INTERNAL INFORMATION SYSTEM POLICY OF

Cintas Adhesivas UBIS, S.A.

February 2024

CHANGE CONTROL

Version	Date	Remarks
v.1	February 2024	

Content

INTRODUCTION

Cintas Adhesivas UBIS, S.A. (hereinafter, Cintas Adhesivas UBIS) has designed an Internal Information System in accordance with the provisions of Act 2/2003, of 20 February 2023, governing the protection of those reporting regulatory violations and the combating of corruption (hereinafter, "Act 2/2023").

The main aim established by Act 2/2023 is that all those obliged to comply with the regulation should implement an internal information system, which means that such companies must have one or more internal information channels.

Cintas Adhesivas UBIS has thus set up a whistleblowing channel made available to employees and third parties that have an occupational or professional link to the organisation (shareholders, suppliers, customers, etc.), allowing them to report any acts that could constitute serious or very serious criminal or administrative violations, or any other irregularities of which they may have learned and which are in breach of the company's code of ethics or infringe the regulations applicable to the company.

This policy is thus intended to comply with all the requirements set forth not only in this regulation, but all those potentially connected to this matter, and the activity of the organisation itself.

APPLICABLE LEGISLATION

I. Law 2/2023, of 20 February 2023, regulating the protection of persons reporting regulatory violations and on combating corruption.
II. REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL, of 27 April 2016, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (the General Data Protection Regulation).
III. Act 3/2018, of 5 December 2023, on the Protection of Personal Data and guarantee of digital rights.
IV. Circular 1/2016, of 22 January 2016, on the criminal liability of legal entities in accordance with the reform of the Penal Code conducted by means of Act 1/2015.
V. Act 10/1995, of 23 November 1995, on the Penal Code.

DEFINITIONS

Internal Information System: Set of procedures and tools for the administration of internal communications which could entail a serious criminal or administrative violation, or a violation of EU regulations.

Internal Information Channel: Mechanism or instrument which can be used to report acts comprising a serious violation of occupational or criminal provisions, or otherwise a violation of EU regulations.

Whistleblower: Person communicating any action or omission that would constitute a serious or very serious criminal or administrative violation or any that could constitute a violation of EU law.

Public Disclosure: Public disclosure is to be understood as making information as to actions or omissions publicly available, under the legally established terms.

Retaliation: Any actions or omissions that are unlawful, or that directly or indirectly entail unfavourable treatment placing the victims thereof at a particular disadvantage compared with another in an occupational or professional context, simply because of their status as whistleblowers or because of the disclosure they made public.

SCOPE

This policy governs the functioning of the Internal Information System of Cintas Adhesivas UBIS, and any person lying within its subjective scope who believes that certain breaches are occurring, may submit a communication in order to report the events and for the relevant measures to be taken.

The Internal Information System protects those reporting offences lying within the objective scope of application of Act 2/2023, in other words acts which constitute violations of EU law, or that are serious or very serious criminal or administrative violations. The exact same protection is also afforded to those reporting other regularities of which they have learned and that are in breach of the Cintas Adhesivas UBIS code of ethics, or infringe the regulations applicable to the company.

The Cintas Adhesivas UBIS whistleblowing channel is designed, established and managed securely, guaranteeing the confidentiality of whistleblowers and of any third party referred to in the communication.

The Whistleblowing Channel is a mechanism made available to all those belonging to the organisation, as well as those that it considers to be its stakeholders, which would include customers, suppliers and other third parties with which it has some type of relationship.

Access to the whistleblowing channel is in any event guaranteed on the part of all whistleblowers subject to Act 2/2023 who work in the private sector and have obtained information as to any violations within an occupational or professional context.

This policy will therefore apply to all stakeholders defined by the organisation within Spanish territory. The scope of application of the standard will in particular extend to the following:

- Employees.

- Employees whose employment relationship with the organisation has ended (ex-employees).
- Sole traders.
- Shareholders, members and those belonging to the governing, senior management or supervisory body of a company, including non-executive members.
- Those working for or under the supervision and management of contractors, subcontractors and suppliers.
- Volunteers, interns, workers on training placements, irrespective of whether or not they receive remuneration.
- Those whose occupational relationship has not yet begun, but who learn of the events in question during the selection or pre-contractual negotiation phase.

The established protective measures likewise apply to individuals who assist the whistleblower, their associates who could suffer retaliation, and legal entities owned by the whistleblower.

Similarly, the protective measures also include workers' representatives providing the whistleblower with advice and support.

