Internal Reporting System Policy

Change control					
Revision	**Date**	**Section affected**	**Effected**	**Reviewed**	**Approved**

Contents

1. PURPOSE OF THE INTERNAL REPORTING SYSTEM POLICY

October 23, 2019, saw the approval of Directive (EU) 2019/1937, of the European Parliament and of the Council, on the protection of persons who report breaches of Union law (hereinafter also referred to as the "**Whistleblowing Directive**"), the purpose of which is to underpin the application of the Law and policies of the Union in specific spheres, by establishing certain minimum common standards to provide a high level of protection for those reporting infringements of EU Law.

On February 20, 2023, Spain passed its Act 2/2023, of February 20, governing the protection of persons who report regulatory breaches, and anti-corruption, in order to transpose the Whistleblowing Directive (hereinafter, the "**Whistleblower Protection Act**"), which took effect on March 13, 2023.

ALUDIUM TRANSFORMACIÓN DE PRODUCTOS S.L. (hereinafter, ALUDIUM) has, within the context of its Crime Prevention Program, and in accordance with the provisions of the Whistleblower Protection Act, implemented an internal reporting system allowing any member of ALUDIUM (including stakeholders or owner companies) or any third party from outside the organization, in particular suppliers and clients, if they learn of or suspect a regulatory breach (either of the legislation or implementing regulations, or otherwise internal corporate standards) committed by a member of ALUDIUM or by third parties in contact with the organization within the context of their occupational activities, to report the matter to ALUDIUM, either anonymously or by identifying themselves.

ALUDIUM espouses all the principles set forth in the Whistleblowing Directive and the Whistleblower Protection Act, and in order to emphasize this commitment, approves this Internal Reporting System Policy, the provisions of which supplement those set forth in the

Procedure for Administration, Investigation and Response to communications received via the internal reporting system (AIR Procedure).

The purpose of this policy is to establish the general principles of the ALUDIUM internal reporting system, the rights enjoyed by whistleblowers, and the procedure governing the manner in which they may inform the System Supervisor of any events concerning the matters referred to in the following subsection regarding the material scope of application.

Likewise, in order to govern the use of the internal reporting system and the procedure for the investigation and resolution of the communications received, ALUDIUM has approved and implemented the *Procedure for Administration, Investigation and Response to communications received via the internal reporting system*, the contents of which likewise comply with the demands of the Whistleblowing Directive and the Whistleblower Protection Act.

2. MATERIAL SCOPE OF APPLICATION

This Policy protects natural persons using any of the channels established in the Policy below to report:

1. Actions or omissions that could constitute **infringements of European Union Law** wherever they would:

    a. Lie within the scope of application of the European Union acts listed in the Annex 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, irrespective of how they would be categorized within the domestic legal system.

    b. Affect the financial interests of the European Union, as provided in Article 325 of the Treaty on the Functioning of the European Union (TFEU).

c. Affect the internal market, as provided in Article 26(2) of the TFEU, including breaches of European Union regulations with regards to competition and State aid, as well as breaches concerning the internal market in connection with acts infringing the standards governing corporation tax, or practices for the purpose of obtaining a tax advantage that would undermine the object or purpose of the legislation applicable to corporation tax.

2. Actions or omissions which could constitute a **criminal offence or serious or very serious administrative infringement**. This will in all cases be understood to include all criminal offences or serious or very serious administrative violations that would constitute a loss to the Tax Office and Social Security.

In addition, the internal reporting system may likewise be used to report issues concerning the following matters, although in these cases neither the whistleblower nor the communication will enjoy the protection granted in the Whistleblower Protection Act and in this Policy:

3. Actions or omissions that could constitute a **minor criminal offence or administrative violation.**

4. Actions or omissions that could constitute a **breach of the Code of Conduct or the internal regulations of the company**, including the values, operational guidelines or behavioral standards of all employees, including compliance with the legislation in force.

