



---

**BACHILLER COMMUNICATIONS  
MANAGEMENT PROCEDURE**

---

## CONTENTS

<b>1.</b>	<b>INTRODUCTION.....</b>	<b>3</b>
<b>2.</b>	<b>STAGES OF THE COMMUNICATION MANAGEMENT PROCEDURE .....</b>	<b>4</b>
<b>2.1.</b>	<b>RECEIVING OF COMMUNICATIONS .....</b>	<b>4</b>
<b>2.2.</b>	<b>ADMISSION PROCEDURE.....</b>	<b>5</b>
<b>2.3.</b>	<b>INVESTIGATION PROCEDURE .....</b>	<b>6</b>
<b>2.4.</b>	<b>COMPLETION OF PROCEEDINGS.....</b>	<b>8</b>
<b>3.</b>	<b>REGISTRATION OF COMMUNICATIONS.....</b>	<b>10</b>
<b>4.</b>	<b>PROTECTION OF PERSONAL DATA .....</b>	<b>10</b>
<b>5.</b>	<b>ADOPTION .....</b>	<b>12</b>
<b>6.</b>	<b>VERSION HISTORY .....</b>	<b>12</b>
<b>7.</b>	<b>ANNEX 1EXTERNAL CHANNELS OF INFORMATION .....</b>	<b>13</b>
<b>7.1.</b>	<b>EXTERNAL INFORMATION CHANNEL OF THE INDEPENDENT INFORMANT PROTECTION AUTHORITY, I.I.P.A.....</b>	<b>13</b>
<b>7.2.</b>	<b>INFOFRAUD.....</b>	<b>14</b>

## 1. INTRODUCTION

BACHILLER has established the following reporting channel: <https://www.corporate-ethicline.com/BACHILLER/>, as a preferred channel available to all directors, employees, collaborators, suppliers and customers, as well as any other third party, to communicate any concerns about a possible breach or violation of the provisions of the Corporate Code of Conduct or any other Internal Policy of the organisation, or to 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 the law of the European Union or its financial interests or criminal or administrative infringement within the Spanish legal framework, as explained in the BACHILLER Internal Information System Policy.

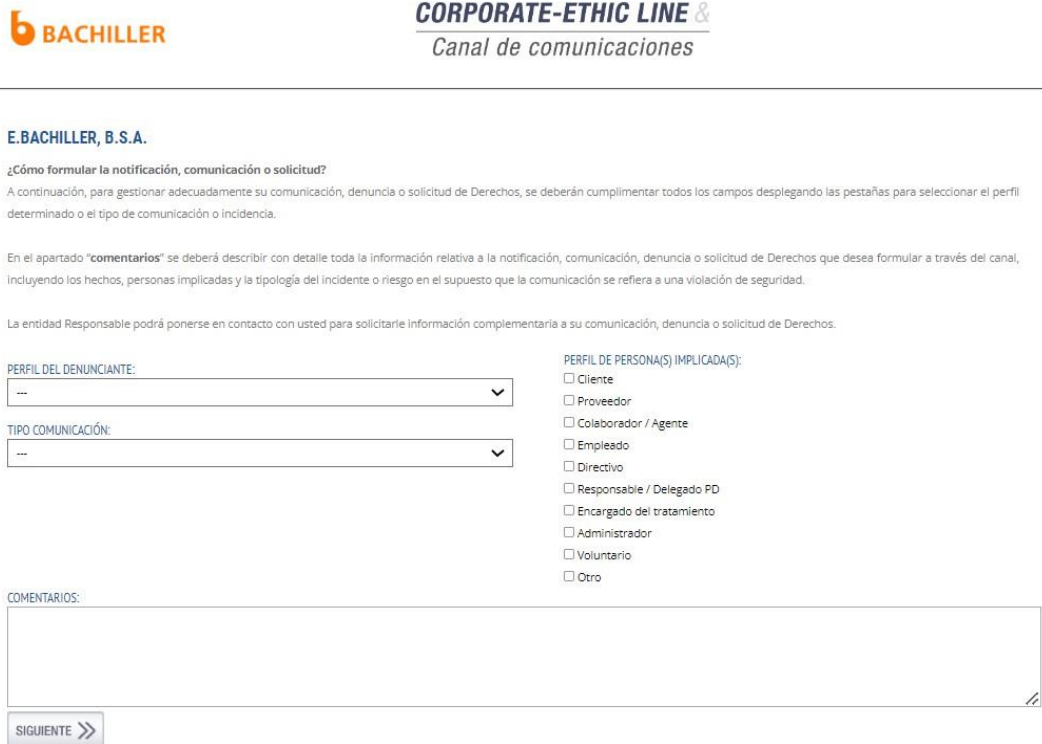
Through this document the Communications Management Procedure is expanded, which establishes the necessary provisions for the internal information system and the internal communication channel in compliance with requirements established in Law 2/2023, of 20 February, regulating the protection of informants reporting on regulatory and anti-corruption offences.

