



**INTERNAL
INFORMATION SYSTEM
POLICY**

CONTENTS

1. INTRODUCTION AND OBJECTIVE	3
2. SCOPE.....	3
3. CONTENT OF COMMUNICATIONS	3
4. COMMUNICATORS OR INFORMANTS	4
5. GENERAL PRINCIPLES AND GUARANTEES	5
6. COMPLIANCE COMMITMENTS.....	9
7. SANCTIONS REGIME	9
8. RESPONSIBILITY AND SUPERVISION	9
9. APPROVAL	10
10. DOCUMENTS RELATED TO THIS POLICY	10
11. VERSION HISTORY	10

1. INTRODUCTION AND OBJECTIVE

This Policy aims to promote and strengthen the culture of communication within E. Bachiller B., S.A. (hereinafter, "BACHILLER"), as a means to prevent and detect threats to the public interest, guaranteeing and prioritising the protection of communicators or informants, under Law 2/2023, of 20 February, regulation of the protection of persons reporting on regulatory and anti-corruption offences, which transposes in Spain Directive (EU) 2019/1937 of the European Parliament and of the Council, of 23 October 2019, on the protection of persons reporting infringements of Union Law.

BACHILLER expects both its members of staff and its business partners to act at all times in accordance with the principle of good faith in the performance of their tasks, which requires, among other aspects, maintaining a constant collaborative attitude toward the organisation.

As a tool to comply with the above, BACHILLER has an Ethics, Communication and Complaints Channel at the following address: <https://www.corporate-ethicline.com/BACHILLER/> as a preferred channel available to all directors, employees, collaborators, suppliers and clients of the company, as well as any other third party.

2. SCOPE

This Internal Information System Policy includes and is binding on all members of staff at Bachiller.

This Policy is translated into those languages that are necessary for all BACHILLER members of staff, as well as business partners linked to the organisation, in order to understand its scope and content.

3. CONTENT OF COMMUNICATIONS

Through this internal information system, managers, employees, collaborators, suppliers, customers and other third parties may report, confidentially and anonymously, if they so wish, any concern regarding a possible breach or violation of the provisions of the Corporate Code of Conduct or any other Internal Policy of the organisation, or report an irregularity that they detect during the performance of their duties, as well as any infringement or omission of which they become aware and which may involve an infringement of European Union law or its financial interests, including criminal or administrative offences within the Spanish legal framework.

In this regard, the communication channel can be used to report actions or omissions that constitute or may constitute infringements in the following areas:

- Health alerts
- Harassment / Discrimination
- Public procurement
- Confidentiality
- Corruption / Fraud
- Competition
- Corporate crime
- Tax / Corporate law

- Finance
- Non-compliance with current legislation
- Non-compliance with policies / procedures / internal regulations
- Non-compliance with Code of Ethics, or other internal codes
- Employment / Workers' Rights
- Environment
- Radiation protection and nuclear safety
- Intellectual property / commercial secrets
- Protocols and rules of the organisation
- Prevention of occupational risks
- Consumer protection
- Protection of privacy and personal data
- Risks or suspicions of money laundering or financing of terrorism.
- Sustainability
- Public health
- Food and feed safety, animal health and animal welfare
- Network and information system security
- Product safety and compliance
- Transport safety
- Others

This reporting channel will only be used for the purpose described and is not to be used as a vehicle for organisational complaints.

The internal information channels authorised to receive any other communications or information outside of the aforementioned provisions, will not be covered by the scope of protection provided by this Policy and Law 2/2023, of 20 February, regulating the protection of persons reporting on regulatory and anti-corruption infringements.

4. COMMUNICATORS OR INFORMANTS

The principles, guarantees and rights outlined in this Policy are focused on the protection of communicators or informants, prohibiting reprisals of any nature and promoting help and assistance for them.

In this context, communicators or informants are those individuals who report on the infringements mentioned in the preceding section, who work in the private or public sector and who have obtained information on infringements within a work or professional context, including in any case:

- Employed workers, including those who have already terminated their employment or professional relationship.
- Self-employed.
- Volunteers.
- Trainees.
- Those in the selection process.
- Partners, shareholders.
- Managers.
- Anyone working under the supervision of contractors, sub-contractors or suppliers.

Likewise, the following will also enjoy the protection established through this Policy, in accordance with Law 2/2023 above:

- the legal representatives of working persons in the exercise of their advisory and support functions related to the informant,
- individuals who, within the framework of the organisation in which the informant provides services, assist the informant in the process;
- individuals who are related to the informant and who may suffer reprisals, such as colleagues or relatives of the informant, and
- legal persons, for whom they work or with whom they maintain any other type of relationship in a work context or in which they have a significant stakeholding. For these purposes, it is understood that a stakeholding in the capital or voting rights corresponding to shares or holdings is significant when, as a result of its proportion, it allows the holder to have the capacity to influence the legal person involved.

5. GENERAL PRINCIPLES AND GUARANTEES

5.1. INTEGRATION OF INTERNAL CHANNELS

The reporting channel within the internal information system of BACHILLER will be available and accessible to all workers or any third party, regardless of their relationship with BACHILLER, as an integral and preferential channel¹ for communication of information.

