PROCEDURE FOR MANAGEMENT OF REPORTS

PR-CPL-03

Note:
The printed copy of this procedure may be out of date. Please be sure to check the database of policies and procedures on the website to verify that you are consulting the most up-to-date version of the policy or procedure.

- **Control of versions**

Version	Date	Author	Changes
1.0	July 2017	Hotel Investment Partners, S.L.	Initial version
2.0	October 2017	HI Partners Holdco Value Added S.A.	Separation of the hotel business
3.0	January 2019	HI Partners Holdco Value Added S.A.	Updating of the Model for Compliance and Prevention of Criminal Risks
4.0	December 2019	Hotel Investment Partners S.A.U.	Change of company name
5.0	November 2021	Hotel Investment Partners S.A.U.	Internal changes and adaptation to the Whistleblowing Directive
6.0	April 2022	Hotel Investment Partners S.A.U.	Adaptation to the SGCP (Criminal Compliance Management System) and SGAS (Environmental and Social Management System)
7.0	June 2023	Hotel Investment Partners S.A.U.	Adaptation to Law 2/2023

- **Approvals**

Approving body	Entity	Date
Management Committee	Hotel Investment Partners, S.L.	13 September 2017
General Meeting of Shareholders	HI Partners Holdco Value Added SAU Approval of separation of the hotel business (universal succession)	4 October 2017
Board of Directors	HI Partners Holdco Value Added, S.A.	25 February 2019
Board of Directors	Hotel Investment Partners S.A.U.	20 December 2021

Management Committee	Hotel Investment Partners, S.L.	26 June 2023
Board of Directors	Hotel Investment Partners S.A.U.	28 June 2023
Board of Directors	HIP History Hotels, S.L.U.	28 June 2023
Board of Directors	HIP History Hotels I, S.L.U.	28 June 2023
Board of Directors	HIP History Hotels II. S.L.U.	28 June 2023

CONTENTS

I. DEFINITIONS

The "**Internal Information System**" or "**IIS**" is the ordered set of procedures, standards and policies that regulate the various channels of communication for the company (HIP) so that it can appropriately manage notifications received, thus complying with applicable laws and regulations.

The **"Whistleblowing Channel**" is the internal information channel made available by HIP to employees and third parties as the preferred channel for the presentation of communications by Whistleblowers, and for making queries about the content and scope of the Codes and Policies and other internal regulations. This channel is available to employees and to any third parties on HIP's website: https://hipartners.integrityline.com/

"**HIP**" has the meaning given to it in section II.

"**HIP Group**" has the meaning given to it in section II.

"**Incident**" for the purposes of this procedure, means the actual, suspected or alleged occurrence of an infraction (or a query, suggestion or concern relating thereto):

(i) of European Union law as included in Directive 2019/1937, and/or

(ii) of Spanish laws and regulations, whether it be a serious or very serious criminal and/or administrative infraction (some examples of all these are to be found in Title IV (a) of this document), and/or

(iii) Of HIP's Code of Conduct and other internal regulations of the HIP Group,

deriving from an act of a person or company linked to HIP in some way (in the meaning explained in Title IV (a) of this procedure).

"**Whistleblower**" means the person reporting an Incident to the company (or some query, suggestion or concern relating to an Incident), whether demonstrable or not and subject to this person's possibly being mistaken, providing he or she acts in good faith and in accordance with this procedure.

"Head of the IIS" means the person (if a single-person body) or persons (if a collegiate body) responsible for the IIS within the company. In the case of HIP this function has been entrusted to the Chief Compliance Officer (CCO).

II. OBJECTIVE

Hotel Investment Partners, S.A.U. ("**HIP**") and its group of companies ("group" being given the meaning attributed to it in Article 42 of the Commercial Code), as well as all companies managed by HIP (the "**HIP Group**"), must operate fairly, with integrity and strive to maintain a position of leadership, prestige and reputation. The unprofessional conduct of an employee, manager or collaborator may damage the

reputation of the HIP Group and expose it and the corresponding employee to possible sanctions. For this reason, HIP works actively to prevent and avoid this possibility.

