewee's Objections to the Interview Record prepared by the Instructor". This new version of the record shall be sent again to the interviewee without the possibility of making or introducing new changes.

b) Analysis and request for information and/or documentation:

The instructor will analyse in detail the information and/or documentation provided in the Alert, as well as any additional information and/or documentation requested from the informant, other members of the Himoinsa Group or third parties.

The instructor may request, through the Committee, from any corporate body, department, area, management or personnel of the Himoinsa Group any information and/or documentation related to the business activity that is necessary, proportional, reasonable and essential for a proper investigation, without the need to justify and provide the reasons for the request to the person to whom it is addressed, beyond their appointment as the instructor of an investigation file by the Chairman of the Committee. Any request for information and/or documentation shall be made in compliance with the regulations on the protection of personal data and the labour regulations applicable to the case.

c) Obtaining digital evidence of equipment and technological and IT resources of the Himoinsa Group.

Obtaining, as part of an investigation file, digital evidence relating to Group information (work documents, files related to the activity, emails of a business nature from the corporate email account, etc.) contained in the technological and computing equipment and resources (fixed or laptop computer, smartphone, or corporate email account) owned by the Group and provided to the person under investigation for the performance of his work (or that contained on the servers of a Group company as a result of the execution of the appropriate back-ups provided for in the Information Security Policy), shall require the prior express approval of the Chairman of the Committee.

This Diligence may only be agreed when it has been duly assessed that its practice is strictly necessary, proportional and convenient for the good outcome of the internal investigation due to

there being no other type of suitable and less intrusive diligence and, in any case, it shall be carried out without prejudice to the rights to confidentiality of communications and personal privacy of the person under investigation and those of third parties potentially affected by it, and respecting the applicable legislation in force, especially with regard to that which is applicable to the internal investigation, it shall be carried out without prejudice to the rights to secrecy of communications and personal privacy of the person under investigation and those of third parties potentially affected by the same and respecting the applicable legislation in force, especially with regard to the protection of personal data, the rights to privacy and personal intimacy and other rights recognised in the applicable legislation in the specific case.

This Diligence shall be carried out, in any case, in accordance with the following rules:

a) Access to the aforementioned technological and IT tools or resources owned by the Group shall be carried out in accordance with the best technological and digital practices, guaranteeing the timely traceability, chain of custody and inalterability of the digital evidence obtained, minimising as far as possible any interference with the personal privacy of the person under investigation and, if technically possible due to the availability of the necessary tools for this purpose, through the use of "keywords" or any other methodology designed for this purpose.

b) If, in the opinion of the investigator, this does not hinder the internal investigation in progress, the person under investigation may be allowed to be present at the time of access, which shall in any case be carried out in a respectful manner and with due consideration, keeping the necessary confidentiality of the data, documents and other information to which access may be obtained.

c) In view of the circumstances of the case and taking into account the seriousness of the facts that are the object of the internal investigation, at the discretion of the investigator, at the time of access, it may be proposed to take a testimonial proceeding - in addition to the technological proceeding - in which at least one member of the body representing the employees of the Company of the Group in question (if any) or, failing this, two employees not affected by the Internal Investigation, shall be called.

The practice of any type of Internal Investigation Diligence that may involve or entail the interception of a communication in progress or the use of technical devices for listening, transmission, recording or reproduction of sound or image to discover the secrets or violate the personal privacy of an employee, manager or director of the Himoinsa Group and without their consent, without prejudice to the lawfulness of the installation of video surveillance systems in accordance with the regulations in force and to safeguard the legitimate interests of the Himoinsa Group, is prohibited in all cases.

d) Technical or expert opinions or reports:

During the course of the internal investigation, the Instructor may request an opinion or technical report from another member of the Himoinsa Group that may be appropriate, necessary and essential for a proper investigation of the reported facts, after verifying that the person in question is not subject to a possible cause for abstention or recusation as provided for in this procedure, and in accordance with the following rules:

a) The Instructor shall inform the Chairman of the Committee of the need for and the necessity of carrying out this Diligence, subject to the latter's decision on whether or not it is appropriate.

b) In the relevant assignment, which shall necessarily be in writing, the investigator shall indicate to the person selected from the Panel to be involved the time limit within which he/she has to prepare his/her report, as well as warn him/her about confidentiality, independence, objectivity, impartiality and fairness in the cooperation.

c) The technical opinion or report shall also be contained in writing and shall be included in the Complaint file. In addition, and at the Instructor's discretion, the author of the report may be called for an interview in order to ratify it and to answer any questions that the Instructor may raise, and the appropriate minutes shall be drawn up for this purpose in accordance with the rules laid down for the interviews of the informant, the person under investigation and witnesses.

