ACS POLICY ON OPERATION OF THE ETHICAL CHANNEL

Reference	16_Política de Funcionamiento de Canal Ético_2021_EN
Title of the *Standard*	ACS POLICY ON OPERATION OF THE ETHICAL CHANNEL
Geographical scope	Worldwide
Category	Policy
Approval date	27 July 2021
Approval body	Board of Directors
Current version	V1

IMPORTANT INFORMATION ABOUT THIS DOCUMENT

Identification of the document	Policy on Operation of the Ethical Channel
Reference	16_Policy on Operation of the Ethical Channel_1_2021
Geographical scope of application	Worldwide
Section of other standards it implements	Code of Conduct
Standards it replaces	Procedure Regulations of the Code of Conduct Monitoring Committee [*Comité de Seguimiento del Código de Conducta*]
Standards it repeals	Procedure Regulations of the Code of Conduct Monitoring Committee
Primary responsibility for oversight	Compliance Committee
Proposing body or department	Audit Committee
Author	Compliance Committee
Approval body	Board of Directors
Approval date of current text	27 July 2021
Application date	October 2021
Publication and accessibility	Internet and Intranet

Change Control

Version	**Date**	**Approval body**	**Author**	**Summary of changes**
1	27 July 2021	Board of Directors	Compliance Committee	

CONTENTS

1. Introduction

1.1 Justification for the reform

On 25 July 2018, the Board of Directors of ACS, ACTIVIDADES DE CONSTRUCCIÓN Y SERVICIOS, S.A. (the "Board of Directors") passed its first resolutions on the subject of implementing a Comprehensive Compliance Management System. Since then, the Board of Directors has continued to demonstrate its commitment to this process by taking the decisions needed to effectively implement policies on the control and management of financial, non-financial, and corporate risks. It has done this in line with the needs of the ACS Group. Its most recent approvals took place on 14 August 2020, for the compliance policies and protocols on the subjects of Competition and Information Security. Its most recent modifications were on the General Risk Control and Management Policy, Sustainability Policy, and Communication Policy for Reporting of economic-financial, non-financial, and corporate Information, and Contacts and Interaction with Shareholders and other Stakeholders, with the aim to adapt these to the Good Governance Code for Listed Companies of 26 June 2020.

On the subject of regulatory and legislative compliance, there is a need to ensure proper application of the legal rules imposed by public authorities, as well as other rules and standards ACS has implemented voluntarily. For this reason, the models on regulatory compliance, internal control, and risk management have been designed with a scope that allows them to cover both categories of obligations. This has allowed the creation of synergies in relation to the required activities, while also avoiding duplications and overlapping in the governance structures. There are also international recommendations that advise that the Compliance function should extend to cover oversight for a company's own internal rules, including codes of conduct and other policies arising from them. In view of the progress made in this direction, there is no longer a need for the *Code of Conduct Monitoring Committee*, which was established before ACS created its Comprehensive Compliance Management System (the "System"). Eliminating this committee prevents redundancies for the tasks now performed by the Compliance Committee, and it contributes to creation of a clear, simple, and effective model for managing reports of conduct and concerns.

The Compliance Committee, which has replaced the *Code of Conduct Monitoring Committee* and taken on its duties, has members with professional qualifications that allow them to appropriately address the growing complexity of communications on the subject of ethical conduct and compliance with legal and internal regulations. The Compliance Committee reports directly to the Audit Committee, and it is able to effectively receive and pass on communications regarding any conduct that fails to comply with the principles established in the Code of Conduct currently in force.

In the context described, this Policy has now been created to ensure that ACS can respond immediately to any report it receives regarding potential infringements of the System. It is defined as the company's means of implementing its whistleblowing channel (the "**Ethical Channel**"), in a manner adapted to the Spanish and European legislation currently in force. It is also designed to reflect the best practices in the market, and to establish a policy that can comply with the highest Spanish and international standards currently applicable, or which are expected to become applicable in the near future. For reporting channels of this type, it is an essential requirement that they must be operated in a professional and confidential manner.

With regard to the various types of channels that reporting persons will be able to use, we must begin by distinguishing between *ordinary channels* and *alternative channels*. All of these channels can be used to report any situations that could represent a non-compliance with the System, with all whistle-blowers being assured that the information they report will reach the appropriate people designated by ACS for such a purpose, with no need for them to be concerned about retaliation. In summary, the fundamental intention is to give the people included in this Policy's scope of application the ability to report any possible non-compliances or concerns, all within the framework defined in this *Policy on Operation of the Ethical Channel*.