5.2. CONFIDENTIALITY AND ANONYMITY

BACHILLER guarantees both the confidentiality and anonymity, if desired, of the informant and any other third party that is or may be mentioned and/or involved in the communication, in the actions carried out as a result of it and in its processing, and the submission of data allowing their identification is not necessary. In this sense, data protection is guaranteed, preventing access by unauthorised personnel.

In this way, the proceedings carried out regarding third parties or other bodies, areas or departments of BACHILLER must be carried out while maintaining the anonymity of the INFORMANT and the INVESTIGATED PERSON, as well as the reasons for the communication.

BACHILLER guarantees that the identity of the informant can only be passed on to the Judicial Authority, the Public Prosecutor's Office or the relevant administrative authority within the context of a criminal, disciplinary or sanctioning investigation.

All those who, for various reasons, take part in tasks to support the investigation of a particular incident, must sign a Confidentiality Agreement for this purpose.

¹ The guarantees set out in this paragraph shall be respected and applicable even if the communication is sent through reporting channels other than those established for those purposes, or to members of staff not responsible for its processing.

In cases where communication reception is managed by an external provider, it shall always be verified that it provides adequate guarantees of respect for their independence, and the confidentiality, data protection and secrecy regarding communications.

In those cases where the communication is sent through internal channels other than those established by BACHILLER or is addressed to staff members not responsible for its treatment, the organisation guarantees the preservation of the confidentiality described above. To do this, BACHILLER has implemented the Annual Compliance Training Plan, through which it will warn (in accordance with the requirement of art. 9.2.(g) of Law 2/2023) that any breach implies a very serious violation of the Law and, likewise, that the receiver of the communication must immediately forward it to the person responsible for the system.

5.3. PRESUMPTION OF INNOCENCE AND HONOUR

At all times BACHILLER guarantees the presumption of innocence and respect for the honour of all people who are affected by a communication.

Persons affected by a communication shall have the right to be informed of the actions or omissions attributed to them, as well as to be heard during the course of the investigation, without in any case being told the identity of the informant.

BACHILLER guarantees people affected by communications: the right to the presumption of innocence, the right of defence and the right of access to the file in the terms outlined under Law 2/2023, as well as the same protection established for informants, preserving their identity and guaranteeing the confidentiality of the facts and data involved in the procedure.

5.4. ACCESS TO EXTERNAL CHANNELS AND PUBLIC DISCLOSURE

Communicators or informants may communicate to the external channel of the Anti-Fraud Office of Catalonia or to the authorities or bodies corresponding to other Autonomous Communities, either directly or by prior communication through the corresponding channel of BACHILLER at the following address: <https://www.corporate-ethicline.com/BACHILLER/>.

Likewise, the possibility of public disclosure is made available to communicators or informants.

Public disclosure consists of making available to the public information regarding the facts that are the subject of communication through this information system.

In this context, in order to extend the protection of Law 2/2023 to persons making public disclosures, the following conditions must be met:

- a) The report has first been made through internal and external channels, or directly through external channels, without appropriate measures having been taken in this regard within the established time frame.
- b) There are reasonable grounds to believe that either the infringement may constitute an imminent or manifest danger to the public interest, in particular in the case of an emergency situation, or there is a risk of irreversible harm, including a danger to the physical integrity of a person; or in the event of communication through an external information channel, that there is a risk of reprisals or to the likelihood of effective treatment of the information due to the particular circumstances of the case being low, such as the concealment or destruction of evidence, the collusion of an authority with the perpetrator of the infringement, or that the latter is involved in the infringement.

5.5. PROHIBITION OF REPRISALS

BACHILLER expressly prohibits actions constituting reprisals, including threats of reprisals and attempted reprisals against persons submitting a communication.

Reprisal means any act or omission which is prohibited by law, or which, directly or indirectly, entails unfavourable treatment which places the persons who suffer them at a particular disadvantage compared to any other within the employment or professional context; as a specific consequence of their status as informants, or because they have made a public disclosure.

For the purposes of the provisions of Law 2/2023, and by way of example, article 36 of that regulation states that reprisals are considered to be those adopted in the form of:

- a) *Suspension of the employment contract, dismissal or termination of the employment or statutory relationship, including the non-renewal or early termination of a temporary employment contract after the probationary period, or early termination or cancellation of contracts for goods or services, imposition of any disciplinary measure, degradation or refusal of promotion and any other substantial modification of working conditions and non-conversion of a temporary employment contract into an open-ended contract, if the worker had legitimate expectations that they would be offered an indefinite post; unless these measures were carried out within the regular exercise of the power of management under the employment legislation or regulating the statute of the corresponding public employee, due to circumstances, facts or proven infringements, and beyond the presentation of the communication.*
- b) *Damage, including reputational damage, or economic loss, coercion, intimidation, harassment or ostracism.*
- c) *Negative evaluation or references regarding work or professional performance.*
- d) *Blacklisting or dissemination of information in a particular sector, which hinder or prevent access to employment or procurement of work or services.*
- e) *Refusal or cancellation of a license or permit.*
- f) *Denial of training.*

g) Discrimination, or unfavourable or unfair treatment.