Thus all managers, employees and other members of the HIP Group who act in the name and/or on behalf of the HIP Group are required to comply at all times with (i) the laws in force, (ii) the Code of Conduct (a document that is accessible on HIP's corporate website) and (iii) internal policies and procedures. In this work of prevention the cooperation of all managers, employees and collaborators of the HIP Group in detecting possible irregular behaviours is also of great importance.

The purpose of this procedure is to:

a) encourage employees to report suspected irregularities (*Incidents*).
b) establish the manner in which reports reaching the IIS are received, and how they will be managed up to the investigation phase.
c) ensure that all persons within the scope of the IIS (potential Whistleblowers) can express their concerns without fear of reprisal, even if they prove to have been mistaken, and with guarantees of confidentiality on the part of the company.

To strengthen and ensure the proper management and confidentiality of any report of an Incident, **HIP has contracted a specific software application for the sending and receipt of reports (including anonymous ones), which is available on HIP's website, the so-called Whistleblowing Channel.**

This procedure has also been adapted to the new regulations on the protection of whistleblowers introduced by means of Law 2/2023 of 20 February regulating the protection of persons reporting regulatory infractions and on the fight against corruption. This Law seeks to makes sure that infractions of European Union Law as included in Directive 2019/1937, and serious or very serious criminal and administrative infractions occurring in an organisation can be reported both internally and to the authorities through channels that ensure Whistleblowers' security and protection and without their having to fear reprisals.

To make sure that all members of the organisation are familiar with the channels of communication available and the procedures regulating their functioning, they are made available to them when they join the organisation, and the use of these channels is promoted through communication plans and training.

III. RESPONSIBILITIES WITHIN THE IIS

a. Head of the IIS

- To receive and evaluate communications and handle them.
- To conduct the investigation and issue the report in accordance with "PR-CPL-08: Procedure for managing investigation".

- Draw up periodic reports containing the communications received through the various channels.

b. Senior Management

- To authorise the use of resources for the proper operation of the whistleblowing channel, including the independence of actions.

c. Persons concerned within the scope of the IIS (potential *Whistleblowers*)

- To report any situation covered by the concept of Incident through the available channels.
- To notify any query, suggestion or concern relating to an Incident through the available channels.

d. Actors external to the channel

- Possible receipt of communications (at the discretion of the Head of the IIS).
- Preliminary analysis of the Incident with the purposes of classifying it in one of the cases included in this procedure.
- Reporting the results of the preliminary analysis to the CCO/Head of IIS as soon as possible.

IV. REPORTING OF INCIDENTS

a. Examples of Incidents

The scope of the IIS encompasses all communications on Incidents, including, but without limitation, the following:

a. Criminal activity (including bribery and/or corruption);
b. Financial fraud or mismanagement;
c. Misappropriation of funds or other form of theft;
d. Falsification of contracts, reports or records;
e. Inappropriate activities of suppliers, contractor or other third parties (such as bribes, illegal commissions, unfair selection processes or failure to report conflicts of interest);
f. Breaches of the Code of Conduct, internal policies, protocols or other internal HIP regulations;
g. Negligence;
h. Failure to fulfil any legal obligation legal or regulatory requirement;
i. Danger to health and safety of employees;
j. Unsafe working conditions;
k. Environmental risks;
l. Bad or inappropriate behaviour;
m. Inappropriate disclosure of confidential information;

n. Violation of the Securities Market Act;
o. Violence or threats;
p. Concealment of any information relating to any of the foregoing matters; or
q. Matters that may pose a serious risk to HIP's reputation.

The IIS must not be used to report events that present an immediate threat to life or property. When emergency assistance is required, the emergency services must be contacted.

The IIS must not be used for complaints relating to one's personal circumstances (unrelated to HIP) or in relation to inter-personal conflicts or rumours, even when they originate or are spread within the working environment.

In the event of any doubts as to the scope of the IIS, advice must be sought through the Whistleblowing Channel or from the Chief Compliance Officer (CCO)/Head of the IIS, whose contact particulars can be found at the end of the procedure, in accordance with this Procedure and as is detailed hereunder.

