



# Whistleblowing Channel Policy

Explotaciones Turísticas 2021, S.L.U.

26/01/2026

Ver. 1.0



This document is the property of Explotaciones Turísticas 2021, S.L.U..

It is expressly prohibited to copy, disclose or distribute it, in whole or in part, through any type of medium without the express authorisation of the company.

Version control			
Edition	Date	Author	Comment
1.0	26/01/2026	P&C	Initial Edition

Approval Control			
Edition	Date	Approver	Position
1.0	26/01/2026	Francisco Valle Mena	System Manager



## Index

- 1 INTRODUCTION ..... 4
- 2 GENERAL PRINCIPLES ..... 4
- 3 SCOPE OF APPLICATION ..... 5
- 4 INTERNAL INFORMATION SYSTEM ..... 6
- 5 CREATION OF THE INTERNAL INFORMATION ..... 6
- 6 THE PERSON RESPONSIBLE FOR THE INTERNAL INFORMATION SYSTEM..... 7
- 7 PROTECTION OF PERSONAL DATA..... 7
- 8 MEASURES TO PROTECT THE WHISTLEBLOWER..... 8
- 9 MEASURES TO PROTECT AFFECTED PERSONS ..... 9
- 10 APPROVAL, ENTRY INTO FORCE AND DISSEMINATION ..... 9



## 1 INTRODUCTION

The approval of Law 2/2023, of 20 February, regulating the protection of persons who report regulatory infringements and the fight against corruption (hereinafter "Law 2/2023"), requires both the public and private sectors to have internal reporting channels designed and implemented to protect persons who detect potential violations in a work or professional context.

Explotaciones Turísticas 2021, S.L.U., hereinafter MYR HOTELS, through this Policy, undertakes to adopt the necessary measures to prevent any type of retaliation, including threats of retaliation and attempts at retaliation against persons who submit a report, as a means of safeguarding and protecting persons who report in good faith information on acts or omissions that contravene the aforementioned law, the MYR HOTELS Code of Ethics and Conduct or the internal regulations and procedures of this institution.

## 2 GENERAL PRINCIPLES

The purpose of this Policy is to establish the Principles governing the actions of MYR HOTELS in the implementation of the Internal Information System and protection of whistleblowers, in accordance with the provisions of Law 2/2023.

1. We guarantee accessibility to the Internal Information System and protection for whistleblowers: the Internal Information System must allow information about regulatory violations and anti-corruption measures to be communicated, either in writing, verbally or in person, to all persons included in its scope of application.
2. We guarantee, through the independent action of the System Manager, the completeness, integrity and confidentiality of the information, the prohibition of unauthorised access, the long-term storage of the information and respect for good faith. The Internal Reporting System will be managed by the manager with complete independence and autonomy from the rest of MYR HOTELS.
3. We guarantee the confidentiality of the identity of the person reporting and of any person mentioned in the communication, as well as of the actions taken in the management and processing of the same. The internal information channel will even allow the submission and subsequent processing of anonymous communications.
4. We guarantee the protection of the personal data of the persons concerned, in compliance with current legislation in this area.

5. We guarantee the confidentiality of communications.
6. We guarantee the safety and protection of whistleblowers and affected persons.
7. We guarantee the presumption of innocence and respect for the honour of the persons concerned.

### 3 SCOPE OF APPLICATION

a) This Policy applies to all members of MYR HOTELS who report, through the procedures set out herein, any:

- Actions or omissions that may constitute a serious or very serious criminal or administrative offence. In any case, all serious or very serious criminal or administrative offences against or involving financial loss to the Treasury and Social Security shall be understood to be included.
- Conduct that may involve, by action or omission and on the part of a member of MYR HOTELS, events that have an effective impact on the professional relationship with MYR HOTELS of the person to whom the communication refers, related to the commission in a work or professional context of any act contrary to the rules of conduct of the MYR HOTELS Code of Ethics or other provisions of the internal regulatory system.
- Any actions or omissions that may constitute infringements of European Union law.

Members of MYR HOTELS are considered to be those who are employees and collaborators of MYR HOTELS at any given time.

b) This Policy also applies to whistleblowers who, although not members of MYR HOTELS, have obtained information about any of the actions or omissions referred to in the previous section in a work or professional context, including in all cases:

- Any person working for or under the supervision and direction of MYR HOTELS, its contractors, subcontractors and suppliers.
- Persons who have been members of MYR HOTELS in the past, having already terminated their employment or statutory relationship with MYR HOTELS.
- Volunteers and interns, regardless of whether or not they receive remuneration.
- Persons whose employment relationship has not yet begun, in cases where information on infringements has been obtained during the selection process or pre-contractual negotiations.

## 4 INTERNAL INFORMATION SYSTEM

The Internal Reporting System referred to in this Policy is the preferred channel for reporting the actions or omissions provided for in Law 2/2023.