5. Any contingency that could represent a **risk to the reputation** of ALUDIUM.

3. PERSONAL SCOPE OF APPLICATION

This Policy extends not only to ALUDIUM employees, but also to such other collaborators as volunteers, internships, workers on training periods, irrespective of whether or not they receive remuneration, candidates in a selection process, workers whose occupational or commercial relationship is ended and workers' representatives, as well as anyone working for or under the supervision and management of contractors, subcontractors and suppliers, in addition to stakeholders, members and persons belonging to the Board of Directors and the governing or supervisory bodies of ALUDIUM, who report a matter via the ALUDIUM internal reporting system with reference to any of the matters indicated in items 1 and 2 of subsection 2 of this Policy ("Material Scope of Application").

The protective measures established in this Policy will likewise, where relevant, apply to: (i) any natural persons who, within the context of the organization where the whistleblower provides their services, assist them in the process; (ii) any natural persons connected with the whistleblower who could suffer retaliation, such as the colleagues or relatives of the whistleblower; and (iii) any legal entities for which they work or with which they have any other type of relationship in a professional context, or any in which they hold a significant stake.

4. FUNCTION OF THE SYSTEM SUPERVISOR

The Governing Body has opted to appoint a collegiate body to perform the functions assigned to the ALUDIUM System Supervisor, as established in the Minutes of November 13, 2023.

In the event that the person affected by the communication is the System Supervisor themselves, and for the purposes provided in Article 8.5 of the Act, in order to avoid possible conflicts of interest, the whistleblower may address their communication for the attention of any of the other members of the collegiate body not involved in the communication, who will then on a provisional basis, and purely for the purposes of handling that communication, perform the functions of System Supervisor. The same provisions will apply if the System

Supervisor is subject to some incompatibility preventing them from dealing with a specific matter. They will then be excluded from all processes concerning the matter in question

5. INTERNAL REPORTING CHANNEL

ALUDIUM has set up an internal reporting channel via two separate methods:

1. By means of the **platform** established for whistleblowers on the Company website (on the home page, in a separate and easily identifiable section): https://aludium.com/en/aludium-information-channel/

2. By **directly** informing the System Supervisor, verbally or in writing.

   - If communication is given verbally, this must be documented either by means of a recording of the conversation in a secure, lasting and accessible format (having first advised the whistleblower that the communication will be recorded, and informing them of the processing of the data in accordance with the provisions of Regulation (EU) 2016/679, of the European Parliament and of the Council, of 27 April 2016), or otherwise by means of a complete and precise transcript of the conversation, drawn up by the staff responsible for handling the matter. The whistleblower will likewise be given the opportunity to check, rectify and sign in acceptance of the transcript of the conversation.

   - If communication is given in writing, it should be sent for the attention of the System Supervisor at the ALUDIUM offices located at the address: Amorebieta, Barrio Ibarguren s/n, 48340, Vizcaya, Spain. The reference "Confidential" should be included on the envelope.

3. In addition, the whistleblower may request an **in-person meeting** to present the communication. This must be held within a maximum of seven days of the request. The meeting must be duly documented, either by recording or transcript.

Aside from the above, any formal communication by a court or public authority will be considered valid notification of a breach. In addition, the internal reporting channel **is open to third parties** from outside ALUDIUM, in particular suppliers, distributors and other commercial partners of the company who might learn or have reasoned suspicions of the commission of a breach which could affect the company.

Communications may likewise be submitted either by an **identified** individual or **anonymously**.

Any communications made must, as far as possible, contain the following aspects:

i. **Full name** of the person to whom the acts and/or conduct reported are attributed.

ii. **Date** of the events and **all information** available about them.

iii. **Any possible documents** or other means of evidence available in accreditation of the reality of the events and/or conduct reported.