The IIS is responsible for detecting any irregularity committed by a member of the HIP Group, in the widest sense, be it an employee, manager, director or agent, this latter being understood to mean any third parties and their employees when acting under contract with any company of the HIP Group for the provision of a supply, work or service, for the direct or indirect benefit of any company in the HIP Group and under its instructions and supervision. Specifically, but without limitation, the following:

- Employees with indefinite employment contracts;
- Temporary employees or employees with fixed term employment contracts
- Consultants;
- Contractors;
- Hotel management companies (and their own personnel);
- Tenants/lessees;
- Personnel on secondment;
- Casual employees;
- Suppliers/providers;
- Partners;
- Customers;
- Shareholders;
- Agents;
- Commercial collaborators / service providers
- Those with an employment or statutory relationship that has ended;
- Volunteers;
- Scholarship holders;

- Workers undergoing training;
- Those whose employment relationship has not yet started;
- Legal representatives of persons working in the exercise of their functions of advice and support to the Whistleblower;
- Natural persons who, in the context of the organisation in which the Whistleblower works, assist the Whistleblower in the process;
- Natural persons who are related to the Whistleblower and who may suffer reprisals, as work colleague or relative of the Whistleblower;
- Legal persons for which the Whistleblower works or with which he or she maintains any other kind of relations in an employment context or in which he or she has a significant equity interest.

b. On the obligation to report Incidents and the channels made available

Any person within the scope of the IIS in the terms set forth in section IV (a) above who has knowledge of any situation susceptible of constituting an infraction, or any doubt, suggestion or concern relating to an Incident, must immediately inform the organisation through one of the following channels:

Option 1- Whistleblowing Channel. Incidents, and queries or suggestions will be communicated through the Whistleblowing Channel as the preferred channel of communication, which is duly available and functioning on HIP's website: https://hipartners.integrityline.com/

Option 2-Email. To the email address of the IIS: cco@hipartners.com.

Option 3-by telephone. By calling the HIP switchboard (931 59 57 75), if you wish to make the report by telephone, asking for the CCO/Head of the IIS (Ms Andrea Schröder), within the following times: from 9:00 am to 7:00 pm from Monday to Thursday and from 9:00 am to 3:00 pm on Fridays.

Option 4- in person. At the request of the Whistleblower a face-to-face meeting may be held with the CCO/Head of the IIS, within seven calendar days maximum.

In the last two cases:

(i) The CCO/Head of the IIS must record the particulars of the Whistleblower in writing, together with the date on which the report is made and a summary of the facts reported;

(ii) The Whistleblower must expressly sign this document after reading it and agreeing to it, and is entitled to receive a copy of it; and

(iii) The CCO/Head of the IIS must inform HIP of the Incident through the Whistleblowing Channel.

Any information received from outside is considered valid for taking note of an Incident, especially if it comes from an official source such as a judicial body or a public administration.

Confidentiality is guaranteed for all channels; however the only channel that allows communications with the guarantee of anonymity is the Whistleblowing Channel.

Additionally, these channels will be open to third parties from outside the HIP Group.

As well as the internal communication channels of the HIP Group, the Whistleblower also has available a series of external channels to the competent authorities, notably the following:

- Agencia Estatal de Administración Tributaria (Tax Agency);
- *Oficina Antifrau de Catalunya*. (Catalan anti-fraud office);
- Servicio Nacional de Coordinación Antifraude (National anti-fraud office);
- Fábrica Nacional de Moneda y Timbre-Real Casa de la Moneda (Royal Mint);
- European Anti-Fraud Office.

c. On the reporting of Incidents

All reports received will be treated with absolute confidentiality, and they may be made anonymously. To ensure correct processing, any person reporting an Incident through the Whistleblowing Channel must provide as much information as possible, including, without limitation, the following:

- Information on the Whistleblower (if not opting to send the report anonymously):
    - Company to which he or she belongs
    - Name and surname(s)
    - Email address
- And in any case, information on the person involved in the facts or events forming the subject of the report:
    - Express indication as to whether the person involved in the facts or events forming the subject of the report can be identified (if he or she cannot be identified, the “observations” field will have to be completed.)
    - Full name of the person or organisation affected by the facts or events forming the subject of the report
    - Company to which he or she belongs
    - Department or area
    - Observations (if any)
- Facts or events forming the subject of the report:

- Company in which the Incident occurred
- Department /area in which the Incident occurred
- Place where the Incident was committed
- Description of the Incident *(mandatory)*

The CCO/Head of the IIS of HIP will prepare regular reports which will include all the reports received through the various communication channels. The purpose of these reports is to generate a periodic record of all communications received through the various communication channels made available to Whistleblowers.