Although the internal communication channel is the preferred channel, alternatively any individual may inform the Independent Informant Protection Authority (hereinafter, "I.I.P.A.") or the corresponding authorities or autonomous bodies, regarding the commission or omission of any action, either directly or by prior communication through the aforementioned internal channel, and in accordance with the terms established in the aforementioned Law 2/2023.

## 2. STAGES OF THE COMMUNICATIONS MANAGEMENT PROCEDURE

### 2.1. Receiving communications

At BACHILLER, the platform automatically notifies the Compliance Officer of the receiving of any communication made through the internal information system, as they have exclusive access to the internal channel of the organisation:



The screenshot shows the 'CORPORATE-ETHIC LINE & Canal de comunicaciones' form. It includes the BACHILLER logo and the following fields:

- E.BACHILLER, B.S.A.**
- ¿Cómo formular la notificación, comunicación o solicitud?**  
A continuación, para gestionar adecuadamente su comunicación, denuncia o solicitud de Derechos, se deberán cumplimentar todos los campos desplegando las pestañas para seleccionar el perfil determinado o el tipo de comunicación o incidencia.
- En el apartado "comentarios" se deberá describir con detalle toda la información relativa a la notificación, comunicación, denuncia o solicitud de Derechos que desea formular a través del canal, incluyendo los hechos, personas implicadas y la tipología del incidente o riesgo en el supuesto que la comunicación se refiera a una violación de seguridad.
- La entidad Responsable podrá ponerse en contacto con usted para solicitarle información complementaria a su comunicación, denuncia o solicitud de Derechos.
- PERFIL DEL DENUNCIANTE:** (dropdown menu)
- TIPO COMUNICACIÓN:** (dropdown menu)
- PERFIL DE PERSONA(S) IMPLICADA(S):**
  - Cliente
  - Proveedor
  - Colaborador / Agente
  - Empleado
  - Directivo
  - Responsable / Delegado PD
  - Encargado del tratamiento
  - Administrador
  - Voluntario
  - Otro
- COMENTARIOS:** (text area)
- SIGUIENTE >>** (button)

Such communication is made in writing and may be anonymous or in the name of the informant, being in any case confidential, including the description of the facts, the identification of the persons involved and, if possible, providing evidence that proves the aforementioned non-compliance, explaining the circumstances in which they have had access to such information.

If a communication is, as an exception, received by word of mouth, it is documented in writing with the informant's consent, either by recording the conversation or through a complete and accurate transcript of the conversation.

Likewise, if in exceptional circumstances the communication is received through internal channels other than those established by BACHILLER or is addressed to staff members not responsible for its treatment, the organisation also guarantees the preservation of confidentiality, warning that failure to comply with the requirement of confidentiality would involve a very serious violation of the Law and that the communication be sent immediately to the person responsible for the system.

Once a communication or information has been received, the Compliance Officer is notified, and as the person responsible for the system, they will initiate the corresponding investigation process, if any, for the clarification of the facts set out in the communication.

