

INTERNAL INFORMATION SYSTEM POLICY AND MANAGEMENT PROCEDURE

Entity: Ateneaskyclub, S.L.

The purpose of this policy is to specify the functionalities, possibilities and use of the internal information channel to be implemented in the company **Ateneaskyclub, S.L.** Pursuant to the provisions of Law 2/2023 of February 20, regulating the protection of persons who report regulatory violations and the fight against corruption (Law 2/22023), legal entities in the private sector that employ fifty or more employees must have this system in place.

Through the ***internal reporting channel***, any person working for or under the supervision of the company may anonymously report any violation that has occurred in a work or professional context.

1. INFORMATION MANAGEMENT PRINCIPLES AND PROCEDURES

In accordance with the provisions of article 9.2 of law 2/2023, this section refers to the principles of the system and the procedure for managing the information received:

- **Management and internal responsible:** The internal information channel of the company will be managed externally by VARONA ASESORES, S.L.P. However, the complaints received will be forwarded to the person or persons responsible within the company.
- **Internal and external channels:** As indicated above, the company's internal information channel will be as follows: [Access to internal information](#) channel. This channel may be used without prejudice to the possibility of the informant using other external information channel(s) with the competent regional or national authorities or European Union institutions.

- **Acknowledgement of receipt:** when a report is forwarded, acknowledgement of receipt of the communication shall be sent to the informant within 7 calendar days of receipt, unless this could jeopardize confidentiality.

- **Minimum requirements of the complaint: in order for** the complaint to be considered and investigated, it must meet a series of minimum requirements as well as a detailed explanation of the suspicious event or situation (e.g., a detailed explanation of the suspicious event or situation). What the conduct consists of, possible persons involved, approximate dates, means used to carry out the conduct, area of activity affected, possible economic or other impact on the entity and, if possible, provide documents or evidence of the facts).

- **Time limit for resolution:** the time limit for responding to the investigation proceedings shall be 3 months from the receipt of the communication or, if no acknowledgement of receipt was sent to the informant, 3 months from the expiration of the seven-day period indicated in the previous point. In cases of special complexity, the term may be extended up to a maximum of 3 additional months.

- **Right to information:** the person affected by the complaint shall have, at all times, the right to be informed of the actions or omissions attributed to him/her and to be heard at any time. Such communication shall take place at the time and in the manner deemed appropriate to ensure the proper conduct of the investigation. Likewise, the entity may maintain communication with the informant and, if necessary, request additional information.

- **Guarantee of confidentiality:** in the event that any complaint is sent through a channel other than the one established or to different persons, the confidentiality of the communication and the immediate forwarding to the person in charge shall be guaranteed. Failure to comply with this guarantee shall be considered a very serious infringement.

- **Presumption of innocence and honor:** in all cases, the principle of presumption of innocence and the honor of the persons concerned shall be fully respected.

- **Protection of personal data:** the protection of personal data will be carried out in accordance with the provisions of Title VI of the law 2/2023. The access of the

The personal data shall be limited, within the scope of its competences and functions, exclusively to: a) the System Manager and whoever manages them; b) the person in charge of human resources, only when disciplinary measures may be taken against an employee; c) the person in charge of legal services; (d) any processing tasks that may be designated; and e) the data protection officer.

- **Retention of information:** the entity shall keep on file the complaints received, investigation reports, conclusion reports and any other documents for the legally established period.
- **Referral to the Public Prosecutor's Office:** any information shall be immediately forwarded to the Public Prosecutor's Office when the facts could be indicative of a crime. In the event that the facts affect the financial interests of the European Union, the matter will be referred to the European Public Prosecutor's Office.

2. USE OF THE INTERNAL INFORMATION CHANNEL

Below are the instructions for the use of the internal information channel, which can be accessed through the section on the home page of the website or directly by clicking on the following access link: [Access to internal information](#) channel. Clicking on it will take you to the following platform, which has been configured so that the entity's information channel complies with all anonymity and data protection requirements.

● MAIN PANEL

The main panel to complete in case you want to report a violation is the one on the right "**Information to Report**". It has a first informative section on the internal information channel and, subsequently, a series of drop-downs that must be completed so that the platform allows the complaint to be entered.

1. Identify the relationship with the organization

First, the relationship with the organization must be identified. If the complainant is an employee, member of the management team, shareholder, etc., this section must be completed with the "*Internal*" option. In any other case, i.e. in case of customers, suppliers, etc. the option to choose should be "*External*".