1.2. Regulatory and legislative context

The need to maintain an Internal Reporting Channel or Ethical Channel is included as an essential element in the Compliance Model and Regulatory Risk Prevention Model. This need is also imposed by section 31 *bis* 5.4 of the Spanish Criminal Code [*Código Penal*], which states that *"(...) the models for organisation and management (...)* ***must impose an obligation to report possible risks and non-compliances to the body responsible for supervising operation of the prevention model and compliance with it****".* Moreover, section 31 *bis* 5.5 of the Criminal Code establishes the need for a Disciplinary System on the subject of Compliance: "(…) the models for organisation and management (...) **must establish a disciplinary system that imposes appropriate penalties for failure to comply with the measures established in the model**". This reform therefore addresses the need to comply with both of those requirements from the Spanish legislation.

From the perspective of ACS's internal regulations, this Policy must be considered as an integral part of the ACS Group's Comprehensive Compliance Management System. ACS also wants to make it clear that its Policy on Operation of the Ethical Channel is not intended to replace the authorities possessed within ACS's ordinary management structure. Therefore, the relationships between these must be based on complementarity, coordination, and collaboration to achieve the best results for resolving any issues that could represent a potential breach in the System.

From the perspective of this Policy's contents and structure, the guidelines followed are those imposed by the following regulatory and legislative sources:

Firstly, there is **Circular 1/2016 of the Office of the** Attorney General, **of 22 January, on criminal liability for legal entities under the reform of the** Criminal Code produced by Organic Law 1/2015 *[Circular 1/2016 de la Fiscalía General del Estado, de 22 de enero, sobre la responsabilidad penal de las personas jurídicas conforme a la reforma del Código Penal efectuada por Ley Orgánica 1/2015],* which states that in order to allow a company's employees to report potentially unlawful conduct, the company must have adequate internal regulation that provides specific protection for whistle-blowers.

This Policy also complies with the **ISO 37001** standard on Anti-Bribery Management Systems [*Sistemas de Gestión de Soborno y la Corrupción*], where special reference is made to the process that must be followed when investigating a report, and which also emphasises the need to develop **internal** report management processes **that guarantee**: (i) the effectiveness of the actions performed; (ii) the authority of the persons in charge of the

investigation; (iii) the required involvement and cooperation of other departments; and (iv) confidentiality for all reports, investigations, and resolution procedures.

The **37301 Standard on Compliance Management Systems** [*Norma 37301 para Sistemas de Gestión de Cumplimiento*] also establishes the need to maintain reporting channels. Specifically, in its section related to reporting concerns, it states: "*Even in cases where there are no requirements imposed by local regulations, organisations should consider developing a reporting mechanism that allows anonymity or confidentiality, and which the organisation's employees and agents can use to report or seek guidance on Compliance breaches, without fear of retaliation".* That standard also makes specific reference to the requirements and recommendations on reporting channels found in the **ISO 37002 Standard on Management Systems of Reports on Ongoing Irregularities** [*ISO 37002 para Sistemas de Gestión de Denuncias de Irregularidades actualmente en tramitación*], which is still under development, but its draft version has been used as a basis for developing this Policy.

Other important reference sources on this subject include **the legislation on the subject of data protection** and on the **subject of protection for** whistle-blowers, especially in view of the protection granted under Directive (EU) 1937/2019 of 23 October 2019, on the protection of persons who report breaches of Union law. The purpose of that Directive is to ensure that whistle-blowers are able to report, both internally and to public authorities, any infringement of European Union law they become aware of at an organisation, by using channels that guarantee their security and allow them to perform such reporting without fear of retaliation by the company.