In the event that the facts or events could be indicative of the commission of a criminal offence, the Head of the IIS will immediately forward the information to the Public Prosecutor.

d. Prohibition of reprisals

Persons making any kind of report of an Incident, in accordance with these provisions and in good faith, i.e. Whistleblowers, are protected from any kind of reprisal, discrimination or punishment for reason of the reports sent. HIP will sanction any kind of reprisal against good faith Whistleblowers.

Reprisal shall be understood to mean any direct or indirect action or omission taking place in a work context that is motivated by an internal or external communication or a public revelation and that causes or may cause unwarranted harm to the Whistleblower. By way of example, but without limitation:

a) suspension, dismissal, removal or equivalent measures;
b) demotion or refusal of promotion;
c) change of job, change of workplace, reduction of salary or change of working hours;
d) denial of training;
e) negative evaluation or references with regard to the results of the Whistleblowers work;
f) imposition of any disciplinary measure, warning or other sanction, including monetary sanctions;
g) coercion, intimidation, bullying or ostracising;
h) discrimination or unfavourable or unfair treatment;
i) non-conversion of a temporary employment contract to an indefinite one if the worker had legitimate expectations of being offered indefinite employment;
j) non-renewal or early termination of a temporary employment contract;
k) damage, including to reputation, particularly in social media, or financial loss. Including the loss of business and income;
l) inclusion in black lists on the basis of a formal or informal sector agreement that may mean that in the future the person concerned will not be able to find employment in that sector;

m) early termination or cancellation of contracts for goods or services;

n) cancellation of a licence or permit;

o) medical or psychiatric references.

The prohibition of reprisals shall also apply to persons who are related to the Whistleblower and who might suffer reprisals at work, such as the colleagues or relatives of the Whistleblower. Similarly, the protection shall extend to such persons as may have assisted the Whistleblower in the process of communication.

The prohibition of reprisals provided in the foregoing paragraph shall not prevent the adoption of such disciplinary measures as may be appropriate if the investigation determines that the report was false and that the person making it was aware of its falseness, having thus acted in bad faith[1].

In addition to such measures or decisions as may be adopted in any particular process of communication, the protective measures against reprisals will include the following:

a) Whistleblowers will not be considered to have infringed any restriction on the disclosure of information, nor will they be held liable in any way in respect of such disclosure, providing they had reasonable grounds for thinking that the communication of this information was necessary in order to reveal an infraction.

b) Whistleblowers will not be held liable in respect of the acquisition of or access to the information which they report, providing that such acquisition or access does not in itself constitute a criminal offence.

c) In proceedings before a judicial body or other authority relating to harm suffered by Whistleblowers, it shall be presumed that the harm was caused in reprisal for the denunciation. In such cases, it shall be for the person taking the measure that caused harm to prove that this measure was based on duly justified reasons.

d) Whistleblowers shall have access to corrective measures for reprisals, as may be appropriate in each particular case, including provisional measures pending resolution of judicial processes.

e. Confidentiality as to the identity of the Whistleblower

HIP guarantees maximum confidentiality as regards the identity of the Whistleblower. As a means of guaranteeing this confidentiality, it is expressly stated that the exercise of the right of access on the part

[1] In this regard it is pointed out that, in accordance with the provisions of Article 456ff. of the Criminal Code, false accusation or denunciation and simulation of criminal offences are themselves considered criminal offences, punishable by up to two years of prison.

of the person concerned by the communication does not in any case include access to the data relating to the identity of the Whistleblower.

Also, all persons who, by reason of the functions the perform in the HIP Group, have knowledge of the communications made, are obliged to observe professional secrecy as to the identity of the Whistleblower.