Whistleblowers will enjoy the protection established in this Policy in using the internal reporting channels available to report any breach committed by members of ALUDIUM, or by third parties that do not belong to the organization but have relations with ALUDIUM within the context of their professional tasks, provided that they involve the breach as referred to in items 1 and 2 of subsection 2 of this Policy ("Material scope of application"), in other words actions or omissions that constitute breaches of European Union Law or criminal or serious or very serious administrative violations.

Likewise, any member of ALUDIUM or an outside third party may use the internal reporting channel to report any actions or omissions that could constitute a breach of the internal regulations of the company,

but do not constitute a breach of European Union Law or a criminal or serious or very serious administrative violation, including the principles and values espoused as the behavioral guide for all employees. They may likewise submit any consultation connected with the scope, fulfilment and interpretation of the regulations applicable to ALUDIUM. In such cases, neither the whistleblower nor the communication will enjoy the protection granted in this Policy, although their confidentiality will in all cases be maintained.

The *AIR Procedure* establishes the investigation process that will apply once a regulatory breach has been reported, in a manner consistent with the guidelines of the Whistleblowing Directive and the Whistleblower Protection Act.

6. EXTERNAL REPORTING CHANNEL AND PUBLIC DISCLOSURE

Although the internal reporting channel is the preferred means of reporting actions and omissions that constitute a breach of European Union laws, or a criminal or serious or very serious administrative violation, any individual may directly contact the external reporting channel created by the Spanish Independent Whistleblower Protection Authority ('A.I.I.'), and the competent regional authority.

At the regional level, in addition to the creation of this system (which nonetheless does not replace the A.A.I. channel), the external complaints inbox of the different antifraud offices may be used, and will in any event be used to report irregularities in breach of public integrity or any which could potentially constitute fraud or corruption at the regional level (including all manner of irregularities reported to protect all forms of public funds).

Both the whistleblower and the communications conducted via the external channel will enjoy the protection granted in this Policy, provided that they fulfil the requirements explicitly established in subsection 7 below.

Likewise, public disclosure or the public release of information as to actions or omissions established within the scope of application

of the Whistleblower Protection Act (in other words, actions and omissions that constitute a breach of European Union laws, or a criminal or serious or very serious administrative violation) will likewise entail whistleblower protection, provided that communication was first performed via internal or external channels, or directly via external channels, if appropriate measures have not been taken in this regard by the established deadline, and wherever the requirements established in the following subsection are furthermore fulfilled.

7. PROTECTION OF WHISTLEBLOWERS

All those communicating or uncovering infringements at ALUDIUM **will enjoy all rights of protection** established in this Policy and in the AIR Procedure, provided that:

1. They have reasonable grounds to believe that the information they communicate to ALUDIUM is accurate at the time of communication, and that the information in question lies within the material scope of application of the Whistleblower Protection Act. In other words, actions or omissions that could constitute breaches of European Union Law and actions or omissions that could constitute a criminal or serious or very serious administrative violation.

2. They admitted the communication or disclosure in accordance with the requirements established to this end by ALUDIUM and the Whistleblower Protection Act.

Those communicating or publicly disclosing information about actions or omissions referred to in the Whistleblower Protection Act on an anonymous basis, but who have subsequently been identified and fulfil the conditions established in this subsection, will be entitled to the protection set forth in this Policy.

Individuals informing the institutions, bodies or organizations belonging to the European Union of any violations that would lie within the scope of application of Directive (EU) 2019/1937, of the European Parliament and of the Council,

of 23 October 2019, will be entitled to protection in accordance with the provisions of the Whistleblower Protection Act and this Policy.