For these reasons, and in compliance with the contents of that Directive, ACS has produced this Policy on Operation of the Ethical Channel. Its purpose is to specifically establish the scope and contents of the reporting process and procedures, and to effectively implement both ordinary and alternative internal reporting channels for ACS. This Policy is also specifically subject to implementation through ACS's *Procedure on Investigation of Reported Concerns and Non-Compliances,* which has been approved by the ACS Compliance Committee. Therefore, in direct relation with said implementing Procedure, this Policy establishes the following specific requirements:

1. **It must be possible for reporting to take place both verbally and in writing**, as well as by telephone and other electronic means, and also in person if the whistle-blowers prefers;
2. **An acknowledgement of receipt for the** report must be produced within a maximum period of 7 days;
3. **The Compliance Committee must be able to appoint an *ad hoc* Investigation Team, to remain active until the case has been resolved, along with** the appointment of a Case Manager who will have the authority to process the report, and to communicate with the whistle-blowers in order to request any additional information and respond to the whistle-blowers' concerns;
4. **All** reports (including anonymous reports) must be addressed in a diligent manner;
5. **A general period of 3 months must be established for giving the** whistle-blowers a response regarding the status of the process, counted from the date the acknowledgement of receipt is produced.

Moreover, section 24 of Organic Law 3/2018 of 5 December, on Protection of Personal Data and Digital Rights [*Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales*] specifically regulates certain aspects of internal

reporting systems created by private enterprises. Some of the most important considerations from that section are summarised below. Firstly, communications and reports can be **anonymous**. Secondly, it establishes **a duty to inform employees and third parties about the existence of these reporting systems ("Ethical Channels"). In addition**, it clearly establishes that **access to information within the system must be restricted to persons with internal control and compliance duties (who may or may not be employed by the company)**, or to designated data processors (however, access by other persons or disclosure of information to third parties or public authorities may be permissible if required in order to apply disciplinary measures or if necessary in relation to judicial proceedings). It is also notable that **the identities and personal data of the persons involved must remain confidential**, especially any information regarding the whistle-blowers in cases where the report has not been performed anonymously.

Finally, in regard to the possibility of an anonymous report, it is necessary to cite **Spanish Supreme Court Judgment 272/2020 of 6 February [*Sentencia del Tribunal Supremo 272/2020 de fecha 6 de febrero*], which considered and upheld the use of anonymous reporting to detect unlawful acts, if those acts can later be corroborated by investigations carried out by the company and by the police, as in the case the Court was addressing. Specifically, the Supreme Court's Criminal Chamber stated that: *"(…) The** performed report is important, where in the absence of an internal regulation compliance programme, it is quite interesting to note that during the period when the proven events occurred, an 'ad intra' mechanism was in place at the company. This type of mechanism has been recently regulated in the form referred to as an "internal reporting channel" or "whistle-blowing channel", as included in the recent Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons who report breaches of Union law".*

2. Purpose of the Policy

The purpose of this Policy, which implements the obligation to make use of the ACS Ethical Channel and describes how it can be used, is to provide advice and certainty in respect to the decisions a person should make after becoming aware of any possible infringements or non-compliances in relation to the System. The intention of ACS is to firmly establish a principle that is consistent with the sources of law summarised in the previous section: **At ACS, any retaliation against a whistle-blowers is prohibited**.[1]

In order to implement this principle, decisions must be made on the following **fundamental aspects**:

1. Subjective scope of application: Who does this Policy apply to?
2. Objective scope of reports: What can I report? When should I make a report?
3. Using the channel: How do I use the ACS Group's Ethical Channel?
4. Consequences of reporting: What happens when I make a report using the Ethical Channel?
5. At ACS, the Policy on Operation of the Ethical Channel is a universal policy. In other words, it is always applicable at ACS, unless there is some legal justification that creates an exception to its applicability.

[1] *In conformity with Recital 37 of Directive (EU) 1937/2019 on the protection of whistle-blowers.*

2.1 Subjective scope of application: Who does this Policy apply to?

This Policy is binding for any person who wants to report a possible non-compliance, infringement, or breach, within a professional context involving the ACS Group. In accordance with the scope of persons to which the System and its Code of Conduct apply, this Procedure is binding for all directors, executives, and employees associated with companies from the Group, regardless of the legal nature of their relationship ("**persons affected**").

It is also binding for all other persons who become aware of a non-compliance or breach during their professional relationship with ACS, even if they are not employed by ACS. It is also binding for all "participants" involved with ACS, in accordance with the definition of that term found in the company's *Policy for Communication of economic-financial, non-financial and corporate information, and regarding Contacts and Relations with Shareholders and other Stakeholders*.

ACS must ensure that the principles established in this Policy are also applied to its non-controlled investee companies and its joint ventures.