Similarly, at any time during the course of the Internal Investigation, the investigator may request a technical opinion or an expert report from third parties outside the Himoinsa Group when, in order to know or appreciate any relevant fact or circumstance related to the information reported, it is necessary or advisable to have qualified technical or scientific knowledge that no member of the Group has, or when, due to the specific circumstances of the case, it would be appropriate to obtain the opinion of a third party outside the Group. The following rules shall apply to the performance of this due diligence:

a) The instructor shall obtain the written approval of the Chairman of the Committee

b) The professional engagement letter or fee proposal submitted by the selected professional must in any case be approved by a member of the Committee

d) The contracted third party shall be given appropriate warnings regarding confidentiality, independence, objectivity and impartiality

e) The technical opinion or expert report shall be in writing. The third party author of the opinion or report may be called, at the discretion of the investigating judge, for an interview in order to ratify the opinion or report and to answer, where appropriate, the questions that the investigating judge may raise regarding its content and conclusions. The appropriate minutes shall be drawn up of this interview in accordance with the rules laid down for the interviews of the informant, the person under investigation and witnesses, unless the external third party contracted is a lawyer, in which case both the technical opinion issued and the clarifications requested shall be protected by professional secrecy.

In conclusion, the Instructing Officer must carry out all those procedures that are considered necessary for the determination and resolution of the facts, always respecting the legality and principles that should govern any investigation, as well as the rights of the informant, the person under investigation and other persons involved in the investigation.

7.6. Proposal for a Resolution

Once the investigation phase has concluded, if the investigator considers the facts and the possible non-compliance to be accredited, he/she must prepare a Proposal for Resolution, which must contain, at least, the following information:

1. A summary of the facts complained of and the investigative steps taken.

2. An evaluation of the outcome of the investigative measures carried out in relation to the facts.

3. The facts that he/she considers to be accredited and the person/s that he/she believes may be responsible.

4. Risk to the Organisation:

a) Legal consequences

b) Internal damage.

c) Reputational consequences.

5. The recommended measures:

a) Urgent measures.

b) Preventive, detective or corrective action to avoid recurrence of non-compliance.

In the event that the facts are not duly accredited or do not merit a sanction, it shall be proposed that the investigation file be closed, the informant and the person under investigation shall be informed of this circumstance, and the Proposal shall be included in the file, leaving a record of the acts of investigation carried out.

7.7 Resolution of the Procedure

7.7.1. Responsible body

The Risk and Compliance Committee shall issue the Resolution concluding the investigation process, which may include one of the following decisions:

a) Closure of the file.

b) Approve the Proposal presented by the instructor without introducing changes (which will determine that the Proposal automatically becomes a Resolution) or make the changes it considers appropriate and even indicate the need to carry out Complementary Proceedings, returning the File to the internal investigation phase or the Resolution proposal phase, as appropriate.

For deliberation and decision making, the Risk and Compliance Committee may require the assistance of consultants, service providers or professionals accredited in the subject related to the infringement.

At the meeting of the Committee convened to take the relevant decision, the examiner shall have the right to speak but not to vote, and the Chairman of the Committee shall have the casting vote in the event of a tie.

The Committee's Decisions resolving an Alert file put a definitive end to it, without the possibility of further proceedings.

7.7.2 Actions to be taken in case of non-compliance

In its Resolution, the Committee may decide to adopt preventive, detective or reactive measures in the event of proven non-compliance.

Preventive measures are those intended to prevent the non-compliance from recurring or to minimise as far as possible its probability of occurrence in the future or its impact, such as the approval of new internal rules or modification of existing ones, proposals for organisational changes, establishment of new processes or procedures, programmes or plans, implementation of training, communication or awareness-raising actions, among others.

