WHISTLEBLOWING SYSTEM POLICY

ISOVOLTA S.A.U.

Approved by the Board of Directors on April 1, 2025

DOCUMENT NAME	Whistleblowing System Policy
DESCRIPTION	This Policy regulates, in accordance with the provisions of Law 2/2023, the general principles governing ISOVOLTA's Whistleblowing System.
SCOPE OF APPLICATION	ISOVOLTA S.A.U.
SUPERVISOR	ISOVOLTA's Responsible of the Whistleblowing System.
APPROVAL DATE	01/04/2025
EFFECTIVE DATE	01/04/2025
VERSION	2.0

DEFINITIONS

Whistleblower Channels	Refers to all the Whistleblowing Channels enabled by Constantia Industries AG to allow the submission of Complaints.
Complaints	Refers to the communication of information on infringements through the Whistleblowing Channels.
Whistleblower	Refers to the natural Person who falls within the scope of this Policy and who communicates Information on infringements to ISOVOLTA or publicly discloses such information.
Directive (EU) 2019/1937	Refers to Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons who report breaches of Union law.
ISOVOLTA	It refers to ISOVOLTA S.A.U., with registered office at Avda. Can Salvatella, 85 a 97, Pican Salvatella, Barbera Del Valles (Spain).
Information of infringements	Refers to all the information about actual or potential infringements that have occurred or are very likely to occur at ISOVOLTA, including reasonable suspicions and attempts to conceal such infringements.
Law 2/2023	It refers to Law 2/2023, of February 20, 23, regulating the protection of persons who report regulatory violations and the fight against corruption.

I. INTRODUCTION

In compliance with Directive (EU) 2019/1937, Constantia Industries AG has implemented a **Whistleblowing System** (hereinafter referred to as the "**System**") in all the companies of the group, including ISOVOLTA.

In order to implement the principles contained in the Directive, as well as in **Law 2/2023,** it has been agreed to approve this "**Whistleblowing System Management Policy**" (hereinafter, the "**Policy**"), which establishes the general principles governing the Whistleblowing System and the rights of the Whistleblower.

II. SCOPE OF APPLICATION

The target scope of this Policy shall include all Complaints submitted by the persons listed below through the Whistleblowing Channels enabled by ISOVOLTA and which involve an alleged Infringement.

The subjective scope of the Policy shall include the following persons:

i. Employees;
ii. Self-employed workers;
iii. Former employees;
iv. Shareholders, participants, members of the administrative, management or supervisory body of the company, including non-executive members;
v. Persons working for or under the supervision and direction of contractors, subcontractors and suppliers;
vi. Volunteers, trainees and workers in paid or unpaid training periods and people who have been part of a selection process or pre-contractual negotiation.

The protection guaranteed to the Whistleblower shall extend to:

- the legal representatives of the employees in the exercise of their functions of advising and supporting the Whistleblower;
- the natural persons who, within the framework of the organization in which the Whistleblower provides his/her services, assist him/her in the Complaint process;

- other individuals who are related to the Whistleblower and who may suffer retaliation, such as co-workers or family members of the Whistleblower.

Likewise, protection shall be guaranteed to legal entities for which the Whistleblower works or with which he/she has any other type of relationship in an employment context or in which he/she holds a significant shareholding.

III. GENERAL PRINCIPLES OF THE WHISTLEBLOWING SYSTEM

The general principles governing ISOVOLTA's Internal Information System are as follows:

1. Guarantee the confidentiality of the information contained in the Complaint and, in particular, the identity of the Whistleblower.
2. To have a person in charge of the Internal Information System who is fully independent and autonomous.
3. Guarantee at all times the presumption of innocence and the right of defense of the persons affected by a Complaint.
4. Always act in compliance with the principles of proportionality, suitability and reasonableness.
5. Zero tolerance for retaliation, if any, that may be taken against a Whistleblower.

IV. CONCEPT OF INFRINGEMENT

For the purposes of this Policy, the concept of "**INFRINGEMENT**" shall include:

1. Acts or omissions constituting breaches of European Union law, provided that:
   a) Enter within the scope of the acts of the European Union listed in the Annex to Directive (EU) 2019/1937, relating to the following areas: public procurement; financial services, products and markets and prevention of money laundering and terrorist financing; product safety and conformity; transport safety; environmental protection; radiation protection and nuclear safety; food and feed safety, animal health and animal welfare; public health; consumer protection; protection of privacy and personal data; and network and information systems security.
   b) Affect the financial interests of the European Union; or
   c) They affect the internal market, including infringements of the European Union rules on competition and aid granted by the States, as well as infringements relating to the internal market in connection with acts that infringe the corporate tax rules or

practices whose purpose is to obtain a tax advantage that distorts the object or purpose of the legislation applicable to corporate tax.

2. Actions or omissions that may constitute a serious or very serious criminal or administrative infraction, including all those that imply economic losses for the Public Treasury and Social Security.
3. Any breach of ISOVOLTA's internal regulations, as well as of the values, guidelines or rules of conduct contained in ISOVOLTA's Code of Ethics;
4. Any contingency that may pose a risk to the reputation of ISOVOLTA and Constantia Group companies;
5. Any other conduct that may be considered as generating an ethical dilemma; and,
6. Any other fact or circumstance that may reflect relevant exposure to a risk of legal or any other type of non-compliance.

Reports shall always be made in good faith and with honesty, presenting reasonable grounds for truthfulness.

