

# Terms of Use and Privacy Policy

This information channel is available to comply with the regulations on the protection of people who report violations of Union Law.

It is a secure and absolutely confidential channel. You can even communicate with us anonymously. Before making a communication through this channel, you must read and accept the conditions of use (to know what facts can be communicated through this channel and which informants are protected by the regulations) and the privacy policy.

It is important that you understand that what is sought to be preserved through said regulations is the protection of the whistleblower from possible retaliation in the employment or professional relationship in which context there is an infraction of the organization that the organization or its employees or managers may have committed, in the areas indicated below, which may constitute a serious or very serious criminal or administrative offense or directly affect the general interest .

Therefore, before providing any information, it is important that you read and take into account the following issues:

## **1.- What information can you provide through this channel?:**

- Certain regulatory violations or information in the framework of the fight against corruption that marks the annex to Directive (EU) 2019/1937, of October 23, 2019, regarding:

- Public procurement and awarding of concessions
- Financial services, products and markets (banking, credit, investment, insurance and reinsurance, personal pension or retirement products, securities services, investment funds, payment), and prevention of money laundering and terrorist financing
- Safety and conformity requirements of products placed on the Union market
- Transport safety
- Environmental Protection
- Radiation protection and nuclear safety
- Food and feed safety, animal health and animal welfare
- Public health
- Consumer protection
- Privacy and personal data protection, network and information systems security
- Infringements of tax, competition and/or public aid laws
- Violations of the rest of the legal system that may constitute a serious or very serious criminal or administrative offense or that directly affect the general interest
- Harassment in any of its forms
- Others (must be detailed in the text of the communication)

**2.- What information can you NOT provide through this channel?:** It is a channel to notify the organization of offenses that it or its employees or managers may have committed in the areas indicated above **that may constitute a serious or very serious criminal or administrative offense or that directly affect the general interest**; NO to communicate violations of private law rules that regulate relationships between individuals and that do not affect the proper functioning of public and private institutions. That is, this is NOT a channel to communicate service complaints; interpersonal conflicts that affect the informant and the people to whom the communication or disclosure refers (unless they constitute a serious or very serious criminal or administrative offense); or make salary claims, vacations...; spread rumors; In short, communicate information that refers to actions or omissions not included in point 1 above.

3.- The protection for whistleblowers provided by the regulations on the protection of people who report violations of Union Law affects people who have obtained information about violations **in a work or professional context**, including:

- public employees and paid workers;
- the self-employed;
- shareholders, participants and persons belonging to the administrative, management or supervisory body of a company, including non-executive members;
- anyone working for or under the supervision and direction of contractors, subcontractors and suppliers
- to the legal representatives of the workers in the exercise of their functions of advice and support to the informant.
- Natural persons who, within the framework of the organization in which the informant provides services, assist him in the process.
- Individuals who are related to the whistleblower and who may face retaliation, such as co-workers or family members of the whistleblower, and
- Legal entities, for which you work or with whom you maintain any other type of relationship in a work context or in which you hold a significant stake.

4.- The information you provide must be based on good faith, since the law does not cover anyone who provides false, misrepresented, or illegally obtained information.

5.- The provision of personal data is the sole responsibility of the informant, who must comply with the regulations in this regard. Likewise, the confidentiality and custody of the user and password to access the application is the responsibility of the informant.

6.- If you wish, you can provide information anonymously; If when making the communication, you identify yourself or indicate an address, email or safe place for the purpose of receiving the notifications, we will send you an acknowledgment of receipt of the communication within seven calendar days of receipt, unless this may jeopardize the confidentiality of the communication.

7.- Whether you identify yourself or not, we recommend that you provide a way to maintain communication with you or request additional information to be able to process, where appropriate, the investigation and also be able to inform you of the actions or omissions attributed to you, and so that you can exercise your right to be heard at any time. If you do not identify yourself and make an anonymous communication, the application will send you a username and password, which you can change, and with which you can check the status of your communication. In this case, we will communicate with you through the application, since we do not know who is behind that username and password nor do we have access to them, so you will have to enter regularly and check if you have messages, otherwise the investigation may be limited

8.- The complaint will be received by the person in charge of the system.

We will preserve the identity of the informant. Said identity will never be subject to the right of access to personal data and can only be communicated to the judicial authority, the Public Prosecutor or the competent administrative authority, demanding that in any case third party access to it be prevented. The person to whom the reported facts refer will not be informed in any case of the identity of the informant or of the person who, where appropriate, has carried out the public disclosure.