Detective measures are all those aimed at allowing or facilitating the future discovery or detection of possible non-compliance prior to its occurrence or at a very early stage after its occurrence, such as the establishment of risk indicators and their periodic measurement, the performance of monitoring activities (new or additional to those already in place), the implementation of reinforced systems of authorisations, verifications or conciliations, among others.

Reactive measures are all those aimed at preventing non-compliance from being left without a punitive or compensatory response from a disciplinary, contractual and/or legal point of view. Without being exhaustive or closed, the following are reactive measures that could be adopted by the Committee:

a) Propose to the corresponding Human Resources Department of the Group company to consider the advisability of initiating disciplinary proceedings against the person under investigation (in the event that he/she is an employee of the Group) in case the facts considered accredited in the Resolution of the proceedings could be classified under any of the disciplinary offences typified in the catalogue of sanctions and offences provided for in the labour legislation, collective bargaining agreement or individual contract to which the person under investigation is subject.

b) Propose to the Management the possible exercise of the appropriate contractual rights (including contractual termination and compensation for damages) against the supplier that has incurred (as perpetrator, necessary cooperator or accomplice) in the noncompliance described in the Resolution of the file generated by the reported Alert.

c) Propose to the Legal Department of the corresponding Group Company to evaluate the convenience or opportunity of informing the competent public authorities of the noncompliance and/or the appropriateness or otherwise of taking legal action (including criminal action) against those responsible for the non-compliance.

With regard to this reactive measure, in the event that during the processing of a file it should appear that there is sufficient evidence of the commission of an offence and the identity of the alleged perpetrator, the Committee shall, in the opinion of the Committee and as soon as such circumstances become known as a matter of urgency, agree to the provisional suspension of said file and shall immediately inform the Board of Directors so that they may assess the appropriateness of notifying the competent authorities. In the event that the authorities are notified, the Committee shall agree the definitive suspension and closure of the file.

Without prejudice to the provisions of the legal, conventional or contractual provisions applicable in each case, in the effective adoption of the measures provided for in the preceding sections, especially when they are reactive in nature, the Compliance Unit may make the appropriate recommendations on their modality, typology and intensity, taking into account criteria of

necessity, proportionality and suitability and duly assessing that there is no other alternative means that is less severe for the persons affected by such measures and/or for the Himoinsa Group.

7.7.3 Duration of the procedure

As a general rule, the processing of the investigation files of alerts admitted for processing shall be concluded within the ordinary maximum period of three (3) months from the date of acknowledgement of receipt or, if no acknowledgement of receipt was issued to the reporter, within three (3) months from the expiry of the period of seven (7) days after the communication was made

As an exception, in cases of particular complexity due to the nature of the facts, the difficulty or quantity of investigative measures to be carried out or due to the concurrence of any other similar circumstance, the Chairman of the Committee, at the proposal of the investigator, may agree to extend the ordinary term of the procedure by an additional three (3) months, stating the reasons for doing so.

In the event that the deadline is extended and the Conclusions Report has not been issued by the end of that period, the file shall be archived in the state in which it was at the time the deadline was reached, without prejudice to the instructor informing the Committee of the reasons why the file could not be concluded, and the Committee may adopt such measures as it considers appropriate outside the framework of the Internal Information System.

7.7.4. Concurrence with judicial or administrative proceedings

If, at any time during the course of the investigation, the existence of judicial or administrative proceedings for the same facts becomes known, the investigation shall be suspended and shall only be resumed if there are relevant aspects not decided in those proceedings, which shall be communicated briefly to the informant.

7.7.5 Final communication to the informant and the investigated person

Once the alert investigation file has been concluded and within seven (7) calendar days following the Resolution of the file, the Secretary of the Committee shall send a communication to the informant and the investigated party informing them of the conclusion of the file.

In the communication addressed to the informant, the result of the investigation will be communicated to him/her in a generic manner, indicating the existence or not of non-compliance. In addition, they shall be reminded of their duty to keep confidential any information that may have been brought to their knowledge regarding the processing of the case opened as a result of the Alert they reported, the rights to which they are entitled (especially with regard to the prohibition of retaliation) as well as, where appropriate, the legal warnings and notices regarding the protection of personal data that may be applicable.

