COMMUNICATIONS MANAGEMENT PROCEDURE

Sercotel
Hotel Group

TABLE OF CONTENTS

1. INTRODUCTION

The SERCOTEL Group has established the following internal communication channel:compliance@sercotel.com (with the option of using regular mail, if the complainant so wishes, by sending a letter to the address: Calle Comte d'Urgell, 240, ático, 08036, Barcelona – for the attention of the Compliance Committee or by telephone; as well as via an internal form available on the intranet through Sercotel Connect and the web form via the link https://www.sercotelhoteles.com/es/compliance) as the preferred channel available to all executives, employees, collaborators, suppliers, and customers, as well as any other third party, to report any concerns regarding a possible breach or violation of the provisions of the Code of Conduct or any other internal policy of the organization, or to report an irregularity they detect in the performance of their duties, as well as any infringement or omission of which they are aware and which may constitute a violation of European Union law or its financial interests, or even criminal or administrative offenses under Spanish law, as explained in the SERCOTEL Group's Internal Reporting System Policy.

This document sets forth the Information Management Procedure, which establishes the necessary provisions to ensure that the Internal Reporting System and the internal communication channel comply with the requirements set forth in Law 2/2023 of February 20, regulating the protection of individuals who report regulatory violations and the fight against corruption.

Although the Internal Communication Channel is the preferred channel, alternatively, any individual may report to the Independent Whistleblower Protection Authority (hereinafter, "A. A. I.") or to the relevant regional authorities or bodies regarding the commission of any act or omission, either directly or after prior communication through the aforementioned internal channel and in accordance with the terms established in the aforementioned Law 2/2023.

2. STAGES OF THE COMMUNICATION MANAGEMENT PROCEDURE

2.1 Receipt of Reports

At Grupo SERCOTEL, the receipt of all communications made through the Internal Reporting System is managed by the Compliance Committee, which, as the CONTROLLER OF THE INTERNAL REPORTING SYSTEM, guarantees at all times respect for independence, confidentiality, data protection, and the confidentiality of communications, and has access only to the organization's internal channel, which is accessible via the email addresscompliance@sercotel.com , postal mail, or the forms available on the intranet and website.

Such communication must be in writing and may be anonymous or named; in any case, it must be confidential and include a description of the facts, the identification of the persons involved, and, if possible, evidence supporting the alleged breach, along with an explanation of the circumstances under which the reporter obtained such information.

Communication may also take place verbally, in person, or by telephone.

Likewise, the whistleblower may request an in-person meeting with the Head of the Internal Reporting System, which will be held within a maximum of seven (7) days from the request, in the manner the Head deems most appropriate and while preserving the confidentiality of the information. The information received during this meeting will be recorded, and the whistleblower will be notified of this in advance. The whistleblower will also be informed about the processing of their personal data in accordance with the provisions of Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016, Organic Law 3/2018 of December 5 on the Protection of Personal Data and the Guarantee of Digital Rights, Organic Law 7/2021 of May 26 on the protection of personal data processed for the purposes of preventing, detecting, investigating, and prosecuting criminal offenses and enforcing criminal sanctions, and the aforementioned Law 2/2023. Alternatively, the meeting may be documented through a complete and accurate transcript of the conversation. Following this referral, its processing and management shall be carried out in accordance with this Procedure.

If a report is received through internal channels other than those established by the Group or is addressed to staff members not responsible for processing it, the organization nevertheless guarantees confidentiality, noting that any breach would constitute a very serious violation of the law and that the report is immediately forwarded to the System Administrator.

Once a report or information is received, the Compliance Committee, as the System Administrator, is the body responsible for initiating the corresponding investigation process, if applicable, to clarify the facts that are the subject of the report.

The Compliance Committee, as the Internal Reporting System Manager, guarantees at all times respect for independence, confidentiality, data protection, and the secrecy of communications.

Within seven (7) calendar days of receiving the report, an acknowledgment of receipt is sent to the whistleblower. This acknowledgment of receipt is included in the file and must, in all cases, contain clear and accessible information regarding external reporting channels to the competent authorities.