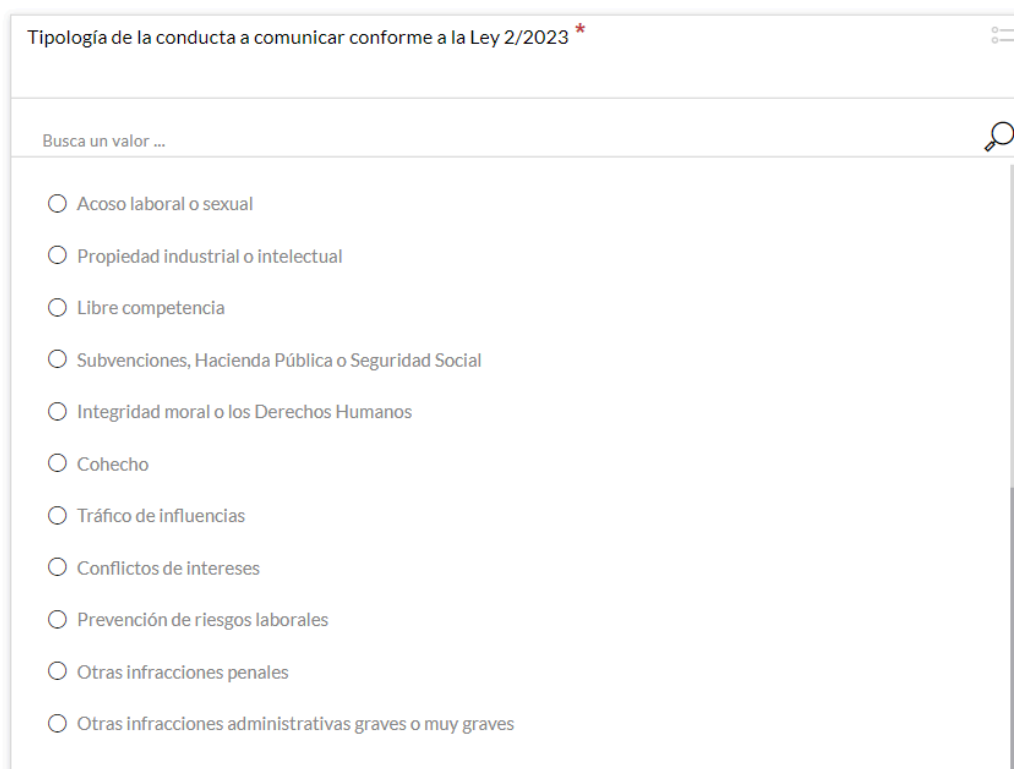
Relación con la organización *

Busca un valor ...

- Interna
- Externa

2. Typology of the behavior to be communicated

Secondly, the type of behavior to be communicated must be identified. To do this, you must select one of those listed.



Tipología de la conducta a comunicar conforme a la Ley 2/2023 *

Busca un valor ...

- Acoso laboral o sexual
- Propiedad industrial o intelectual
- Libre competencia
- Subvenciones, Hacienda Pública o Seguridad Social
- Integridad moral o los Derechos Humanos
- Cohecho
- Tráfico de influencias
- Conflictos de intereses
- Prevención de riesgos laborales
- Otras infracciones penales
- Otras infracciones administrativas graves o muy graves

While there are several categories, the behavior itself may not be defined so that, in the end, there are two generic options that can be used: "*Other criminal offenses*" or "*Other serious or very serious administrative offenses*".

3. Anonymity in communication

Third, the whistleblower may choose to remain anonymous or identify himself/herself. If you wish to make it anonymous, you must indicate "Yes" in the drop-down box. Otherwise, you must indicate "no" and, in turn, state your full name and surname, e-mail address for notification purposes and, if you wish, a landline or mobile contact telephone number.

