Forjas de Berriz
GRUPO BERRIZ DE FORJA

Internal Information Systems Policy and Whistleblower Protection

The Communication Channel, in application of Law 2/2023, of February 20, regulating the protection of persons who report regulatory infringements and the fight against corruption, as well as Directive (EU) 2019/1937, of the European Parliament and of the Council, of October 23, 2019, on the protection of persons who report breaches of Union law; has as its mission to promote the strengthening of the culture of information, the integrity infrastructures of organizations and the promotion of the culture of information or communication as a mechanism to prevent and detect threats to the public interest.

In this regard, the organization understands that obtaining relevant information that may affect its Compliance System—whether in the form of system non-compliance or inquiries regarding how to proceed under it—is a priority. The organization's Compliance System is based on the provisions of Article 31 bis of the Criminal Code—and subsequent and related articles arising from the reforms to the Criminal Code enacted by Organic Law 5/2010, of June 22, and Organic Law 1/2015, of March 30—regarding the obligation of every company to establish within itself an organizational, management, and control model for the prevention of crimes. Therefore, non-compliance with the Compliance System will be related to the prevention, detection and rejection of matters that affect the criminal liability of legal entities, including, but not limited to, matters related to corruption, trade secrets, the privacy of individuals, fraud against individuals or committed in the public sector, smuggling, public health and land use planning, among others.

Furthermore, the organization rejects any illegal behavior, particularly that which falls under the aforementioned regulations. In this regard, it is absolutely convinced that obtaining any information that may be relevant to preventing, addressing, or reporting to the appropriate authorities any legal breaches—in accordance with the aforementioned regulations—that may arise within its organization is essential. To facilitate access to this useful information and promote good governance and appropriate, legal conduct within the organization, the Communication Channel has been established.

This channel has the appropriate characteristics to allow its users to provide relevant information for the aforementioned purposes.

In this regard, the channel will guarantee a secure, independent, and confidential operating system and structure, ensuring that only those involved in the process, in accordance with the aforementioned legal provisions, have access to the information contained therein, including data relating to the identification of individuals. This will

prevent unauthorized personnel from accessing the information during the entire process of data collection and its subsequent processing.

The organization intends, through the creation of this channel, to unify, as far as possible, the existing information channels, facilitating communication through all available means, whether written or verbal.

That being said, the channel will have appropriate systems in place to protect users from reprisals for the information they provide, in accordance with the law; always within the framework of a firm rejection of any false accusations that may arise and respect for the presumption of innocence of every person involved in the process.

Usage Procedure

Communication Channel: Information to be submitted through the Internal Information System must be sent in writing to the email address:

confidencial@forjasdeberriz.com

Informants may also submit their communications in writing through the suggestion box located on the premises or to the Independent Authority for the Protection of Whistleblowers by accessing its website **www.porteccioninformante.gob.es**, or to any other competent body.

• Once the communication is received, the channel user will be acknowledged within seven calendar days.

• In the event of inadmissibility after content assessment, the user will be notified if possible.

• Admitted communications will be investigated by the compliance officer.

• The process will conclude with a resolution report within three months of receiving the communication.