In cases where issuing an acknowledgment of receipt could jeopardize the confidentiality of the report, to ensure confidentiality, it will not be issued until a period deemed prudent has elapsed.

As mentioned in the preceding paragraphs, as an alternative to this preferred internal channel, any act or omission that may constitute one of the violations reportable through the Internal Reporting System[1], either directly or after prior reporting through the aforementioned internal channel, in accordance with the provisions of Annex 1 regarding external reporting channels.

[1] For more information, see Section 3, “Content of Communications,” of the Internal Reporting System Policy.

2.2 Admission Procedure

Upon receiving the report, the System Manager (the Compliance Committee) assigns it a REGISTRATION NUMBER corresponding to its FILE and a series of CODES to anonymize the whistleblower, the subject of the investigation, the facts, and any other third party that may be affected by the report.

As it is a collegiate body, the System Manager delegates, depending on the nature or subject matter of the report, the authority to manage the Internal Reporting System and handle investigation files to one of the members of the Compliance Committee.

If the Compliance Committee determines that the reported facts may constitute a crime based on prima facie evidence, it immediately forwards the information to the administrative body, which must decide whether to immediately refer the matter to the Public Prosecutor's Office.

It is verified that none of the members of the Compliance Committee is implicated in said report. If that were the case, the Board of Directors is informed and the implicated person is removed from the proceedings. If it is necessary to replace the affected person, the Compliance Committee shall designate the replacement for the purpose of continuing the investigation in the manner most appropriate to the interests of the parties involved. Such replacements and new appointments shall be recorded in writing in the minutes and at the opening of the file.

Finally, upon receipt of the report, the System Administrator records the following information:

- The objective details of the report: facts, dates, names, amounts, locations, contacts, etc., provided by the person making the report.
- The subjective details: opinions, rumors, ideas, and assessments that the whistleblower deems necessary in the account of the report.
- The Compliance Committee's assessment of whether the report is related to a potential or alleged violation or whether it is merely a complaint or suggestion regarding improving a business area, the work environment, etc.

2.3 Investigation Process

If the report is accepted for processing, the investigation is led by the System Manager's Representative and conducted by the System Manager.

First, and following agreement with the whistleblower, any preventive precautionary measures deemed appropriate are taken.

If possible, the whistleblower may be asked to provide additional information necessary for the investigation prompted by their report.

At this stage, the PERSON UNDER INVESTIGATION is notified and INTERVIEWED, and informed of their right to be informed of the actions or omissions attributed to them, and may also exercise their right to be heard, without under any circumstances being informed of the identity of the whistleblower.

Any third parties involved (if any) are also summoned and interviewed so that they may explain and present the arguments they deem appropriate. As many investigative procedures as necessary for the parties will be carried out, and a documentary record of all actions taken will be kept in the file.

Any proceedings conducted with third parties or other bodies, areas, or departments of the SERCOTEL Group must be carried out while maintaining the anonymity of the INFORMANT and the PERSON UNDER INVESTIGATION, as well as the reasons for the communication.

The confidentiality of information is guaranteed at all times, as are the presumption of innocence and respect for the honor of all individuals involved.

During this stage, the Compliance Committee:

1. Investigates the reported facts and, specifically:

- The objective and subjective elements provided by the whistleblower, prioritizing objective elements supported by documentation that substantiates, in whole or in part, the reported facts.
- The reputation, integrity, and reliability of the whistleblower.

- The allegations and exculpatory evidence provided by the person under investigation.
- The evidence gathered from third parties, or from other related bodies, areas, or departments.

2. Analyze and assess the potential consequences that the reported facts may entail:

First, the Compliance Committee verifies whether these facts occurred due to a significant lack of internal controls within the Group. If so, it will propose urgent remedial and preventive measures to avoid new risks.