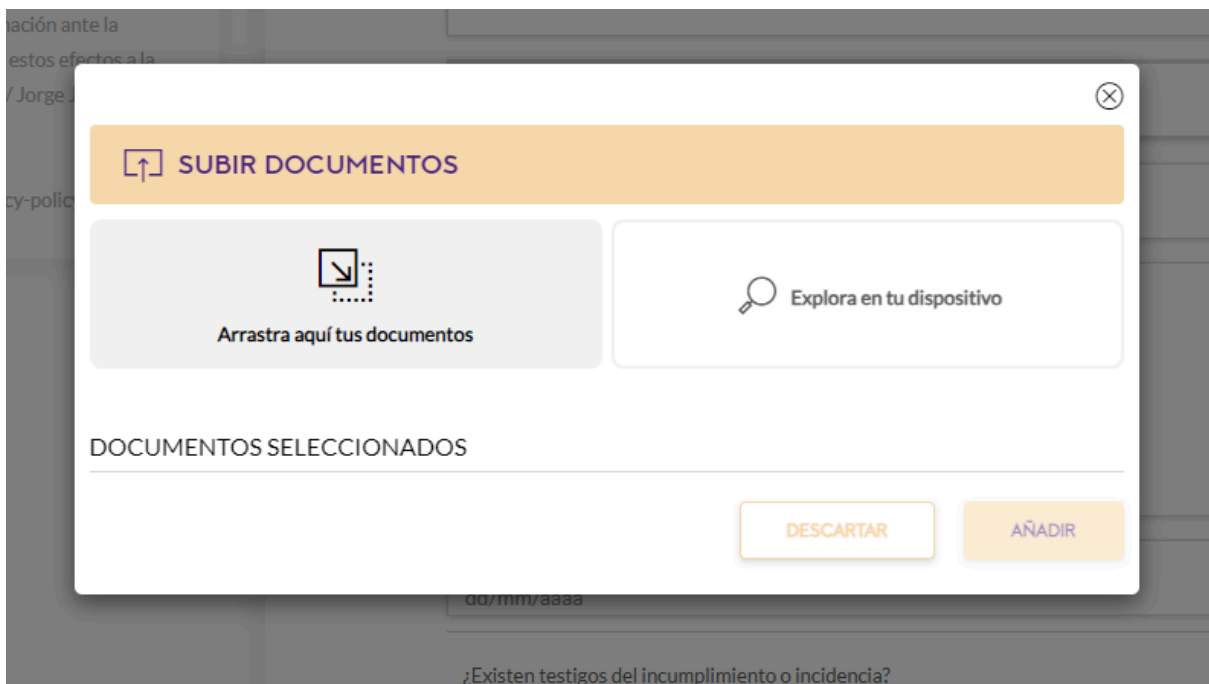
¿Desea que la comunicación sea anónima?	▼
No	
Nombre y Apellidos *	▲
Email *	✉
Teléfono	▲

4. Description of the violation

Fourth, the platform has some fields to describe the infringement to be reported.

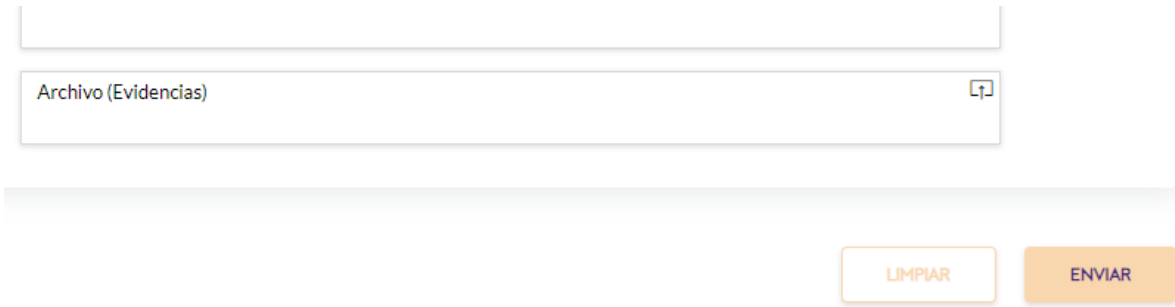
- *Description of the violation*: this is a mandatory field to be filled in. The text to be included is free and the complainant may state the complaint in it.
- *Incident date*: this is an optional field, which can be filled in if the exact date on which the violation occurred is known.
- *Witnesses*: this is also an optional field. If there were witnesses to the violation you can check "Yes" and, if applicable, list them including their name and surname so that they can be contacted during the investigation of the complaint. Otherwise, "No" will be indicated.
- *File (evidence)*: this last field, also optional, allows you to attach files. For example, screenshots, pictures, audios, etc. They will be added by dragging and *clicking* "Add".