V. RECEIPT AND PRELIMINARY ANALYSIS OF REPORTS OF INCIDENTS

a. Acknowledgement of receipt

Upon receipt of any report of an Incident through any of the channels referred to in the Procedure for Management of Reports, the CCO/Head of the IIS or the external advisers, as the case may be, shall issue an acknowledgement of receipt within seven calendar days.

Providing the Whistleblower has identified himself or herself, the investigators shall inform him or her of the collection and processing of his or her personal data, which will be processed confidentially in accordance with the provisions of the laws in force.

b. Request for expansion of the information received

If the CCO/Head of the IIS considers that the information received abut the Incident is insufficient, he or she may ask the Whistleblower to expand it. In such case it is advisable to detail in the request the specific aspects of the information that need to be expanded.

c. Establishment of the dossier and preliminary analysis of the information received

With the information received and the corresponding acknowledgement of receipt, the Head of the IIS will establish an individual dossier for each case, which will be appropriately numbered.

In the event that different reports or communications are received relating to the same fact or event or to related facts or events, the CCO/Head of the IIS may combine the various dossiers.

The CCO/Head of the IIS together with the external advisers, is do decided, shall carry out a preliminary analysis of the Incident report received - or of those that the CCO/Head of the IIS detects by any other means and considers it opportune to investigate - in order to verify the entity concerned by the information, its sufficiency and plausibility and the significance in this context of the fats or event reported, determining whether they may constitute a serious or very serious criminal or administrative infraction of European Union Law as provided in Directive 1937/2019 or of HIP's internal regulations.

Depending on the result of the preliminary analysis, the CCO/Head of the IIS, shall adopt one of the following decisions, issuing the appropriate deed with reasons:

A. Non-admission of the notification and immediate filing of the dossier when:
    a. the facts or event reported are not within the scope of the IIS; or
    b. the content is manifestly irrelevant; the information is insufficient to proceed with any further action; or the facts or events reported are implausible or totally lacking in credibility.

    In such case, the report will be kept in anonymised form in order to for HIP to be able to demonstrate the functioning of its crime prevention model.

B. Admission of the communication and establishment of the corresponding investigation dossier if the facts or events are or it is reasonably foreseen that they will be within the scope of the IIS.
C. If the facts or events reported are not within the scope of the IIS, but constitute or may constitute a breach of the rules of employment subject to sanctions by virtue of the disciplinary regime applicable in HIP, the notification shall be forwarded immediately to the HR Department for them to consider opening a disciplinary dossier in accordance with the established procedure.

d. Information to the Whistleblower on the processing of the dossier

The CCO/Head of the IIS shall inform the Whistleblower of the admission of the communication, its non-admission, the filing of the case or its having been forwarded to another body, as the case may be, and of any additional measure that may have been adopted. However, occasionally the need for confidentiality may prevent the Whistleblowers being given specific details of the preliminary investigation. In any case, the Whistleblower must treat any information on any aspect of the notification as confidential

The obligation of confidentiality shall be conveyed to the Whistleblower by HIP at the time it replies to the communication received.

VI. INVESTIGATION PROCEDURE

If the notification is admitted, the corresponding investigation dossier will be opened. The investigation will be conducted in accordance with the provisions of *"PR-CPL-08 Management of Incidents".*

VII. SPECIAL FEATURES OF THE PROCEDURE IN THE EVENT THAT THE COMMUNICATION SHOULD CONCERN THE CCO/HEAD OF IIS OR A MEMBER OF THE BOARD OF DIRECTORS OF HIP OR OF THE MANAGEMENT COMMITTEE[2]

In the event that the facts or events forming the subject of the report should be directed against or concern the CCO/Head of IIS, he or she may not take part in its processing. In fact in the Whistleblowing Channel the option of excluding him or her from receipt of the report is provided. In the following cases it will be considered that there is a risk of conflict of interest preventing the CCO/Head of the IIS from taking part in the investigation:

- The existence of family ties with the Whistleblower or persons affected by the facts or events forming the subject of the report;
- Being or having been the subject of another report by the Whistleblower;
- Having a direct interest in the facts or events forming the subject of the report;
- Forming part of the area or department affected by the report;
- The existence of manifest enmity with the Whistleblower or persons affected by the facts or events forming the subject of the report;
- Being or having been in a situation of hierarchical subordination with respect to the Whistleblower or persons affected by the facts or events forming the subject of the report;
- Any other circumstance that might prevent the CCO/Head of the IIS from acting independently, impartially and objectively.