The Compliance Officer, as the person responsible for the internal information system, guarantees respect for the independence, confidentiality, data protection and secrecy of communications at all times.

Within seven (7) calendar days of receiving the communication, an acknowledgement of receipt must be sent to the informant. This acknowledgement of receipt is incorporated within the file, including, in all cases, clear and accessible information on the external channels of communication to the relevant authorities.

In cases in which making an acknowledgement of receipt could jeopardise the confidentiality of the communication, to guarantee it, it will not be made until a period that is considered prudential has elapsed.

As mentioned in previous paragraphs, alternatively to this preferred internal channel, reports may be sent to the I.I.P.A. or to the corresponding authorities or autonomous bodies, regarding the commission or omission of any action that may constitute any of the infringements liable to be reported through the internal information system<sup>1</sup>, either directly or after communication through the internal channel, in accordance with the provisions of Annex 1 on external channels of communication.

## 2.2. ADMISSION PROCEDURE

After receiving the communication, a REGISTRATION NUMBER will be assigned to the FILE, and a series of CODES, to render anonymous both the informant and the investigated person, the facts, and any other third party who may be affected by the communication.

If the Compliance Officer warns that the facts reported may be inadvertently constituting an infringement, they will forward the information to the administrative body immediately, which must decide whether to refer it immediately to the Public Prosecutor's Office.

The Compliance Officer is not involved in such communication. If this is the case, the Administrator will be informed and that person will be removed from the proceedings. If it is necessary to replace the person concerned, the Sole Administrator will appoint a substitute for the purpose of continuing the investigation in the manner most appropriate to the interests of the parties involved. Such replacements and reappointments will be recorded in writing in the Minutes and at the moment the file is opened.

---

<sup>1</sup> In this regard, see the provisions of paragraph 3, "Content of communications", in the Internal Information System Policy.

Finally, after receiving the communication, the Compliance Officer will record the following information:

- The objective data contained in the communication: the facts, dates, names, quantities, places, contacts, etc., that the person who made the communication has provided.
- Subjective data: opinions, rumours, ideas and insights the informant considered necessary in the narration of the communication.
- The Compliance Officer's assessment of whether the communication is associated with a possible or alleged infringement or if it is a mere report or suggestion related to improving an area of the business, the employment situation, etc.

### 2.3. INVESTIGATION PROCEDURE

If the communication is admitted for processing, the investigation will be led and carried out by the Compliance Officer.

Where possible, the informant may be asked to provide additional information necessary for the course of the investigation to which the communication has given rise.

At this stage, the INVESTIGATED PERSON is notified and INTERVIEWED, being notified of their right to be informed of the actions or omissions attributed to them and of their right to be heard, without being told the identity of the informant.

Any third parties involved are also cited and interviewed for the purpose of explaining and clarifying the allegations being considered. All investigative steps necessary will be carried out for the parties and a documentary record will be created regarding all the actions in the file.

The proceedings that are carried out in relation to third parties or other bodies, areas or departments of BACHILLER must be done while maintaining the anonymity of the INFORMANT, the INVESTIGATED PERSON and the reasons for the communication.

The confidentiality of information is guaranteed at all times, as well as the presumption of innocence and respect for the honour of all persons affected.

During this stage the Compliance Officer:

1 - Investigates the facts communicated and, specifically:

- The objective and subjective elements provided by the informant, prioritising the objective elements supported by documentation that backs up, in whole or in part, the facts reported.
- The reputation, seriousness and reliability of the informant.
- The allegations and evidence of the allegation(s) against the investigated person.
- The evidence is evaluated with third parties, and any related bodies, areas or departments.

2 - Analyses and assesses the possible consequences that the facts communicated may produce:

First, the Compliance Officer checks whether these events were caused by a significant lack of internal control in BACHILLER. Where appropriate, they will propose urgent remedial and preventive measures to avoid further risk.