OBJECTIVES

This policy is intended to determine the operational principles of the organisation as regards management of the internal information system so as to fulfil the provisions of Act 2/2023 and provide all stakeholders with access to appropriate channels to report any type of violation of which they may learn within the organisation, or any which could affect it.

The System implemented by Cintas Adhesivas UBIS furthermore has an internal whistleblowing management procedure in place, which complies with the principles of confidentiality and integrity of personal data and the information contained, in accordance with the requirements established by Act 2/2023.

INTERNAL INFORMATION SYSTEM SUPERVISOR

The Internal Information System has a supervisor, who is an executive at the organisation, appointed by the Board of Directors of Cintas Adhesivas UBIS, who will perform this role on an independent basis, and must undertake these functions autonomously of all other governing bodies of the organisation, without receiving any instructions of any kind in undertaking the role.

The System Supervisor handles functions derived from implementation of the internal channel, and will be responsible for administering the whistleblowing channel, receiving any communications submitted via this system, assigning the person who is to handle the case, coordinating any investigation that might result from the complaint, proposing the imposition of

the corresponding disciplinary penalties, as well as supervising the proper functioning of the channel, complying at all times with the requirements set forth in Act 2/2023.

PRINCIPLES OF ACTION

Transparency and accessibility

This policy, the essential principles of the whistleblowing channel management procedure, and access to the whistleblowing channel established by Cintas Adhesivas UBIS, will be published on the homepage of its website, in an easily visible location.

Channels

Whistleblowers may choose whichever channel of communication they see fit from among all the channels comprising the organisation's internal information system. Whistleblowers are thus provided with access to the following internal channels:

- Cintas Adhesivas UBIS Whistleblowing Channel, accessible via the following link: https://cybersecurity.telefonica.com/sandasgrc/?organization=CCD057D1-7F62-47CD-BC2E-463B5BC738B0

Aside from these internal channels, users are informed of the existence of other external channels which they may turn to, namely the following:

- Employment Inspectorate.
- Spanish Data Protection Agency (AEPD).
- Independent whistleblower protection authority (A.A.I.), once this has been established.
- Where relevant, the competent regional authorities or bodies, once they have been established.
- Where relevant, the institutions, bodies or entities of the European Union.

For information as to the procedure to be followed, they should contact the Supervisor of the Internal Information System via the following email address: p.ibarbia@ubis.es

Guarantees and protective measures

All those making use of the internal information channel will be entitled to protection, so long as the following circumstances apply:

a) they have reasonable grounds to believe that the information submitted is accurate, at the time when it was communicated or disclosed, even if they do not provide conclusive evidence, and that the information falls within the objective scope of application of the law.

b) the communication or disclosure was conducted in accordance with the legally established requirements.

Any acts which would constitute retaliation are explicitly forbidden, including threats of retaliation and attempted retaliation against those submitting a communication.

To this end, and in order to guarantee the confidentiality of informers, communication may be conducted anonymously via the internal information channel.

The directors of the whistleblowing channel, and its supervisory bodies, undertake to maintain due confidentiality in all actions and in connection with all persons involved.

The identity of the whistleblower may only be communicated to the Court Authorities, the State Prosecution Service or the competent administrative authority within the context of a criminal, disciplinary or punitive investigation.

Respect for the rights of those referred to in the events will be guaranteed at all times. These are essentially the right to be informed of the investigation process being conducted and of the acts of which they are accused, the right to be presumed innocent, the right of defence and the right of personal reputation.

Exemption from the obligation of secrecy

Those communicating information as to actions or omissions comprising a violation, or making a public disclosure, will not be deemed to have breached any restriction on the disclosure of information, and they will not be subject to any type of liability in connection with such public disclosure or communication, provided that they have reasonable grounds to believe that the communication or public disclosure of such information was necessary in order to uncover an action or omission.

This measure will not apply to criminal liabilities.

All the foregoing extends to the communication of information by the workers' representatives, even if they are subject to legal obligations of secrecy or non-disclosure of private information. All the foregoing applies without prejudice to the specific protection regulations applicable under employment legislation.

Whistleblowers will not be subject to any liability regarding the acquisition of or access to the information communicated or publicly disclosed, provided that such acquisition or access does not constitute a criminal offence.

PUBLICITY OF THE INTERNAL INFORMATION SYSTEM

All information concerning the use of the internal information system, and the essential principles of the administrative procedures of the Internal Information System, will be provided

in a clearly and easily accessible manner in a separate and easily identifiable section of the organisation's website.

