

Informative summary clause on data protection for the processing of personal data in the management of the internal information system

Controller: ALTADIA GROUP CORPORATE, S.A.U.

Tax ID: A-05348669

Purpose: To manage and process reports submitted regarding possible regulatory infringements and cases of corruption and, where appropriate, to carry out the relevant investigations into the reported facts and adopt the necessary legal or disciplinary measures.

Legal basis: The processing of personal data is based on compliance with legal obligations and on the performance of a task carried out in the public interest (where it is not mandatory to have an internal information system).

Recipients: The System Controller and internal control personnel managing the reporting system, and, where appropriate, courts, tribunals and supervisory bodies, the Public Prosecutor's Office, and other competent authorities or relevant entities.

Rights and additional information: You may exercise your rights of access, rectification, erasure, restriction of processing, data portability, and objection, in accordance with the terms and limitations established by applicable regulations. To exercise these rights or to make any enquiry or complaint related to the processing of your personal data, you may contact us at dpo@altadiagroup.com.

Informative data protection clause for the processing of personal data in the management of the internal information system

Purpose: This informative clause is intended to provide clear and transparent information regarding the processing of personal data in the context of an internal information system (whistleblowing channel) established pursuant to Law 2/2023, of 20 February.

- **Data Controller:** ALTADIA GROUP CORPORATE, S.A.U.
- **Tax ID (CIF):** A05348669
- **Address of the Data Controller:** Ctra. CV-20 km. 2.3 - P.O. Box 194. 12540 Vila-real (Castellón), Spain
- **Data Protection Officer:** dpo@altadiagroup.com

Purpose of processing: The purpose of the processing of personal data collected through the internal information system or whistleblowing channel is to manage and process reports submitted regarding possible regulatory infringements and cases of corruption and, where appropriate, to carry out the relevant investigations into the reported facts and adopt the necessary legal or disciplinary measures.

The processing, investigation, and clarification of reports may involve the determination of liabilities, the implementation of corrective actions, and, where appropriate, the initiation of legal and disciplinary actions before the competent bodies.

Personal data that is collected in error or that is not relevant to the handling of the report will be immediately deleted.

Legal basis for processing: The processing of personal data is based on compliance with legal obligations and on the performance of a task carried out in the public interest (where it is not mandatory to have an internal information system). The applicable mandatory regulation is Law 2/2023, of 20 February, regulating the protection of persons who report regulatory infringements and the fight against corruption, which establishes the obligation for organisations to have whistleblowing channels in order to protect persons who report such infringements. Additionally, the operation of an internal information system may be based on the following regulations:

- Organic Law 3/2018, of 5 December, on Personal Data Protection and the guarantee of digital rights.
- Organic Law 10/1995, of 23 November, of the Criminal Code.
- Organic Law 3/2007, of 22 March, for the effective equality of women and men.

Categories of Personal Data: Within the whistleblowing channel, the following categories of personal data may be processed, as applicable: identification data (name, surname, DNI/NIF, etc.), contact data (postal address, email address, telephone number, etc.), employment data (position, department, etc.), and any other data relevant to the management of the report.

In no case shall personal data that is not necessary for the knowledge and investigation of the acts or omissions referred to in Article 2 of Law 2/2023, of 20 February, regulating the protection of persons who report regulatory infringements and the fight against corruption, be processed. In the event that personal data not related to such acts or omissions is received, it shall be immediately deleted. Likewise, any personal data that may have been disclosed and that relates to conduct not included within the scope of application of said law shall be deleted. This ensures the protection of privacy and the minimisation of the data processed in the context of the whistleblowing system established.

Are there automated decision-making or profiling activities?

No automated decisions will be made regarding your personal data, nor will any profiling be carried out.

Internal Recipients of Personal Data: Personal data collected through the internal information system may be disclosed, where appropriate, to:

- The System Controller and internal control personnel directly managing it: Access to the data contained in these systems is strictly limited to those performing internal control and compliance functions.
- Personnel with human resources management and control functions: Where disciplinary measures against an employee may arise, access shall be granted to personnel with human resources management and control functions
- The head of the organisation's legal services, where the adoption of legal measures in relation to the facts reported in the communication is appropriate.
- Any data processors that may be appointed from time to time.
- The Data Protection Officer.

External Recipients of Personal Data: Personal data collected through the internal information system may be disclosed, where appropriate, to:

- Courts, tribunals, and supervisory bodies: Disclosure shall take place when the verified and substantiated facts reveal indications of an infringement by the relevant party.
- The Public Prosecutor's Office, where there are indications that the facts may constitute a criminal offence. In particular, if the facts affect the financial interests of the European Union, the case shall be referred to the European Public Prosecutor's Office.
- Other competent authorities or relevant entities, in compliance with legal obligations.