The decision as to the existence of a situation of conflict of interest in the person of the CCO/Head of the IIS must be notified prior to the start of the investigation by the CCO/Head of the IIS to the external advisers or to the designated investigating team and the decision will fall to the Management Committee.

If the communication were to concern a member of the Board of Directors of HIP, the CCO/Head of the IIS shall inform the CEO of HIP so that he can help the CCO/Head of the IIS with the selection of the investigating team that can count on the support of the external advisers. If the facts or events forming the subject of the communication were to concern the CEO of HIP, the CCO/Head of the IIS shall inform the remaining members of the Board for the same purposes.

If the communication were to concern a member of the Management Committee of HIP, the CCO/Head of the IIS shall inform the Board of Directors so that it can help the CCO/Head of the IIS with the selection of the investigating team that can count on the support of the external advisers.

[2] This being understood for these purposes to mean any communication concerning a member of the Board of Directors or Management Committee of (i) Hotel Investment Partners S.A.U., (ii) a company in its group and/or (iii) a company managed by Hotel Investment Partners, S.A.U.

VIII. CONTACT

Chief Compliance Officer and Head of the IIS	Andrea Schröder Tel. 931 59 57 75 cco@hipartners.com

IX. PROTECTION OF PERSONAL DATA

The persons sending a communication through the communication channel represent and warrant that the personal data provided are true, exact, complete and up to date, and shall save HIP harmless from any liability that might derive from the breach of these representations and warranties.

The data provided in the context of communications and consultations made through the communication channel, and any updates thereto, will be processed by HIP, with its registered office at Avenida Diagonal, 662 Fl. 2 (Module D), 08034 Barcelona, Tel. 931 59 57 75, whose data protection officer can be contacted at dpo@hipartners.com.

HIP will keep the personal data of the persons concerned by the reports and of the whistleblowers, for such time as may be strictly necessary to decide whether it is appropriate to undertake an investigation into the facts or events reported and, once this has been decided, they will be kept duly blocked in order to comply with such legal obligations as may apply in each particular case.

In any case, the personal data will be deleted in the maximum term of three months from their entering the communication channel, except if they are kept to demonstrate the functioning of HIP's crime prevention model. Once this period has elapsed, the may continue to be processed for the time necessary for the investigation of the facts or events reported, providing they are not kept in the communication channel itself. Reports that have not been processed can be shown only in anonymised form.

The legal basis for the processing of data is to comply with the legal obligation to resolve consultations made, applicable by virtue of the provisions of Organic Law 10/1995 of 23 November on the Criminal Code.

Said personal data will be communicated only to third parties to whom HIP is legally or contractually obliged to provide them, and to the corresponding asset managers in each case and to firms in the judicial sector and in its group of companies to which it has entrusted the provision of consultancy and advisory

services in relation to the management of the channel on behalf of HIP, insofar as necessary for the provision of those services.

In no case will HIP transfer personal data to third countries or to an international organisation, except when strictly necessary and insofar as there is adequate protection and always subject to applicable laws. Only in the event that the factor event reported gives rise to administrative or judicial actions may the data provided be communicated to the competent authorities for investigation and possible sanction.

The rights of access, rectification, suppression, objection, restriction of processing, or to object top processing in the cases legally permitted, as well as the right to portability of the personal data may be exercised, in the terms specified by the regulations in force, by writing to HIP (*by email* - dpo@hipartners.com- *or by post* - Avenida Diagonal, 662, Fl. 2 (Module D), 08034 Barcelona-*, with the reference "Data Protection"*) attaching a photocopy of an ID document and indicating the particular right that you wish to exercise. You also have the right to submit a complaint to the Spanish Data Protection Agency.

The purpose of this processing is the investigation and resolution of inappropriate actions or behaviours, especially in criminal matters and regulatory compliance, as described in this procedure. Its purpose is also the management of consultations, queries and/or proposals for improvement of HIP's systems.