This Policy, together with all others comprising the documentation system of the Internal Information System, will therefore be made fully available via the website of Cintas Adhesivas UBIS: https://ubis.es/

OBLIGATION OF COMMUNICATION

Anyone who, in their occupational or professional context, detects acts which could constitute serious or very serious criminal or administrative violations, or learns of any conduct in breach of the internal regulations of the organisation, will be obliged to report this via the Internal Information Channel implemented at the organisation, which is accessible via the aforementioned website at this link: https://cybersecurity.telefonica.com/sandasgrc/?organization=CCD057D1-7F62-47CD-BC2E-463B5BC738B0

OPERATION OF THE WHISTLEBLOWING CHANNEL

The Whistleblowing Channel will be accessible via the website of the organisation, where the whistleblower may not only report the events which have occurred in writing, but may also do so by means of a voice recording.

There is one single Whistleblowing Channel for Cintas Adhesivas UBIS, and the events communicated will therefore be associated with this company.

Any action intended to prevent communication being made via the Whistleblowing Channel will be penalised in accordance with the applicable occupational and disciplinary regime.

Once the communication is sent, it will be assigned an identification code which the whistleblower can then use to monitor the procedural status of the alert or consultation, and communicate with the case manager, even anonymously. The whistleblower will likewise receive a receipt in confirmation of the communication sent.

Once the communication is received, it will be decided whether it should be processed or not; in the event that the complaint proves unfounded or insufficient information is provided, it will not be admitted for processing. If it is admitted for processing, there will then be an analysis and confirmation of the acts reported, which may, if necessary, involve a call for other areas of the company to cooperate. The persons involved must enjoy a presumption of innocence throughout the investigation process.

Once the analysis of the acts reported has ended, the conclusions will be passed on to the competent area, which may give rise to the following:

- The act investigated does not constitute a criminal offence or regulatory violation, and will therefore be shelved.
- Existence of the violation is deemed to be proven, in which case it will be passed on to the area affected for any disciplinary consequences decided.

DATA PROTECTION

The internal information systems, external channels, and those receiving public disclosures will not obtain data allowing them to identify the whistleblower, and must have appropriate technical and organisational measures in place to safeguard the identity and guarantee the confidentiality of the data corresponding to those affected, and any third party mentioned in the information provided, in particular the identity of the whistleblower, if they have been identified.

Access to the personal data contained in the System will, within the scope of their responsibilities and functions, be confined solely to:

- The System Supervisor and the person directly administering it.
- The Head of Human Resources, only if it may be appropriate to adopt disciplinary measures against an employee.
- The head of legal services at the organisation, if the adoption of legal measures would be appropriate in connection with the events reported in the communication.
- Any data processors that might be appointed.
- The Data Protection Officer.

Personal data will not be gathered unless they are necessary and relevant for the investigation of the acts, and if they are gathered, they will be erased without undue delay. Nor will special category data be gathered, and if such data are ultimately included by the complainant in the communication submitted via the Internal Information System, they will be immediately erased, without being recorded or subsequently processed.

The purpose of personal data processing will be the administration and handling of the corresponding complaints received via the Whistleblowing Channel. Processing will not be conducted for any other or incompatible purposes.

The processing of data resulting from the application of this policy will be as strictly required to guarantee compliance, and will in any event have the legitimate basis of fulfilment of a legal obligation and/or a task performed in the public interest, ensuring the confidentiality of the whistleblower's data by maintaining their anonymity, without communicating them to third parties, unless identification is a necessary and proportionate obligation imposed by EU or national law within the context of an investigation conducted by the national authorities or in the framework of court proceedings, in which case the data must be communicated to the authorities responsible for the matter.

Where applicable, the data will be communicated to a service provider acting as data processor, which will guarantee the proper administration of the complaints received. The data will likewise

be communicated to the authorities responsible for any criminal or administrative investigation process that may be required.

The data will be stored for as long as essential to decide whether or not an investigation of the acts reported should be initiated. Once these periods have elapsed, they will be erased from the channel, but may remain stored in blocked status if necessary to provide evidence of the functioning of the criminal prevention model or where they could be required by the competent authority to initiate the corresponding investigation of the acts.

In any event, three months after the report is received, if no investigative actions have begun, the information must then be deleted, unless the purpose of storage is to retain evidence of the functioning of the system.

Those complaints that have not been acted upon may only be recorded in anonymous form.

For further information as to the processing of your data and how to exercise your rights, you may consult the Privacy Policy of the whistleblowing channel, available on our website.

APPROVAL

This internal information system policy is subject to the approval of the Board of Directors of Cintas Adhesivas UBIS, who will oversee its application, and will remain in force until any update, revision or repeal is agreed, being reviewed periodically, or whenever a subsequent change would make this necessary.