International Data Transfers: International data transfers may take place exclusively under the terms set out in Altadia's Data Protection Policy.

The platform used for the management of the internal information system belongs to the company OneTrust, which operates globally and has its headquarters in the United States. Therefore, the personal information provided in the internal information system may be transferred to and accessed from anywhere in the world. To ensure the adequacy of international transfers, OneTrust relies on:

Adequacy decisions adopted by the European Commission ("EC"), pursuant to Article 45 of Regulation (EU) 2016/679 (GDPR): for more information and access to the full list of countries currently deemed adequate, please visit https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en?prefLang=es

The Standard Contractual Clauses of the European Commission ("SCCs") and the International Data Transfer Addendum ("IDTA") of the UK Information Commissioner's Office, as applicable, supplemented by additional security measures as recommended by the European Data Protection Board (if you are an OneTrust customer, to access our standard customer SCCs, please visit: <https://www.onetrust.com/legal-sccs>

These contractual clauses establish obligations and safeguards to protect personal data during transfer and subsequent processing. In addition, OneTrust implements appropriate technical and organisational measures to ensure the security and confidentiality of personal information stored in its internal information system. These measures include data encryption, restricted access to information only for authorised and trained personnel, and the implementation of robust security and privacy policies.

Personal Data Retention Periods: Data undergoing processing may be stored in the information system only for the time strictly necessary to decide whether to initiate an investigation into the reported facts.

Accordingly, personal data relating to reports that are not admitted for processing and therefore will not be subject to investigation shall be deleted immediately¹, unless the data controller considers that it is under a legal obligation to retain them, for example where the lack of truthfulness of the information

¹ In this case, they shall be immediately deleted, without giving rise to their blocking or retention.

provided may constitute a criminal offence, in which case the information shall be retained for as long as the relevant judicial proceedings are ongoing.

With regard to reports admitted for processing that conclude without the reported facts being substantiated and are therefore closed, the personal data obtained in the course of the investigation shall be erased² when they are no longer necessary and relevant, and in any case within a maximum period of three (3) months from the closure of the case file.

Communications that have not been processed may only be recorded in anonymised form, and the blocking obligation provided for in Article 32 of Organic Law 3/2018, of 5 December, shall not apply.

Finally, personal data collected during investigations of reports that result in sanctions and/or disciplinary actions shall be retained, duly blocked, for the limitation period applicable to the offences, as from the closure of the case file. However, in no case shall data be retained for more than ten years.

Protection of the Identity of the Whistleblower and Affected Persons: The data controller undertakes to implement appropriate technical and organisational measures to preserve the identity and ensure the confidentiality of the data relating to affected persons, as well as any third party mentioned in the information provided. In particular, it shall ensure that data relating to the identity of the whistleblower is not disclosed to the reported person during the investigation. These measures shall ensure that the internal information system does not collect data that could reveal the identity of the whistleblower or third parties mentioned, thereby protecting confidentiality and anonymity in the processing of personal data, while respecting fundamental rights at all times.

These measures shall apply without prejudice to any actions that may be taken by the competent judicial authorities.

As an exception, the identity of the whistleblower may only be disclosed to the judicial authority, the Public Prosecutor's Office, or the competent administrative authority in the context of a criminal, disciplinary, or sanctioning investigation. Such disclosure shall only take place in the cases and under the procedures established by applicable law. It shall be ensured that such disclosure of the whistleblower's identity is carried out lawfully and with due respect for the rights and protection of all parties involved.

Data Subject Rights: Data subjects may exercise their rights of access, rectification, erasure, restriction of processing, data portability, and objection, in accordance with the terms and limitations established by applicable regulations. To exercise these rights or to make any enquiry or complaint related to the processing of their personal data, they may contact the Data Controller using the contact details provided above.

Where the person mentioned in the facts reported in the complaint exercises their right to object, it shall be presumed, unless proven otherwise, that there are compelling legitimate grounds justifying the processing of their personal data.

Supervisory Authority: Data subjects have the right to lodge a complaint with the competent data protection supervisory authority if they consider that the processing of their personal data does not comply with applicable regulations.

Updates to the Information Clause: This information clause may be updated at any time in accordance with changes in legislation or any changes in the processing of personal data. Data subjects are advised to review this clause periodically to stay informed about updates.

Date of update: 28 May 2026

² In accordance with the Organic Law on the Protection of Personal Data, erasure shall result in the blocking of the data, which shall be retained solely at the disposal of Public Administrations, courts, and tribunals, for the purpose of addressing any potential liabilities arising from the processing, during the limitation period applicable to such liabilities. Once this period has elapsed, the data shall be deleted.