Meanwhile, the protection established in this Policy and in the AIR Protocol **will not apply** to those communicating or disclosing:

3. Information contained in communications that have been rejected for any of the following reasons:

    a. If the events recounted lack all credibility.

    b. If the events recounted do not constitute a legal violation lying within the scope of application of the Whistleblower Protection Act, in other words, actions or omissions that could constitute breaches of European Union Law and actions or omissions that could constitute a criminal or serious or very serious administrative violation.

    c. If the communication clearly lacks any basis, or in the judgment of the System Supervisor, there is reasonable evidence that it was obtained by committing a crime. In the latter case, as well as rejecting the communication, the list of events ascertained and believed to constitute an offence will be referred to the Public Prosecution Service.

    d. If the communication does not contain new and significant information about violations in comparison with a prior communication concerning which the corresponding procedures have been concluded, unless new factual or legal circumstances arise that would justify a different continuation of the case. The System Supervisor will in such cases give reasoned notification of the decision.

4. Information connected with claims concerning interpersonal disputes or those affecting solely the whistleblower and the persons to whom the communication or disclosure refers.

5. Information that is already fully available to the public or would constitute mere rumor.

6. Information referring to actions or omissions that do not lie within the material scope of this Policy.

The whistleblower will be informed of the rejection of the communication submitted via the appropriate established channels within five business days, unless the communication was given anonymously, or the whistleblower has waived the right to receive communications regarding the procedure.

8. NO RETALIATION

ALUDIUM will adopt the necessary measures to prohibit any act constituting retaliation, including threatened and attempted retaliation, against those presenting a communication with reference to actions or omissions that do not lie within the material scope of application of the Whistleblower Protection Act (in other words, actions or omissions that could constitute breaches of European Union Law and actions or omissions that could constitute a criminal or serious or very serious administrative violation).

Retaliation should be understood as any actions or omissions that are unlawful, or that directly or indirectly entail unfavorable 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.

For the purposes provided in this Policy, and purely by way of example, retaliation would be understood to include any of the following actions:

1. Suspension of employment contract, dismissal or termination of occupational or statutory relationship, including failure to renew or premature

termination of a temporary employment contract once the trial period has ended.

2. Premature termination or cancellation of contracts for goods or services.

3. Imposition of any disciplinary measure, demotion or denial of promotion, and any other substantial modification of employment conditions.

4. Failure to convert a temporary employment contract into a permanent contract, if the worker had legitimate expectations that they would be offered permanent employment.

5. Harmful acts, including those involving reputation, economic loss, coercion, intimidation, harassment or ostracism.

6. Negative appraisal or references with regard to occupational or professional performance.

7. Inclusion on blacklists or distribution of information within a particular sectoral scope, which would hamper or prevent access to employment or works or service contracts.

8. Denial or cancellation of leave or leave of absence.

9. Denial of training.

10. Discrimination or unfavorable or unfair treatment.

The measures set out under items 1 to 4 above will not be considered as retaliation if they are performed within the regular exercise of managerial powers in accordance with employment legislation or the corresponding legislation governing the statute of public employees, because of circumstances, acts or infringements that have been proven, and are unconnected with the submission of the communication.

It is likewise here stated that any person whose rights are infringed as a result of their communication or disclosure after the period of two years has expired may apply to the competent authority for protection. On exceptional and justified grounds, the period of protection may be extended, an audience having first been granted to any individuals or bodies that could be affected (any refusal of such an extension to the protection period must be reasoned).

It is likewise here stated that any acts serving to prevent or hamper the submission of communications and disclosures, and any constituting retaliation or causing discrimination after the submission thereof will, in accordance with the Whistleblower Protection Act, be deemed fully null and void, and will where applicable give rise to disciplinary corrective measures or liability, which may include the corresponding compensation for damages payable to the injured party.

Whistleblowers will furthermore, where applicable, be granted access to the following support measures provided by the Independent Whistleblower Protection Authority and/or the competent regional body:

1. Full and independent information and advice, easily accessible to the public and free of charge, as to the available procedures and resources, protection against retaliation and the rights of the person affected.

2. Effective assistance by the competent authorities in dealing with any relevant authority involved in their protection against retaliation, including certification that they are entitled to protection under the terms of the Whistleblower Protection Act.

3. Legal assistance in criminal proceedings and civil proceedings of a cross-border nature, in accordance with EU regulations.