We will also preserve the information of the people to whom the facts reported in the communication refer to the risk that the information, even with apparent signs of truth, has been manipulated, is false or responds to motivations that the Law cannot protect. In these cases, the sole and exclusive responsibility of the informant, who must respond in any case, exempting the owner entity, as well as the manager of the internal information system.

9.- Access to our internal information system is limited:

- The person in charge of the system and, where appropriate, the person who manages it directly and the persons in charge of the treatment that may be designated.
- To the person in charge of human resources in the field of disciplinary measures
- To the person in charge of the legal services of the entity, only if legal measures must be adopted
- To the Data Protection Delegate .

10.- In any case, we will respect the presumption of innocence, the right to be heard and the honor of the people investigated.

In the event that we open an investigation, the maximum duration of the investigation may not exceed three months from the receipt of the communication, except: cases of special complexity that require an extension of the term, in which case, this may be extended up to a maximum of three additional months or specific cases that have legally established other terms (eg, harassment) .

11.- In addition to this internal channel, you can also use, when created, the external channels of information before the competent authorities, in this case, the Independent Authority for the Protection of Informants and, where appropriate, before the institutions, bodies or agencies of the European Union.

12.- In order to calculate the deadlines provided in the regulations for the management of the information received, the closing periods of the entity in which you make the communication will not be calculated, according to the calendar applicable to it (holidays, holidays, non-business days in general...)

13.- **Privacy policy :**

<b>INFORMATION ON THE PROTECTION OF PERSONAL DATA</b>	
<b>Responsible treatment</b>	ZAYER, S.A. - A01002955 Mailing address: C/Portal de Bergara 7 01013 Vitoria-Gasteiz (Álava) - Spain Email: lopd@zayer.es Telephone: 945 26 28 00
<b>Purpose and legitimacy</b>	<b>Purpose:</b> registration and management of communications made through the internal information system  <b>Legitimation:</b> Compliance with legal obligations derived from the regulations governing the protection of persons who report violations of regulations and the fight against corruption, and fulfillment of a mission carried out in the public interest or in the exercise of public powers conferred on the person responsible.

<b>automated decisions</b>	We do not make decisions based solely on automated processing, including profiling, that produce legal effects on the data subject or significantly affect them in a similar way.
<b>Recipients</b>	We will communicate to third parties the necessary data to process the complaint and/or the disciplinary, sanctioning or criminal procedures that, if applicable, proceed (eg, to the company that manages the internal information system, if it is outsourced, or to the necessary authorities, entities or organizations). Communication is a legal requirement. We do not carry out international data transfers, unless it is necessary for the previous case. We do not process special categories of data, unless they are contained in the information provided by the complainant.
<b>conservation criteria</b>	The personal data related to the communications received and the internal investigations carried out will be kept for the necessary and proportionate period to comply with the applicable regulations. After three months have elapsed from the receipt of the communication without initiating investigation actions, they will be deleted, unless they are kept to demonstrate the operation of the system. Communications that are not processed will only be anonymous, without applying the blocking obligation of article 32 LOPD 3/2018. In no case will the data be kept for a period of more than 10 years.
<b>Rights</b>	<p>You can, when appropriate, access, rectify, delete, oppose, request the portability of the data, limit the treatment, and not be subject to only automated decisions, as detailed in the additional and complete information in the privacy policy of <a href="http://www.zayer.es">www.zayer.es</a>.</p> <p>If the person to whom the facts reported in the communication refer exercises the right of opposition, it will be presumed that, unless proven otherwise, there are compelling legitimate reasons that legitimize the processing of their personal data. The person to whom the reported facts refer will not be informed of the identity of the informant or of the person who made the public disclosure.</p> <p>We will preserve the identity of the informant. Your identity will never be subject to the right of access to personal data and can only be communicated to the judicial authority, the Public Prosecutor or the competent administrative authority, demanding that in any case third party access to it be prevented.</p> <p>Those who make the communication through this internal channel can also do so through the external channels of information before the competent authorities (once they are available), in this case, the Independent Authority for the Protection of Informants and, where appropriate, before the institutions, bodies or agencies of the European Union</p>
<b>Origin</b>	If they do not come from the interested party, the data has been collected from the informant and from the information contained in the information provided by him.