Secondly, if the gravity, specific nature or complexity of the facts so warrants, the Compliance Officer may appoint another management professional or a third specialised person to assist with the investigation. Likewise, if losses of assets could occur as a result of the facts reported, the Compliance Officer takes measures to prevent or mitigate such losses. If evidence relevant to communication may be leaked or destroyed, prior to the start of the investigation, the Compliance Officer is responsible for ensuring evidence is secured. The Compliance Officer also evaluates the relevance of notifying governing bodies regarding the communication. Finally, they check whether there is a possibility that damage has been inflicted on third parties, in which case they assess the damage and the need to notify the injured third party.

The time frame for conducting the investigation and giving a response to the informant about the actions that have been carried out, as well as their outcome, depends on the seriousness of the facts reported and their potential consequences, with the duration of this stage remaining at the criterion and risk of the Compliance Officer. However, in accordance with the provisions of Article 9.2.(d) of Law 2/2023, of 20 February, regulating the protection of persons reporting on regulatory violations and anti-corruption, this period may not exceed three (3) months from having received the communication, or if no acknowledgement of receipt was sent to the informant, three (3) months from the expiry of the period of seven (7) days following the time the communication was made. This time frame shall be respected, except in cases of particular complexity, when it may be extended to a maximum of three (3) additional months<sup>2</sup>.



---

<sup>2</sup> These time frames shall be respected, in any case, without prejudice to the provisions of employment regulations or collective agreement applicable to each case, whose periods shall prevail in the event of contradiction

If the communication contains personal data regarding third parties other than the person investigated (e.g. witnesses, suppliers, customers, etc.), the Compliance Officer shall state in writing that any personal information provided that is not necessary for the investigation must be deleted and that third parties whose data will be processed must be notified. The information will comply with information requirements under data protection regulations, omitting from the information the identity of the informant, which must remain confidential.

All these notifications are decided on by the Compliance Officer in their role as head of the system, and are written in the file and executed through the Ethics, Communication and Complaints Channel at the following address: <https://www.corporate-ethicline.com/BACHILLER/>.

#### 2.4. TERMINATION OF THE PROCEEDINGS

After the investigation of the communication and with supporting documentation to clarify the facts, a VERDICT or RESOLUTION is prepared and approved by Extraordinary Act issued by the Compliance Officer, with the following content:

- Description of the facts: registration no. of the communication, date of communication, the facts reported, parties involved, documentation provided throughout the investigation by both parties (informant and investigated person), by other bodies, areas or departments or by third parties, the interviews with the investigated person and/or with third parties, etc.
- Analysis and evaluation of the evidence obtained.
- In the event that the reported irregularity is verified, the Compliance Officer will dedicate a section of the verdict to making the recommendations considered necessary to implement or to improve the internal controls and protocols that have been deficient on this occasion.
- Resolution: With the approval of the governing bodies, the resolution is substantiated and contains the reasons for FILING WITHOUT SANCTION or FILING WITH SANCTION.

I. FILE WITHOUT SANCTION: After the investigation, if the conclusion reached is that the alleged violation is manifestly minor and does not require further follow-up, it is FILED. It is also the case for repeated complaints that do not contain new and significant information about violations already reported and whose investigation procedure has already been completed, unless new factual or legal circumstances exist that warrant fresh follow-up. In such cases, the complainant must be notified of the decision, and reasons for it given.

II. FILE WITH SANCTION: The Compliance Officer may propose the application of a sanction, but the decision falls to the governing body in coordination with the human resources area, in accordance with the procedures indicated for the application of employment sanctions within the organisation.

III. NOTIFICATION OF THE AUTHORITIES: If the communication received a priori appears to be related to the commission of a crime, the Compliance Officer shall immediately notify the administrative body for the purpose of assessing the complaint by the Public Prosecutor's Office.

In this sense, the Spanish Criminal Procedure Law provides in art. 259 that whoever witnesses the perpetration of any public crime<sup>3</sup> is obliged to immediately notify the investigating judge, magistrate, district or municipal judge, or the public prosecutor closest to the place where they are, at the risk of a fine of 25 to 250 pesetas<sup>4</sup>.