The Whistleblower shall be protected even if the information is inaccurate or, upon investigation, the Whistleblower is proven to be mistaken.

V. THE PERSON RESPONSIBLE FOR THE INTERNAL INFORMATION SYSTEM

The competent body to manage, investigate and respond to the Complaints filed through the Complaints Channels shall be the Responsible of the Whistleblowing System, appointed by the ISOVOLTA Board of Directors.

The Responsible of the Whistleblowing System, among other responsibilities, shall be the body responsible for supervising, interpreting and ensuring compliance with this Policy, as well as supervising the Whistleblower Channel.

His appointment and termination shall be communicated to the Competent Authority for the protection of the informant.

The Responsible of the Whistleblowing System shall perform his functions in an independent, impartial and autonomous manner, having been provided with the necessary means for the development of his competencies.

VI. RIGHTS AND GUARANTEES OF THE WHISTLEBLOWER

a. Whistleblowers shall be able to file Complaints anonymously or by name.

b. The Confidentiality of the data provided in the Complaint, as well as the identity of the Whistleblower, shall be guaranteed in any case.

c. The Affected Person(s) to whom the facts related in the Complaint refer shall in no case be informed of the entity of the Whistleblower.

d. The processing of personal data carried out within the framework of the Whistleblowing Channels shall be governed by the provisions of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, Organic Law 3/2018 of 5 December and Organic Law 7/2021 of 26 May.

e. Retaliation against the Whistleblower will be declared null and void and will result in a penalty. Protection against retaliation shall extend for a period of two (2) years from the initiation of investigations. Retaliation is understood to be any act or omission that is prohibited by law, or that, directly or indirectly, involves unfavorable treatment that places the persons who suffer it at a particular disadvantage with respect to another in the labor or professional context, solely because of their status as Whistleblowers.

f. Independence, impartiality and absence of conflicts of interest are guaranteed in the processing of Complaints.

g. Whistleblowers may report Infringements through the Whistleblowing Channels managed by the competent authorities, i.e. to the Independent Whistleblower Protection Authority. However, priority will be given to the internal Whistleblowing channel whenever possible.

h. Whistleblowers, provided they fall within the scope of protection of Law 2/2023, may access the following support measures:

   (i) full and independent information and advice on available procedures and remedies, protection against retaliation, and the rights of the person concerned,

   (ii) effective assistance by competent authorities to any relevant authority involved in their protection against retaliation, including certification that they are eligible for protection under the Act,

   (iii) legal assistance in criminal proceedings and in cross-border civil proceedings in accordance with Community law, and

(iv) financial and psychological support, on an exceptional basis, if so decided by the Independent Whistleblower Protection Authority.

VII. PROTECTION OF PERSONAL DATA

The processing of personal data shall be governed by the provisions of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, Organic Law 3/2018 of 5 December on the Protection of Personal Data and Guarantee of Digital Rights, and Organic Law 7/2021 of 26 May.

No data shall be collected if it is not manifestly relevant to the processing of a specific Complaint or, if collected by accident, it shall be deleted without undue delay. In any case, personal data that are not necessary for the knowledge and investigation of Infractions shall not be processed and, if necessary, shall be immediately deleted.

The personal data contained in the complaints may be communicated to Judges and Courts, to the Public Prosecutor's Office or to the competent Public Administrations only in those cases in which it is considered that the irregularities allegedly committed could constitute a specific administrative infraction or crime and are strictly necessary for the development of the pertinent investigation by the competent bodies.

Access to the data contained in these systems shall be limited, within the scope of their competencies and functions, exclusively to:

1. The person in charge of the internal system and whoever manages it directly;
2. The Director of Human Resources when disciplinary measures may be taken against an employee;
3. The Director of Legal Services, should legal action be taken in relation to the facts described in the Complaint;
4. The persons in charge of the treatment that eventually are designated.
5. The Data Protection Officer.

However, access to personal data by other persons, or even its communication to third parties, shall be lawful when necessary for the adoption of disciplinary measures or for the processing of investigation or judicial proceedings, as the case may be.

The necessary technical and organizational measures have been adopted to preserve the identity of the Complainant and to guarantee the confidentiality of the data corresponding to the Persons Affected by the Complaint and any third party mentioned in the Complaint.

In the event that the Affected Person exercises his/her right to object, it will be presumed, in the absence of evidence to the contrary, that there are compelling legitimate reasons that legitimize the processing of his/her personal data.

The data being processed may be kept in the system for the time necessary to decide on the origin of the investigation or, once the investigation has begun, when they are no longer necessary or relevant for the purpose for which they were collected, proceeding, in the first case, to their anonymization and, in the second case, to their blocking.

For more information about the processing of your personal data, please consult our Privacy Notice .

VIII. THE EXTERNAL WHISTLEBLOWING CHANNEL MANAGED BY THE INDEPENDENT WHISTLEBLOWER PROTECTION AUTHORITY (I.W.P.A.)

All individuals who are part of the groups with access to the Whistleblowing System may contact the Independent Whistleblower Protection Authority (IPA), or the corresponding regional authorities or bodies, to report the commission of any of the Infringements included in the scope of application of this Policy.

IX. POLICY UPDATE AND REVIEW

At the proposal of the Responsible of the Whistleblowing System, the content of this Policy shall be updated and revised when necessary due to regulatory developments, best practices in the field, as well as changes in ISOVOLTA's business model.