Second, if the seriousness, nature, or complexity of the facts so warrants, the Compliance Committee may appoint another senior executive or a specialized third party to assist with the investigation. Likewise, if the reported facts could result in asset losses, the Compliance Committee takes measures to halt or mitigate such losses. If there is a risk of the loss or destruction of evidence relevant to the report, the Compliance Committee secures such evidence prior to the start of the investigation. The Compliance Committee also assesses the appropriateness of informing the governing bodies about this report. Finally, it assesses whether harm may have been caused to third parties; if so, it evaluates the extent of the harm and the need to inform the affected third party.

The timeframe for conducting the investigation and providing a response to the whistleblower regarding the actions taken, as well as the results thereof, depends on the severity of the reported facts and their potential consequences, with the duration of this stage being at the discretion and risk of the Compliance Committee. However, in accordance with the provisions of Article 9.2. d) of Law 2/2023, of February 20, regulating the protection of persons who report regulatory violations and the fight against corruption, this period may not exceed three (3) months from the receipt of the report or, if no acknowledgment of receipt was sent to the whistleblower, three (3) months from the expiration of the seven (7)-day period following the submission of the report[2] . This does not apply in cases of particular complexity, in which the deadline may be extended by up to an additional three (3) months.

If the report contains personal data of third parties other than the person under investigation (e.g., witnesses, suppliers, customers, etc.), the Compliance Committee will document in writing that all personal information provided that is not necessary for the investigation must be redacted, and will proceed to notify the third parties whose data will be processed. The information will comply with the disclosure requirements of data protection regulations, omitting the identity of the whistleblower, which must remain confidential.

All such notifications are decided by the Compliance Committee in its capacity as System Administrator, are recorded in writing in the file, and are processed via the email address compliance@sercotel.com.

2.4 Conclusion of Proceedings

Following the investigation of the report and based on the supporting documentation used to clarify the facts, a VERDICT or RESOLUTION is drafted and approved by an extraordinary meeting of the Compliance Committee, containing the following:

- Description of the facts: report reference number; date of the report; facts reported; parties involved; documentation provided throughout the investigation by both parties (the whistleblower and the subject of the investigation), by other bodies, areas, or departments, or by third parties; interview with the subject of the investigation and/or with third parties, etc.
- Analysis and assessment of the evidence obtained.
- If the reported irregularity is indeed confirmed, the Compliance Committee will dedicate a section of the verdict to making the recommendations it deems necessary to implement in order to improve the internal controls and protocols that were deficient on this occasion.

[2] These deadlines shall be met, in any case, without prejudice to the provisions of the labor regulations or collective bargaining agreement applicable to each case, the deadlines of which shall prevail in the event of a conflict.

- Resolution: Upon approval by the governing bodies, this resolution is substantiated and contains the reasons why the case is DISMISSED WITHOUT PENALTY or DISMISSED WITH PENALTY.

I. CLOSURE WITHOUT PENALTY: Following the investigation, if it is concluded that the reported violation is clearly minor and does not require further follow-up, the case is CLOSED. The case shall also be closed in instances of repeated reports that do not contain new and significant information regarding violations previously reported and for which the investigation procedure has already concluded, unless new factual or legal circumstances arise that justify a different course of action. In such cases, the decision must be communicated to the whistleblower and must be substantiated.

II. CLOSURE WITH SANCTION: The Committee may propose the imposition of a sanction, but the decision rests with the governing body in coordination with the human resources department, in accordance with the procedures established for the imposition of disciplinary sanctions within the organization.

III. NOTIFICATION TO THE AUTHORITIES: If a report received initially appears to be related to the commission of a crime, the Compliance Committee will immediately bring it to the attention of the board of directors for the purpose of evaluating whether to file a complaint with the Public Prosecutor's Office.