2.2 Objective scope of reports: What can I report? When should I make a report?

2.2.1 What can I report by applying this Policy on Operation of the Ethical Channel?

This Policy encourages reporting of any concerns a reporting person has regarding possible non-compliances or infringements in relation to ACS's Comprehensive Compliance Management System, in conformity with the scope of reporting defined in Directive (EU) 1937/2019. This means the reporting of breaches in the broadest possible sense, including but not limited to reasonable suspicions, actual or potential breaches, those that have occurred, and those that seem very likely to occur.[2]

In relation to this, we must emphasise the following potential reasons for reporting:

- To report a situation that could represent a non-compliance on the subject of prevention of money laundering and financing of terrorism;
- To prevent bribery and corruption;
- To improve health and safety in the workplace;
- To prevent conflicts of interest in relation to any type of professional activities;
- To prevent discrimination, as well as sexual and non-sexual harassment.
- To prevent internal fraud;
- To protect fair competition and the rules of international trade;
- To ensure responsible use of the company's assets;
- To safeguard the integrity of the company's taxation procedures, business affairs, and financial records;
- To create a more inclusive and respectful workplace;
- To protect ACS's information, when disclosure could harm the interests of the Group or the rights of third parties protected by law;
- To protect ACS from hacking or cyber attacks;
- To allow compliance with the laws and regulations on urban planning and

[2] *In conformity with Article 5 of Directive (EU) 1937/2019 on the protection whistle-blowers.*

zoning;
- To protect human rights;
- To protect compliance with laws and customary practices globally and locally, with relationships with public-sector authorities being restricted to the professional environment.
- Among other potential reasons.

2.2.2. When should I make a report?

At ACS, we believe that the best way to encourage reporting is to start by generating an environment where people feel comfortable sharing any information that could represent a non-compliance with ACS's Comprehensive Compliance Management System. Therefore, the company promotes development of a workplace where circumstances involving possible infringements of said System can be openly discussed.

This must be done in line with a principle that applies to all relationships between ACS and its stakeholders: Reporting or whistle-blowing must always take place in good faith,[3] which is equivalent to the implementation of what is referred to in Directive (EU) 1937/2019 as a "just culture". This means that when reporting occurs, the whistle-blower must have reasonable grounds for believing that the information being reported is accurate and involves a potential non-compliance, breach, or infringement.

2.2.3 What if it is an urgent matter?

It is clear that in order to process the reports received through the various channels ACS offers, the body responsible for receiving tsaid reports (which is the Compliance Committee) must perform its own internal classification, based on the contents of the reports. This classification will allow reports to be processed in an appropriate manner. The way in which reporting is classified for that purpose is detailed in the *Procedure on Investigation of Reported Concerns and Non-Compliances at ACS*.

What is required in all cases is the assurance that the information reported will reach the appropriate hierarchical level or the Regulatory Compliance Office at ACS as soon as possible. This will allow each issue to be addressed in the most effective manner in view of the facts and events reported, in accordance with the applicable laws and regulations, and in conformity with the *Procedure on Investigation of Reported Concerns and Non-Compliances at ACS*.

2.3 Using the channel: How do I use the ACS Ethical Channel? Can reports be anonymous?

2.3.1 Steps to follow when making a report

Any type of report covered by this Policy can be performed using one of the channels detailed below:

a) **Ordinary** Channels:

[3] *In conformity with Recital 32 of Directive (EU) 1937/2019 on the protection of whistle-blowers.*

1. Reporting to the whistle-blower´s direct supervisor or a member of ACS's management;
2. Reporting to a member of the Compliance Committee;
3. Reporting to the Regulatory Compliance Office.
4. By postal mail sent to:

To the attention of: Canal Ético Grupo ACS
Avda. Pío XII 102, 28036 Madrid, Spain.

b) **Alternative** Channels: The following are considered to be "**Alternative Channels**":

5. The online channel accesible through the corporate web site https://www.grupoacs.com/compliance/canal-etico/

   or directly through the following link:
   https://secure.ethicspoint.eu/domain/media/en/gui/108376/index.html

6. The telephone channel, available 24 hours a day, seven days a week:

Country	Hotline Number
Spain	900 876 841
United States	833 7781 528
Canada	833 7781 528
France	0 800 99 08 46
United Kingdom	0800 077 3019

ACS encourages all its employees to use those reporting channels to notify the company of any possible infringements, within the context described in section 3.2.1.