A person whose rights have been infringed as a result of their communication or disclosure after the expiry of the two-year period may request the protection of the relevant authority, which may, in exceptional circumstances and with due justification, extend the period of protection; after hearing the persons or bodies that could be affected. Reasons shall be given for any refusal to extend the period of protection.

5.6. SUPPORT MEASURES

In accordance with the rules established by Law 2/2023, BACHILLER shall make available to the communicator or informant the appropriate means of support that, after evaluating the circumstances, are deemed duly necessary.

This shall occur regardless of the assistance that may correspond to protection under Law 1/1996, of 10 January, on free legal assistance, for representation and defence in judicial proceedings derived from the presentation of the communication or public disclosure.

5.7. PROTECTIVE MEASURES AGAINST REPRISALS: EXEMPTION FROM LIABILITY

Persons who disclose information under this Policy shall not be deemed to have violated any restriction on disclosure, nor shall they incur any liability in connection with such disclosure, provided they have reasonable grounds to believe that this communication or, in the event, public disclosure, was necessary in order to reveal an action or omission under this Policy.

Informants shall not be liable for the acquisition or access to information that is communicated or disclosed publicly, provided that such acquisition or access does not constitute a criminal offence.

5.8. PROTECTION OF PERSONAL DATA

BACHILLER undertakes to treat the data contained in the communication in strictest compliance with legislation on the protection of personal data and informants, guaranteeing at all times the absence of reprisals.

The processing of personal data arising from the application of Law 2/2023 on which this Policy is based, shall be governed by the provisions of Section VI of that Law, by the provisions of Regulation (EU) 2016/679 of the European Parliament and of the Council, of 27 April 2016, in Organic Law 3/2018, of 5 December, on Protection of

Personal Data and guarantee of digital rights, in Organic Law 7/2021, of 26 May, on the protection of personal data processed for the purposes of prevention, detection, investigation and prosecution of criminal offences and the implementation of criminal sanctions.

Personal data the relevance of which is not evident for processing specific information will not be collected or, if collected accidentally, will be deleted without undue delay.

6. COMPLIANCE COMMITMENTS

All persons who interact with BACHILLER must be familiar with the principles of ethics and responsibilities, as well as all the provisions and obligations contained in the various control measures (Internal Information System Policy, Criminal Code Compliance Policy, Code of Corporate Conduct, Protocol of Harassment, etc.) adopted by the organisation, being obliged to comply with them, as well as to preserve the organisation's integrity and reputation.

This Policy, together with the Corporate Code of Conduct and the rest of the Protocols, policies and internal standards implemented by BACHILLER, constitute the essential foundations of the culture of compliance for the organisation. For this reason, this Policy is mandatory for all persons who are linked to BACHILLER, as well as for business partners, and thus not only requires compliance with current legislation, but also compliance with the ethical and responsible values and principles of the organisation.

To facilitate knowledge of this Policy, as well as compliance, it is made available to all members of staff of BACHILLER through the Intranet, and is available to interested third parties through the external communication channels of the organisation.

7. SANCTIONS REGIME

Any action that may imply a limitation on the rights and guarantees of informants, or their confidentiality and anonymity, violation of the duty of secrecy of the information received and the data contained therein, may constitute a serious or very serious breach of the provisions of Law 2/2023, of 20 February, regulating the protection of persons who report on regulatory violations and the fight against corruption.

8. RESPONSIBILITY AND SUPERVISION

The BACHILLER COMPLIANCE OFFICER is responsible for this internal information system, is in charge of ensuring its proper functioning and will be responsible for the diligent processing of the information received. They are also responsible for the management of the system and the processing of investigation files.

The COMPLIANCE OFFICER enjoys independence and autonomy in the performance of their functions and they were duly appointed by the Sole Administrator of BACHILLER, with notification of the appointment being sent to the Anti-Fraud Office of Catalonia, in the form and terms established under Law.

This Policy will be reviewed and/or modified by the COMPLIANCE OFFICER, who may outsource the service to specialist professionals:

1. Whenever relevant changes in the organisation, control structure or activities of the institution make this advisable.
2. Whenever there are legal modifications involved that make this advisable.
3. Whenever relevant breaches of its provisions are revealed, which also make this advisable.

This Policy will be reviewed periodically, even if none of the circumstances described above occur.

9. APPROVAL

This Internal Information System Policy has been approved by the Sole Administrator and may be modified in order to improve the confidentiality and effectiveness of the management of communications sent.

10. DOCUMENTS RELATED TO THIS POLICY

- . BACHILLER Communications Management Procedure.
- . Roles, Responsibilities and Statute of Operation of the Compliance Officer of BACHILLER.
- . BACHILLER Corporate Code of Conduct.
- . Anti-Corruption, Anti-Fraud and Sanctions Policy
- . BACHILLER Anti-Corruption.

11. VERSION HISTORY

Version	Date	Approved by	Reason for the change
V. Original	01.10.2021.	Sole Administrator	
V.1.	20.04.2023.	Sole Administrator	Adaptation to Law 2/2023