

**INTERNAL INFORMATION SYSTEM POLICY - WHISTLEBLOWER COMPLAINTS  
AND ADVOCACY CHANNEL AND WHISTLEBLOWER PROTECTION OF THE  
ENTITY KAROSSERIEWERKEN DRESDEN ESPAÑA S.L.U.**

**I.- STATEMENT OF COMPLIANCE**

In **KAROSSERIEWERKEN DRESDEN ESPAÑA S.L.U.**'s commitment to the daily work of building a sustainably successful company/entity and promoting responsibility, professional ethics, integrity, honesty, loyalty and efficiency, we adhere to the principles, values and standards of conduct that should inspire and guide the behaviour of the people integrated in our organisation in the development of their work and professional activity.

We are committed to promoting a strong integrity infrastructure and fostering a reporting culture as a mechanism to prevent and detect conduct within the company contrary to the code of ethics, corporate policies approved by the company, the criminal code, measures and actions implemented in our Plans and Protocols, as well as threats to the public interest.

For this reason, our organisation rejects any situation in which violations of the law, internal rules, the regulatory compliance system and business ethics may occur, including financial or accounting fraud, harassment, intimidation, discriminatory treatment of employees or third parties, deception of customers, unfair treatment of competitors or inappropriate behaviour affecting the professional development of our staff. Such conduct is unacceptable and may seriously affect the development of the aims and objectives of our organisation and the people who form part of it, as well as relations with our customers, suppliers and collaborators.

In its fulfilment, the entity's management body has agreed to design, implement, maintain and improve an INTERNAL REPORTING SYSTEM in accordance with the provisions of Law 2/2023 of 20 February, regulating persons who report regulatory infringements and the fight against corruption, in order to provide adequate protection for whistleblowers and strengthen the reporting culture in our organisation.

In order to guarantee the diligent management of the internal information system, the entity's management body has appointed the person in charge (or Committee in charge) of the System as the person responsible for it, who, as an executive of the entity, shall carry out his or her functions independently and autonomously from the entity's administrative and management bodies, with his or her functions including ensuring the correct application of the principles that form part of this policy.

**2.- PERSONAL SCOPE OF APPLICATION**

Although the commitment to regulatory compliance in the development and implementation of the SIS starts with the initiative of the entity's administrative (or governing) body, the entire management team and the entire workforce assume the commitment to share its implementation and make it their own, as well as to involve, as far as possible, their collaborators, working to achieve its dynamisation until it is fully consolidated in the corporate culture.

This policy therefore applies to the company's shareholders, its management body, executives, employees, partners and collaborators.

### 3.- SCOPE OF ACTION

In addition to the reference to the material scope of application of Law 2/2023 of 20 February, as provided for in Article 2 of the Law, the scope of the Internal Information System covers the following fields:

- (a) Personal responsibility.
- (b) Law enforcement.
- (c) Relations with co-workers.
- (d) Relations with customers and suppliers.
- (e) Professional development and training.
- (f) Health and safety at work.
- (g) Environmental protection.
- (h) Prevention of money laundering.
- (i) Right to privacy.
- (j) Confidentiality and use of company information.
- (k) Use and protection of company and third-party assets.

### 4.- GENERAL PRINCIPLES OF THE SYSTEM

The internal information system is governed by the following principles:

- **Accessibility and Advertising:** The entity shall provide internal information channels that allow the persons described in article 3 of Law 2/2023 of 20 February to report breaches of the aforementioned regulations in a work or professional context in writing, verbally or both. Information on reporting channels shall be clear, easily accessible and easy to use for persons wishing to report an infringement. In addition, the functioning of the reporting channels will be public. To this end, we will set up a specific space on our corporate website.
- **Confidentiality:** Communications through the information channels provided may be made anonymously (except for information relating to the Protocol for the prevention of sexual harassment and harassment based on sex), and at all times the internal information channels shall be confidential and shall have technical security guarantees. In the event that the informant decides to make the communication without remaining anonymous, his or her identity shall be treated as confidential information. The processing of this information shall be limited to a small group of persons, so that the identity of the informant and that of third parties affected may not be revealed, except in the cases expressly provided for in the applicable regulations. The necessary technical and organisational measures shall be employed to ensure that the communications and investigations managed in the system are handled securely, confidentially and in compliance with the regulations on the protection of personal data..
- **Efficiency:** The information system and enabled channel will be processed as quickly and diligently as possible and always respecting the deadlines established in the applicable regulations. As a general rule, receipt of the communication must be acknowledged within 7 days, and the period for responding to the investigation actions shall not exceed 3 months from the communication, except in cases of greater complexity, in which case the response period may be extended up to a maximum of 6 months.
- **Objectivity:** Communications made through the information system shall be treated objectively and the presumption of innocence of the persons affected by communications

shall be maintained until the end of the investigation. The person in charge (or the Committee in charge, as the case may be) of the System and the persons in charge of managing the communications shall try to avoid in all cases any type of conflict of interest that may arise.

## **5.- WHISTLEBLOWER PROTECTION**

Persons who report possible infringements through the internal information system of our entity in compliance with the requirements established by Law 2/2023 of 20 February, shall enjoy the guarantees of protection against possible reprisals provided for in the regulations.

Our company expressly prohibits the commission of any retaliatory acts, including threats and attempts of retaliation, arising from the disclosure made. Whistleblowers will be protected from acts or omissions prohibited by law, unfavourable treatment or disadvantage in the employment context because of their status as a whistleblower or because they have made the public disclosure..

## **6.- ADVERTISING**

To ensure the correct management and proper functioning of the internal information system, this system policy will be duly disclosed on the organisation's website, so that all staff and persons related to the company are aware of its principles and can be governed by them.

## **7.- VALIDITY AND REVISION**

The present Policy of our Internal Information System has come into force from the date of its approval by the governing body on ....., and its validity will be indefinite, without prejudice to its periodical review, proceeding to its modification when appropriate, in which case it must be communicated to the interested parties.