2.3.2 What information do I need to provide when using the channel?

ACS would like **the information it receives to be as complete and accurate as possible**. Therefore, it asks all whistle-blowers to share all information they are aware of regarding potential infringements in the most detailed manner possible. It is also preferable to provide, or clearly make reference to, any supporting evidence or documents for the report. This will allow ACS to address the case as quickly and effectively as possible.

2.3.3 Identification of the whistle-blower: anonymity

ACS's Ethical Channel **allows anonymous reporting**.[4]

However, ACS encourages all whistle-blowers to identify themselves by providing their name, position, and contact information. This will allow the persons handling the case to contact the whistle-blower to perform any necessary follow-ups. ACS also believes that this is the best way to confirm compliance with its policy of non-retaliation against whistle-blowers.

In relation to this, it must be remembered that when (non-anonymous) reports occur, ACS ensures that the entire internal reporting procedure takes place in a secure manner, with confidentiality guaranteed for whistle-blowers's identity and other related information.

2.3.4 What happens when I make report using the ACS alternative reporting channels?

In line with the requirements from Directive 1937/2019, ACS uses an online platform to support use of the alternative channels it offers.

Any reporting that takes place through those alternative reporting channels is stored directly on the platform, which must have robust information security measures implemented, designed to preserve the integrity, availability, and confidentiality of the information.

The platform must allow the reporting person to specify the place, date, and company or division involved, and to identify the people related to report. The platform also offers an anonymous reporting option. In addition, it has a feature that allows the whistle-blower to attach supporting documentation for the information being reported.

Through its Regulatory Compliance Office,[5] ACS will issue an acknowledgement of receipt within a period of 7 days.[6]

Once the acknowledgement of receipt has been produced, and in cases where the whistle-blower has not opted to remain anonymous, ACS will be able to directly contact the whistle-blower through the internally appointed person known as the Case Manager, who will be able to introduce himself or herself as the investigator and provide any pertinent comments and updates. Processing of the report must be completed within a reasonable time period of no more than three months[7] from issuance of the acknowledgement of receipt. That period can also be extended to six months[8] under circumstances with special relevance or complexity. However, after the first three months have passed from the time when the report was made, any information of a personal nature must be deleted from the reporting channel. This

[4] *In conformity with section 24.1 of Organic Law 3/2018 of 5 December, on Protection of Personal Data and Digital Rights [el artículo 24.1 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de derechos digitales].*

[5] *During any specific periods of absence, such as those caused by vacations, vacant positions, medical leave, or other reasons, a person must be designated as temporarily responsible for receiving the reporting submitted via ACS's platform used for the Ethical Channel.*

[6] *In conformity with Article 9.1(b) of Directive (EU) 1937/2019 on the protection of whistle-blowers.*

[7] *In conformity with Recital 58 of Directive (EU) 1937/2019 on the protection of whistle-blowers.*

[8] *In conformity with article 11.1(d) of Directive (EU) 1937/2019 on the protection of whistle-blowers.*

includes information relating to the whistle-blower, people whose acts or conduct have been reported, and any third parties. The exception to the deletion of said personal information is in cases where it is essential to preserve it as evidence to be used in accordance with the crime prevention model.

It is important to emphasise that the platform transfers the information reported only to the specific persons within the ACS organisation who are authorised to manage said report. The internal team that manages the documents submitted also receives training on how to effectively handle those documents and the associated reporting, as well as on the best manner of ensuring the confidentiality of all information submitted.

The guiding principle is that if the information reported suggests that a potential infringement of ACS's Comprehensive Compliance Management System exists, then an investigation must be initiated in conformity with the *Procedure on Investigation of Reported Concerns and Non-Compliances at ACS*.

ACS must provide the whistle-blower with information about the report submitted, and to the extent possible, about the results of the evaluation performed. It must be borne in mind that in some cases there can be restrictions on how much updating information can be given about a case, in conformity with the contents of the *Procedure on Investigation of Reported Concerns and Non-Compliances at ACS*.

2.3.5 Fair and responsible treatment of reports

The principle of good faith also applies to the company. At ACS the rights of the employees are always respected, and it must, therefore, also be ensured that the rights of any employees mentioned in the report received are protected in accordance with this Policy.

2.3.6 Prohibition of retaliation

ACS does not tolerate any form of retaliation. This includes threats and any other attempt to intimidate a whistle-blower who has acted in good faith when reporting conduct covered by this Policy.