However, the duty to report to the relevant authorities is increased with respect to specific infringements under criminal law. In this regard, the Spanish Criminal Code, in its art. 450<sup>5</sup>, provides for the "failure to prevent crimes or to promote their persecution", punishing anyone who does not prevent the commission of an infringement affecting persons in their life, integrity or health, freedom or sexual freedom, being able to do so through their immediate intervention and without risk to themselves or others, and who, being able to do so, do not go to the authority or their agents to prevent one of these crimes whose next or current commission they are aware of.

Therefore, if, once the investigation of the facts is completed, the veracity of the facts is confirmed, BACHILLER will take all necessary measures to put an end to the alleged situation and, if appropriate and taking into account the nature of the event, shall apply the actions deemed appropriate and included within the disciplinary regime, the employment legislation in force and, where appropriate, in accordance with the criminal legislation referred to above.

<sup>3</sup> The classification of an infringement as a public offence is related to whoever encourages its prosecution (by right of office or by the injured party), public offences being prosecutable by right of office without the need for any prior complaint by the injured party. In addition to crimes against life and freedom, in the catalogue of crimes that generate criminal liability of the legal person there are, by way of example, the following public offences: fraud, bribery, influence trafficking, money laundering, financing of terrorism, etc. crimes against the Treasury and Social Security, crimes against the environment and natural resources, crimes against land use planning, against fundamental rights and public freedoms, smuggling, amongst others. On the other hand, slander and insults between individuals are private offences (the courts can only act when an injured person lodges a charge or complaint) and semi-public offences are prosecutable by right of office once the injured party has initially made the complaint (crimes of discovery and disclosure of secrets, crimes against intellectual property, assault, sexual harassment and abuse, amongst others).

<sup>4</sup> According to current literal wording of art. 259 of the Spanish Criminal Procedure Act.

<sup>5</sup> Art. 450 of the Spanish Criminal Code: 1. Whoever, being able to do so through their immediate intervention and without risk to themselves or others, does not prevent the commission of an offence affecting persons in their life, integrity or health, freedom or sexual freedom, shall be punished by imprisonment for six months to two years if the offence was against life, and by a fine of six to 24 months in other cases, unless the offence not prevented had the same or lesser penalty; in which case the penalty is lower in degree than that of the former. 2. The same penalties shall be incurred by anyone who, being able to do so, does not notify the authorities or their agents so that they may prevent an offence of those provided for in the preceding paragraph and of whose subsequent or current commission they are aware

The measures that may be imposed internally will not prevent, at any time, BACHILLER taking any legal action.

In all cases, both the informant and the investigated party will be NOTIFIED of the RESOLUTION, taking into account the maximum period of three (3) months from receiving the communication, while the informant will not be notified if they have waived such right, if no contact details are available, or they are an anonymous informant.

After this, the Compliance Officer closes the FILE, while respecting in any event the current legislation on data protection.

In the event of a SANCTION, the notification sent to the investigated person shall contain the adoption of the contractual, disciplinary or judicial measures to be taken.

BACHILLER guarantees, as stated in its Internal Information System Policy, that reprisals will never be taken against any person who in good faith notifies them of the commission of a wrongful act, assists in its investigation or helps to resolve it. This guarantee does not apply to those who act in bad faith in order to disseminate false information or to harm people. Against such unlawful conduct, BACHILLER will adopt the appropriate legal or disciplinary measures.

### **3. REGISTRATION OF COMMUNICATIONS**

The head of the system has a book-record of the information received and the subsequent internal investigations, in order to store and / or retrieve key information about each incident, including the date and source of the original communication, the plan for the investigation, the results of interviews or any other investigative procedure, pending tasks and final resolution, as well as chain of custody for any key evidence or information.