Descripción de la infracción *	🗑
Fecha de incidencia	📅
dd/mm/aaaa	



5. Sending the complaint

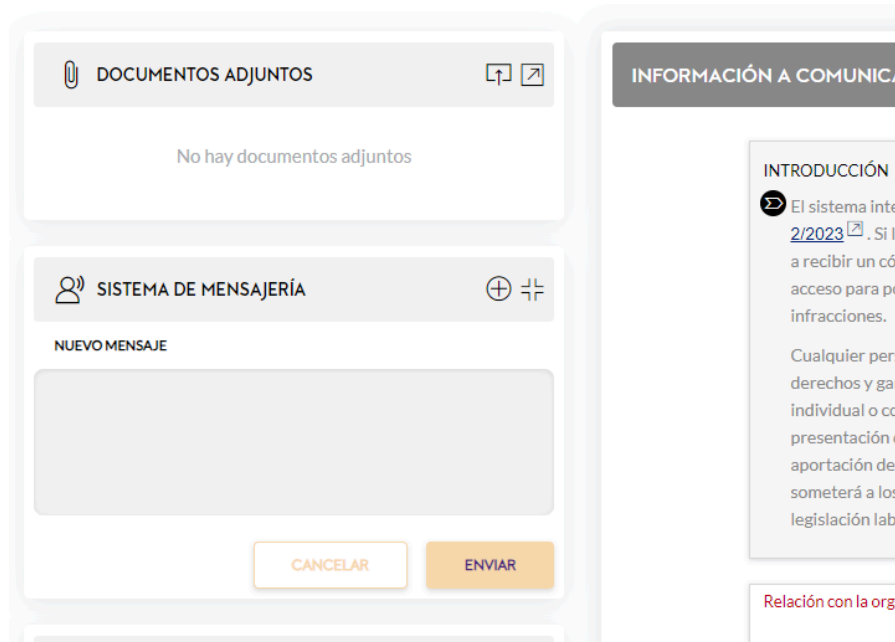
Once all the required fields have been completed, the report can be sent by clicking on the "Send" button located at the bottom right of the screen.



● **SECONDARY PANELS**

On the left side of the platform, there are two secondary panels that can also be used.

1. **Attached documents.** Allows you to upload additional documents attached to the complaint. It works with the same system as the *Archive (Evidence)* section.
2. **Messaging system.** Through this panel, the informant can send messages to the channel manager and the channel manager can, in turn, respond.



3. FREQUENT QUESTIONS

How can I access the complaint channel?

The complaints channel can be accessed either through:

- The company's website.
- Through the link contained in this document: [Access to internal information channel.](#)

Once the complaint has been filed, how can it be followed up?

- If the report is anonymous, the informant will receive a code and a URL once the form has been completed. You must save the access to be able to consult at any time the status of the resolution of the complaint or if the person in charge or the entity managing the channel has been contacted through this channel.
- If the complaint is not anonymous, the complainant shall identify himself/herself by indicating name and surname, e-mail address and, if applicable, telephone number. In this case, you will receive a link to the e-mail to know the status of the complaint.

What is the complaint handling procedure?

As indicated in the section "*Principles and procedure for information management*", the channel will be managed externally by VARONA ASESORES, S.L.P., who will receive the complaints posted on the platform. A first filter will be carried out and they will be communicated within a maximum of 5 working days to the internal manager who will carry out the appropriate investigations.

How does the new regulation protect the whistleblower?

Articles 35 et seq. of law 2/2023 provide that persons who report or disclose violations are entitled to protection when:

- a) have reasonable grounds to believe that the information referred to is true at the time of communication or disclosure, even if they do not provide conclusive evidence, and that such information falls within the scope of this law,
- b) the communication or disclosure has been made in accordance with the requirements of this law.

The law also expressly prohibits acts constituting retaliation, including threats and attempts. Some examples of retaliation would be suspension of employment contract, dismissal, negative performance evaluation or references, denial of training, denial or cancellation of a license or permit, discrimination, etc.

What measures apply to the respondent?

During the processing of the file, the persons affected by the communication shall have the right to the presumption of innocence, the right of defense and the right of access to the file under the terms regulated in this law, as well as the same protection established for informants, preserving their identity and guaranteeing the confidentiality of the facts and data of the procedure.

This policy may be modified in the event of new regulatory modifications that affect its content. The entity is not responsible for the use of this document as well as the internal information channel for uses other than those established, i.e. in accordance with article 2 of the law 2/2023.