In this regard, Article 259 of the Spanish Criminal Procedure Act provides that anyone who witnesses the commission of any public offense[3] is obligated to immediately report it to the investigating judge, of

[3] The classification of a crime as a public offense relates to who initiates its prosecution (ex officio or at the request of the injured party), with public offenses being prosecutable ex officio without the need for a prior complaint by the injured party. In addition to crimes against life and liberty, the list of crimes that give rise to criminal liability for legal entities includes, by way of example, the following public offenses: fraud, bribery, influence peddling, money laundering, terrorist financing, crimes against the Treasury and Social Security, crimes against the environment and natural resources, crimes against land use planning, crimes against fundamental rights and public freedoms, and smuggling, among others. In contrast, private offenses include slander and libel between private individuals (the courts may only act when the injured party files a complaint or a civil suit), and semi-public offenses are prosecutable ex officio once the injured party has initially filed a complaint (offenses involving the discovery and disclosure of secrets, intellectual property offenses, assaults, sexual harassment, and sexual abuse, among others).

the local, regional, or municipal police, or the law enforcement officer nearest to the location where the person is found, under penalty of a fine of 25 to 250 pesetas[4] .

However, the duty to report to the competent authorities is heightened with respect to certain crimes specified in criminal law. In this regard, the Spanish Criminal Code, in Article 450[5] , addresses the “failure to fulfill the duty to prevent crimes or to promote their prosecution,” penalizing anyone who fails to prevent the commission of a crime that affects individuals’ life, physical integrity, health, liberty, or sexual freedom, when they could do so through immediate intervention without risk to themselves or others, and anyone who, being able to do so, fails to contact the authorities or their agents to prevent one of these crimes, of which they have knowledge regarding its imminent or current commission.

Therefore, if, once the investigation of the facts is completed, their veracity is confirmed, Grupo SERCOTEL will take all necessary measures to put an end to the reported incident and, if appropriate and taking into account the nature of the incident, will apply the actions it deems appropriate as set forth in the disciplinary regulations, current labor legislation, and, where applicable, in accordance with the aforementioned criminal legislation.

Any measures imposed internally shall in no way limit the exercise of legal actions that Grupo SERCOTEL may pursue.

In all cases, the DECISION shall be NOTIFIED to both the whistleblower and the person under investigation, taking into account the maximum period of three (3) months from receipt of the report; the whistleblower shall not be notified if they have waived this right, if contact information is not available, or if the whistleblower is anonymous.

[4] According to the current literal wording of Article 259 of the Spanish Criminal Procedure Act.

[5] Article 450 of the Spanish Criminal Code: “1. Any person who, being able to do so through immediate intervention and without risk to themselves or others, fails to prevent the commission of a crime that affects a person’s life, physical integrity, health, liberty, or sexual freedom, shall be punished by imprisonment for a term of six months to two years if the crime is against life, and a fine of six to twenty-four months in all other cases, unless the crime that was not prevented carries an equal or lesser penalty, in which case the penalty one degree lower than that of the crime shall be imposed. 2. The same penalties shall apply to anyone who, having the ability to do so, fails to notify the authorities or their agents to prevent a crime as described in the preceding paragraph, of which they have knowledge regarding its imminent or current commission.

Following this, the Compliance Committee orders the CASE TO BE CLOSED, in full compliance with current data protection legislation.

In the event of a CLOSURE WITH SANCTION, the notification to the person under investigation shall include the contractual, disciplinary, or judicial measures to be taken.

The SERCOTEL Group guarantees, as set forth in its Internal Reporting System Policy, that no retaliation will ever be taken against any person who, in good faith, reports the commission of an unlawful act, cooperates in its investigation, or assists in resolving it. This guarantee does not apply to those who act in bad faith with the intent to disseminate false information or to harm others. Against such unlawful conduct, the Group will take the appropriate legal or disciplinary measures.

3. RECORDING OF COMMUNICATIONS

The System Administrator maintains a logbook of the information received and the internal investigations that resulted from it, which serves to store and/or retrieve key information about each incident, including the date and source of the original report, the investigation plan, the results of interviews or any other investigative procedures, pending tasks, the final resolution, as well as the chain of custody for any evidence or key information.