The Internal Reporting System consists mainly of the communication channel set up to receive communications provided for within the scope of this Policy, the System Manager and the management procedure to be followed for processing such communications.

## 5 CREATION OF THE INTERNAL INFORMATION CHANNEL

The Internal Reporting System includes the Reporting Channel, which is the preferred channel for reporting the conduct provided for in section 3 of this Policy.

The aforementioned Internal Information Channel allows:

- a) Communications to be made in writing or verbally, or both, under the conditions set out in Law 2/2023.
- b) When making the communication, the informant may indicate an address, email or secure location for the purpose of receiving notifications.
- c) The submission and subsequent processing of anonymous communications.
- d) To inform those who make communications through it, in a clear and accessible manner, about the external channels of information available to the competent authorities and institutions.
- e) The receipt of any other communications or information not covered by the scope established in section 3 of this Policy, although such communications and their senders will be outside the scope of application and protection provided by it.
- f) Appropriate measures shall be taken to ensure the confidentiality of communications sent through channels other than those established or to members of staff not responsible for their processing (who must immediately forward them to the SII Manager).

## 6 THE DATA CONTROLLER OF THE INTERNAL OF PERSON

1. The persons responsible for the System shall be a collegiate body or person, either internal or external, with the characteristics set out in Article 8 of Law 2/2023.
2. The Independent Whistleblower Protection Authority shall be notified, in accordance with the provisions of Article 8.3 of Law 2/2023, of the appointments of the members of the collegiate body responsible for the System within ten days of their appointment. Their dismissals, resignations and the reasons for them shall also be notified within the same period.
3. In the exercise of their functions, the persons responsible for the System shall not receive instructions from any superior, shall not be subject to hierarchy within the collegiate body, nor may they be removed from their posts for reasons related to their legitimate participation in the internal information system.

## 7 PROTECTION OF PERSONAL DATA

The processing of personal data arising from the application of Law 2/2023 shall be governed by the provisions of the GDPR and Organic Law 3/2018 of 5 December on the Protection of Personal Data and Guarantee of Digital Rights (LOPDPGDD), in compliance with the provisions of Law 2/2023.

The internal information system must prevent unauthorised access, preserve the identity and guarantee the confidentiality of the data corresponding to the persons concerned and any third party mentioned in the information provided, with special attention to the identity of the informant if they have been identified.

The identity of the whistleblower may only be disclosed to the judicial authority, the Public Prosecutor's Office or the competent administrative authority in the context of a criminal, disciplinary or sanctioning investigation, and these cases shall be subject to the safeguards established in the applicable regulations.

If the information received contains special categories of personal data subject to special protection, it shall be deleted immediately, unless processing is necessary for reasons of substantial public interest in accordance with Article 9.2.g) of the GDPR, as provided for in Article 30.5 of Law 2/2023.

In any case, personal data whose relevance is not evident for the processing of specific information will not be collected or, if collected by accident, will be deleted without undue delay.

Communications that have not been processed may only be recorded in anonymised form, without the blocking obligation provided for in Article 32 of the LOPDPGDD being applicable.

## 8 MEASURES TO PROTECT THE WHISTLEBLOWER

Persons who report infringements shall be entitled to the protection measures established in Law 2/2023, provided that the following circumstances apply:

- a) Have reasonable grounds to believe that the information referred to is accurate at the time of communication or disclosure, even if they do not provide conclusive evidence, and that the information falls within the scope of this policy.
- b) The communication or disclosure has been made in accordance with the requirements set out in this policy and in Law 2/2023.

The following persons are expressly excluded from the protection provided for in Law 2/2023:

- Information contained in communications that have been rejected by an internal information channel or for any of the following reasons:
  - When the facts reported lack any credibility.
  - When the facts reported do not constitute a violation of the legal system included in the scope of this policy.
  - When the communication is manifestly unfounded or there are reasonable grounds to believe that it has been obtained through the commission of a crime.
  - When the communication does not contain new and significant information about infringements compared to a previous communication for which the corresponding procedures have been concluded, unless there are new factual or legal circumstances that justify a different follow-up.
- Information related to complaints about interpersonal conflicts or that only affects the informant and the persons referred to in the communication or disclosure.
- Information that is already fully available to the public or that constitutes mere rumour.
- Information relating to actions or omissions not covered by this policy.

## 9 MEASURES FOR PROTECTION MEASURES PERSONS PERSONS AFFECTED

During the processing of the case, persons affected by the communication shall have the right to the presumption of innocence, the right to defence and the right of access to the case file under the terms provided for in Law 2/2023, as well as the same protection established for whistleblowers, preserving their identity and guaranteeing the confidentiality of the facts and data of the proceedings.

## 10 APPROVAL, ENTRY INTO FORCE AND DISSEMINATION

This Policy shall be effective from the moment of its approval by the Management of MYR HOTELS, and shall be published on the corporate websites of MYR HOTELS.

This Policy will be reviewed and updated whenever necessary to make any modifications.