The communication addressed to the person under investigation shall inform him/her of the sense of the Resolution issued by the Committee as to the existence or not of non-compliance, whether he/she is considered responsible for such non-compliance and, if so, the measures proposed by the Committee. This communication to the person under investigation may be adapted in time and form to the specific circumstances, especially in the event that disciplinary measures have

been proposed against him/her. In any case, he/she shall be given the legal warnings and notices on personal data protection that may be required.

8. Recording of information

The Committee shall have a Register Book in which the Consultations received shall be reflected and another Register Book, independent of the first one, in which the Alerts received and the internal investigations to which they have given rise shall be recorded, with the following data being filled in:

The Register of Consultations shall contain a record of the following:

a) Date of submission

b) Reference assigned by the Committee

c) Summary of the consultation

d) The decision taken in the admissibility procedure

e) Resolution of the consultation

f) Date of communication to the Consultant

g) Date of closure of the file

The Alert Record Book shall contain the following information:

a) Date of submission

b) Reference assigned by the Committee

c) Typology of the conduct associated with the reported facts

d) Typology of the proceedings carried out

e) Date of Resolution

f) Conclusion on whether or not there is non-compliance and, if so, its typology

g) Measures taken

h) Dates of the final communication to the informant and the investigated person

i) Closing date

These registers shall not be public and only at the reasoned request of the competent judicial authority, by means of an order, and within the framework of judicial proceedings and under the guardianship of that authority, may access all or part of the content of the said register.

9. Archive

All documentation generated in an investigation must be archived by the Risk and Compliance Committee outside the scope of ordinary management and processing of the Ethical Channel, for a maximum period of 10 years, and compliance with the requirements established by personal data protection legislation must be guaranteed at all times, especially integrity, availability, authenticity and confidentiality

10. Relationship with other existing procedures

This Ethical Channel does not cancel or replace other specific procedures that are in place in the company and that do not conflict with the material scope of the Ethical Channel.

11. Existence of external reporting channels to Competent Authorities.

The Ethical Channel, as the Himoinsa Group's internal information system, is the preferred channel for the subjects included in the scope of application of the Channel to report the facts that must be communicated through the Ethical Channel (Sections 2 and 3.2 of the Channel's General Policy).

However, any natural person may report to the Independent Whistleblower Protection Authority or to the corresponding regional authorities or bodies, the commission of any actions or omissions included in the scope of application of the Ethical Channel, either directly or after prior communication through the Ethical Channel.

At the time of approval of this Procedure, the Ministry of Justice has not yet created the Independent Authority for the Protection of the Informant, but the following regional authorities exist and may act within the scope of their competences and territories:

The Anti-Fraud Office of Catalonia: https://www.antifraud.cat

The Office for the Prevention and Fight against Corruption of the Balearic Islands: https://www.oaib.es

The Andalusian Office against Fraud and Corruption: https://antifraudeandalucia.es

The Office of Good Practices and Anti-Corruption of Navarre (recently created, no website).

The Valencian Anti-Fraud Agency: https://www.antifraucv.es

To the European Union: https://european-union.europa.eu/contact-eu/make-complaint_es

12. Entry into force, revision and updating of this procedure.

This Procedure, previously consulted with the Legal Representatives of the Workers, shall enter into force when the links to this Channel are incorporated into the corporate website and the intranet, which shall be communicated to the interested parties by the ordinary means of dissemination of the Himoinsa Group.

This Procedure must be kept up to date over time, for which purpose it shall be reviewed on an ordinary annual basis, and on an extraordinary basis whenever objective situations or applicable legislation require it, in which case the Risk and Regulatory Compliance Committee shall draw up a proposal for modification and submit it to the Board of Directors for approval.

The Procedure shall also be the subject of appropriate communication, training and awarenessraising actions for its timely understanding and implementation.

Change Control:

Version	Date	Changes introduced	Items affected
2.0 Final Version	21/09/2023	Approval of the original version of the Procedure	All