4. PERSONAL DATA PROTECTION

As set forth in the SERCOTEL Group Internal Reporting System Policy, the processing of personal data arising from the application of said Policy and this Communications Management Procedure is governed by the provisions of Title VI of Law 2/2023, by the provisions of Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016, by Organic Law 3/2018 of December 5 on the Protection of Personal Data and the Guarantee of Digital Rights, and by Organic Law 7/2021 of May 26

May, on the protection of personal data processed for the purposes of prevention, detection, investigation, and prosecution of criminal offenses and the enforcement of criminal sanctions.

In accordance with the data minimization principle of the General Data Protection Regulation as incorporated into Law 2/2023, Grupo SERCOTEL will process only the personal data necessary for the investigation of the actions or omissions under investigation through the Internal System. Consequently, to the extent that the personal data collected is not deemed necessary or is proven to be inaccurate, Grupo SERCOTEL will proceed to delete it in accordance with the terms established in Article 32 of Law 3/2018[6] .

Likewise, Grupo SERCOTEL may only process special category data[7] when such data is necessary for the adoption of the corresponding corrective measures or disciplinary proceedings that may need to be initiated; otherwise, it must proceed to immediately delete such data in accordance with the terms mentioned above.

Finally, the SERCOTEL Group must ensure that individuals affected by the processing of personal data carried out as a result of the investigation can exercise their rights of access, rectification of inaccurate data, erasure, restriction, data portability, objection, and the right not to be subject to a decision based solely on automated processing. With regard to the exercise of rights, the right of access may not include information about the informant, and the right to object of the persons under investigation may be denied for legitimate reasons.

5. APPROVAL

The Communications Management Procedure has been approved by the Board of

[6] When deletion is warranted, GRUPO SERCOTEL will block the data by taking all necessary measures to prevent the processing of the blocked information (except when making it available to judicial authorities, the Public Prosecutor's Office, or competent public administrations for the purpose of establishing potential liability) for the time necessary to preserve evidence of the system's operation, which, considering the statute of limitations set forth in Law 2/2023, is established at 3 years. It should be noted that the obligation to block and retain data does not apply to personal data contained in communications that are not under investigation; such data may only be retained in anonymized form.

[7] Personal data revealing ethnic or racial origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data, data concerning a person's health, sex life, or sexual orientation.

Administration of Sagatu Asociados Comercial Hotelera, S.L.U. and may be modified for the purpose of improving confidentiality and the effectiveness of the management of communications processed.

Likewise, this Procedure is reviewed and/or modified by the COMPLIANCE COMMITTEE, which may outsource the service to specialized professionals:

- Whenever significant changes occur in the organization, the control structure, or the activities carried out by the entity that warrant such action.
- Whenever legal changes make it advisable to do so.
- Whenever significant violations of its provisions come to light that likewise warrant such a review.

It is also reviewed, even if none of the circumstances described above occur, at least once every two years.

6. VERSION HISTORY

Version	Date	Approved by	Reason for change
Original V.	06/10/2021	Compliance Committee and Board of Board	
V.1.	07/19/2023	Board of Directors of Sagatu Asociados Comercial Hotelera, S.L.U.	Compliance with Law 2/2023
V.2.	10/04/2023	Compliance Committee	Change of address registered
V.3	12/16/2024	Compliance Committee	Amendment to Art. 2.1
V.3	01/29/2025	Sagatu Board of Directors Asociados Comercial Hotelera, LLC	Amendment to Article 2.1

7. APPENDIX 1. EXTERNAL INFORMATION CHANNELS

7.1 External reporting channel of the Independent Whistleblower Protection Authority (A.A.I.)

Any individual may report to the A.A.I. or to the relevant regional authorities or bodies any acts or omissions referred to in the GRUPO SERCOTEL Internal Reporting System, either directly or after first reporting through the internal channel.