2.3.7 What is the meaning of good faith, for the company and for the whistle-blower?

From the whistle-blower's perspective, good faith means only reporting concerns when there are reasonable grounds to support the belief that the information being reported about a potential breach or infringement is accurate at the time of the report.

From the company's perspective, good faith in the context of reporting channels means that the company will not allow any retaliation based on the fact that a report has occurred, and it will protect the confidentiality and identity of the whistle-blower in all circumstances, with only the following exceptions:

a) When some type of law or regulation requires disclosure to a judicial or governmental authority.
b) When disclosure to ACS's external advisers, consultants, or other service providers is essential in order to allow operation of the Ethical Channel, or to allow investigation of the situations reported, all in conformity with section 3.6 of this Policy. In these

cases, ACS applies contractual terms and conditions that require maximum confidentiality from the providers.

2.3.8 What does prohibition of retaliation mean?

The prohibition of retaliation covers any direct or indirect act or omission that could cause harm to a whistle-blower, when taking place in response to their report, made in good faith, of possible infringements.

For example, ACS will not take any of the following actions against whistle-blowers:

1. Suspension, dismissal, removal, or equivalent measures;
2. A negative performance evaluation;
3. Denial of a promotion;
4. An unjustified change of workplace, salary reduction, or change in working hours;
5. Coercion, intimidation, harassment, or ostracism;
6. Discrimination or disadvantageous or unfair treatment;
7. Non-renewal or early termination of a temporary employment contract;
8. Any type of harm, including harm to the person's reputation (in particular on social media sites) and financial loss (including loss of business and loss of income);
9. Early termination of a contract for supplying goods or services;
10. Cancellation of a licence or permit;
11. Any other measures that could be considered to be retaliatory.

2.3.9 Prohibition of retaliation in cases of external reporting and public disclosures

This protection against retaliation also covers persons who report potential infringements externally to the competent authorities.

- Both direct and indirect forms of retaliation are prohibited

The scope of the Policy on Operation of the Ethical Channel prohibits retaliation against the following persons:

1. Any third party related to the whistle-blower (such as co-workers and family members) who could be subject to retaliation in a workplace context;
2. Any person who assisted the whistle-blower during the reporting process;
3. Any legal entity that the whistle-blower owns, works for, or is in some other way connected to by an employment or professional relationship.

If any person from ACS infringes this Policy by performing some direct or indirect act of retaliation, ACS must take responsibility for implementing the measures necessary to ensure that the retaliation is ended as soon as possible, and when appropriate, it must apply disciplinary measures against those responsible.

3. Data protection and storage

3.1 Identity of the data controller

The personal data of the whistle-blower will be processed by the entity from the ACS Group that receives the report.

The ACS group is committed to strict protection of privacy and security and proper storage of that data, as detailed in our policies and procedures on the subject of Compliance. These same standards must also be applied with respect to all other personal data associated with the report taking place in accordance with this Policy.

3.2 Storage of personal data

ACS maintains a register to record all the report its receives. These records, and the personal data they contain, are maintained in a strictly confidential manner. In all cases, these records are stored for the entire time period required in order to comply with the legal requirements applicable at any given time, but never for a time period longer than necessary.

Specifically, ACS will store the whistle-blowers's personal data for the time period essential for deciding whether it is appropriate to initiate an investigation about the conduct or concerns being reported. Once that decision has been made, the data will be deleted from the Ethical Channel. However, that data can still be processed outside of that system to allow investigation of the pertinent facts and events, for the time period required in order to reach a decision. Once the investigation has been completed for the report received, and any appropriate actions have been taken, the data taken from any report that has been investigated will be stored in order to comply with the legal obligations applicable to each case, but with access to that information appropriately blocked.

In all cases, personal data will be deleted from the Ethical Channel within a maximum time period of three (3) months after being entered, unless storage for an additional time period is necessary in order to comply with any legal obligations or with the company's need to maintain evidence regarding the operation of the crime prevention model. If investigation of the report has not been completed within said time period, the data can be processed outside of the Ethical Channel for the period of time required to allow that investigation to be finalised.

In cases where a decision is made not to further investigate the report received, the information can be stored after being made anonymous.