### **4. PROTECTION OF PERSONAL DATA**

As stated in the BACHILLER Internal Information System Policy, the processing of personal data derived from the application of that Policy and this Communication Management Procedure, are governed by the provisions of Section VI of Law 2/2023, 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, of Protection of Personal Data and Guarantee of Digital Rights, in Organic Law 7/2021, of 26 May, protection of personal data processed for the purposes of prevention, detection, investigation and prosecution of criminal offences and the execution of criminal penalties.

Considering the principle of data minimisation in the General Data Protection Regulation contained in Law 2/2023, BACHILLER will only handle the personal data necessary for the investigation of the actions or omissions being investigated through the internal system. Consequently, to the extent that the personal data collected are not considered necessary or that it is proved that the information is not true, BACHILLER will proceed with its deletion under the terms established in Article 32 of Law 3/2018<sup>6</sup>.

Likewise, BACHILLER can only process special category data<sup>7</sup> when necessary for the adoption of the corresponding corrective measures or the sanctioning procedures that may be carried out, and, if not, must proceed with their immediate deletion in the terms mentioned above.

Lastly, BACHILLER must ensure that the subjects affected by the processing of personal data carried out as a result of the investigation can exercise the rights of access, rectification of inaccurate data, erasure, limitation, portability, and opposition and not to be subject to a decision based solely on automated processing, taking into account in the exercise of rights that the right of access may not include information about the informant and that the right of objection from the investigated persons may be denied on legitimate grounds.

---

<sup>6</sup> When deletion is appropriate, BACHILLER will block the data, taking all necessary measures to prevent the processing of the blocked information (except for making it available to judicial authorities, the prosecutor's office or the relevant public administrations for the enforcement of possible responsibilities) during the time necessary to maintain evidence regarding the functioning of the system, which, considering the limiting periods indicated in Law 2/2023, is set at 3 years.

It should be noted that the obligation regarding blocking and storage does not apply to personal data contained in communications not investigated, which can only be rendered anonymous.

<sup>7</sup> Personal data that reveals ethnic or racial origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic, biometric data, data relating to a person's health, sexual life or sexual orientation.

## 5. APPROVAL

The Communications Management Procedure has been approved by the Administrator and can be modified in order to improve the confidentiality and effectiveness in the management of communications sent.

Likewise, this procedure can be reviewed and/or modified by the COMPLIANCE OFFICER, who can outsource the service to specialist professionals:

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

It will also be reviewed periodically, even if none of the circumstances described above occur.

## 6. VERSION HISTORY

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

## 7. ANNEX 1 EXTERNAL CHANNELS OF COMMUNICATION

### 7.1. External communication channel of the Independent Informant Protection Authority, I.I.P.A.

All individuals may notify the I.I.P.A. or the corresponding authorities or autonomous bodies of the commission of any actions or omissions referred to in the BACHILLER internal information system, either directly or by prior communication through the internal channel <https://www.corporate-ethicline.com/BACHILLER>.

Specifically, in the Autonomous Community of Catalonia the relevant body in this matter is the Catalonia Anti-fraud Office<sup>8</sup>, which has set up an anonymous complaints box, guaranteeing at all times both the confidentiality of communications and the anonymity of the complainant, which is available through the following link:

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

---

<sup>8</sup> <https://www.antifrau.cat/es/es>

## Buzón de denuncias anónimas

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



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

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

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

### 7.2. Infofraude

The National Anti-Fraud Coordination Service<sup>9</sup> (SNCS), as a national body responsible for coordinating actions to protect the financial interests of the European Union, and reporting to the General Intervention of the State Administration, enables citizens to report facts of which they are aware and which may constitute fraud or any other irregularity in relation to projects or operations financed with funds from the European Union.

In this way, the form for the communication of fraud and irregularities can be accessed via their website (also known as infofraude) and can be used with guarantee of confidentiality:

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

<sup>9</sup> <https://www.igae.pap.hacienda.gob.es/sitios/igae/es-ES/snca/paginas/inicio.aspx>