Specifically, in the Autonomous Community of Catalonia, the competent body in this matter is the Oficina Antifrau de Catalunya[8], which has set up an anonymous reporting mailbox, guaranteeing at all times both the confidentiality of communications and the anonymity of the whistleblower, available via the following link:

https://www.antifrau.cat/es/comunicaciones-anonimas

Oficina Antifrau de Catalunya

Quiénes somos Qué hacemos Recursos Prensa Transparencia Trámites Corrupción Denuncia Preguntas **Sede electrónica**

Denuncia / Buzón de denuncias anónimas

Buzón de denuncias anónimas

El buzón de denuncias anónimas garantiza en todo momento la confidencialidad de las comunicaciones y el anonimato del denunciante.

Usted tiene dos opciones para realizar la denuncia de forma anónima mediante este canal:

—Utilizando su navegador. En este caso, queda rastro de la dirección IP desde la cual se realiza la comunicación.

—Utilizando **una red de anonimización, que garantiza plenamente el anonimato** de la comunicación en el entorno digital (también de la dirección IP, que puede identificar a quien navega por Internet). **La herramienta más utilizada para ello es la red TOR.** Como cualquier otro navegador, para hacer uso de la herramienta TOR es necesario descargar el navegador desde la **página de descarga**. Este **enlace** muestra un **vídeo tutorial** sobre cómo descargar TOR.

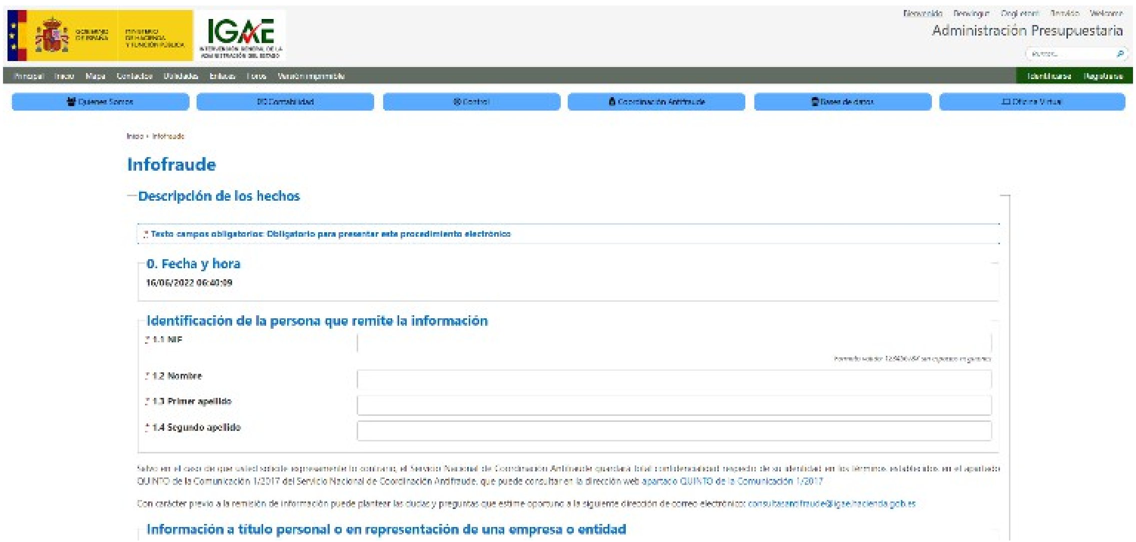
[8] https://www.antifrau.cat/es/es

7.2 Infofraude

The National Anti-Fraud Coordination Service[9] (SNCS), as the national body responsible for coordinating actions aimed at protecting the financial interests of the European Union, and reporting to the General State Audit Office, enables citizens to report any facts of which they are aware that may constitute fraud or any other irregularity in connection with projects or operations financed with funds from the European Union.

Thus, the form for reporting fraud and irregularities (also known as infofraude) is available on its website and can be used with a guarantee of confidentiality:

https://www.igae.pap.hacienda.gob.es/sitios/igae/es-ES/snca/Paginas/ComunicacionSNCA.aspx



[9] https://www.igae.pap.hacienda.gob.es/sitios/igae/es-ES/snca/paginas/inicio.aspx