3.3 What personal data does ACS collect?

When processing the report made in accordance with this Policy, ACS collects the following types of personal data and information, both at the time when report occurs and during the subsequent investigation:

- The whistle-blowers's name and contact information (unless the report is anonymous), and whether that person is an ACS employee;
- The names and other personal data of the persons mentioned in the report (persons committing alleged infringements, possible witnesses, and other persons), if information about them is provided (in other words, a description of

their positions and contact information, and the nature of their role or participation in the events being reported);
- A description of the alleged infringement, as well as the circumstances surrounding the incident(s).

3.4 Why does ACS process personal data?

At all times, the only personal data processed is the data strictly necessary for purposes of managing, processing, and investigating the reporting received in relation to commission of irregularities or acts that are unethical, unlawful, or contrary to the ACS Group's corporate rules; for performing any acts necessary to investigate the facts and events reported; and for applying any appropriate disciplinary or legal measures.

No personal data will be used for any purpose other than those described.

3.5 What is the legal basis of the processing?

The legal basis of processing personal data in the context of the Ethical Channel is the existence of a public interest; processing taking place under the terms established in article 6.1(e) of the European Union's General Data Protection Regulation (GDPR); processing for purposes of detecting and preventing claims and therefore any resulting harm and liability risks for ACS; and processing as defined in section 24 of Organic Law 3/2018 of 5 December, on Protection of Personal Data and Digital Rights, by creating and maintaining an internal system for reporting and investigating suspected irregularities or acts that are unethical, unlawful, or contrary to the company's corporate rules.

Processing personal data can also be based on compliance with a legal obligation or on satisfaction of the company's legitimate interest.

Therefore, processing the whistle-blowers's personal data is strictly necessary in order to manage the report and comply with the purposes and legal obligations described above. In no case will the ACS Group perform automated decision-making based on the data submitted.

3.6 Who are the recipients of the personal data?

Personal data collected in the context of report taking place through the alternative reporting channels can be processed by, or disclosed to, the following parties when necessary:

- The service provision entity for the platform, which is responsible for day-to-day management of the alternative reporting channels;
- Members of the ACS Compliance Committee;
- Authorised representatives of ACS, if the nature or scope of the reported events or concerns makes their participation necessary;
- External investigators, advisers, or consultants contracted to assist ACS in evaluating the report, investigating the matter, or advising ACS in relation to the matter;
- The police or any other regulatory or law enforcement authorities.

3.7 What data protection rights do whistle-blowers have?

The whistle-blower can exercise their right to access their own personal data at any time, under the terms established in the applicable legislation. If the whistle-blower believes that their data is inaccurate or incomplete, they can submit a request for rectification in accordance with the applicable legislation. They can also request erasure of their data if it is no longer necessary, except in cases where there is a legal obligation to store it. They can also request restriction of processing of their personal data or object to such a process, and they can request data portability. They also have the right to withdraw their consent to processing. At the time when they submit their report, they will be informed about how they can exercise all of those rights.

If they believe it is appropriate, they can also submit a claim to the competent data protection authority.

3.8. How can I obtain more information about personal data processing?

Upon request, any person can obtain more information about processing of their personal data, or can receive the contact information for the company's representative existing for this purpose, such as the Data Protection Officer or another person responsible for matters related to privacy. At the time when they submit their report, they will be informed about how they can obtain that information.

4. Related procedures

The Policy described in this document is directly related to the other policies or procedures listed below, which ACS considers to be the most important in terms of understanding the scope, purpose, and intentions of this Policy.

Specifically, these are the procedures connected to or affected by this Policy, and they are posted in the "Compliance Policies and Procedures" section of the company's website:[9]

- Code of Conduct
- Code of Conduct for Business Partners
- General Risk Control and Management Policy
- Criminal and Anti-Bribery Compliance Policy
- Human Rights Policy
- Corporate Due Diligence Protocol Regarding Human Rights
- Diversity Policy
- Sustainability Policy

[9] *As of the production date of this Policy, the following link can be used: https://www.grupoacs.com/compliance/compliance-policies-and-procedures/*

- Policy for Communication of economic-financial, non-financial and corporate information, and regarding Contacts and Relations with Shareholders and Other Stakeholders
- Environmental Policy
- Information Security Policy
- Remuneration Policy
- Competition Compliance Policy and Protocol
- General Compliance Policy

This Policy on Operation of the ACS Ethical Channel **repeals**:

1. Procedure Regulations of the Code of Conduct Monitoring Committee