4. Financial and psychological support, on an exceptional basis, if so decided by the Independent Whistleblower Protection Authority and/or the competent

regional body, following an appraisal of the circumstances resulting from submission of the communication.

All the above furthermore applies irrespective of any assistance to which the whistleblower might be entitled under the terms of Act 1/1996, of January 10, on free public assistance, for representation and defense in court proceedings derived from the submission of the communication or public disclosure.

9. MEASURES TO PROTECT AGAINST RETALIATION

ALUDIUM will adopt the necessary measures to ensure that whistleblowers are protected against retaliation. The main protection measures established both in the Whistleblowing Directive and in the Whistleblower Protection Act are set out below for the information of all potential whistleblowers. ALUDIUM adheres to these provisions and undertakes to facilitate their effective application:

1. Those communicating information as to the actions or omissions set forth in items 1 and 2 of subsection 2 of this Policy, or making a public disclosure in accordance with the Whistleblower Protection Act, will not be deemed to have breached any information non-disclosure provision, nor will they be subject to any liability in connection with such communication or public disclosure, provided that they had reasonable grounds to believe that the communication or public disclosure of the information was necessary in order to uncover an action or omission under the terms of this Policy and the Whistleblower Protection Act, all the foregoing without prejudice to the provisions of Article 2.3 of the Whistleblower Protection Act[1]. This measure will not apply to criminal liabilities.

[1] Article 2.3 of the Whistleblower Protection Act: *"The protection established in this Act for workers reporting violations of Employment Law with regard to health and safety at work, is understood to apply without prejudice to the provisions of the specific regulations".*

The terms of the above paragraph extend to the communication of information by the representatives of the workers, even if they are subject to legal obligations of secrecy or non-disclosure of confidential information. All the foregoing applies without prejudice to the specific protection regulations applicable under employment legislation.

2. 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.

3. Any other possible liability that might result for whistleblowers from acts or omissions not connected with the communication or public disclosure or that would not be necessary to uncover a violation under the terms of the Whistleblower Protection Act, will be subject to liability under the terms of the applicable regulations.

4. In proceedings conducted before a court or other authority in connection with the damages suffered by whistleblowers, once the whistleblower has provided reasonable proof that they communicated the information or made the public disclosure in accordance with the Whistleblower Protection Act and suffered harm, this harm will be presumed to have occurred as retaliation for submitting the information or making public disclosure. In such cases the person who adopted the harmful measure will be responsible for proving that the measure was based on duly justified grounds not connected with the communication or public disclosure.

5. In court proceedings, including those involving defamation, breach of copyright, breach of secrecy, violation of data protection standards, disclosure of trade secrets, or requests for compensation based on employment or statutory law, those submitting a communication in accordance with this Policy and the Whistleblower Protection Act will not be subject to any liability as a consequence of communications or public

disclosures protected by the Act. These individuals will, within the context of the aforementioned court proceedings, be entitled to present as exonerating evidence the fact that they communicated or made a public disclosure, provided that they had reasonable grounds to believe that the communication or public disclosure was necessary in order to reveal an infringement under the terms of the Whistleblower Protection Act.

10. PROTECTIVE MEASURES FOR PERSONS REFERRED TO IN THE COMMUNICATION

ALUDIUM will guarantee that those persons referred to in the communication are granted a hearing within the context of the internal corporate investigation, enjoy the right to be presumed innocent, the right to defense and the right of access to the case record on the terms governed by the Whistleblower Protection Act.

The identity of the person referred to in the communication of a violation will likewise be protected and treated in a confidential manner, as will the events communicated, in the same manner as for the identity of the whistleblower themselves, and at all times in accordance with any limits and exceptions that may need to be determined so as to guarantee the proper progress of the investigation, or any possible communication to the competent authorities.

11. PENALTIES

ALUDIUM will, in accordance with the corresponding employment regulations and legislation, essentially the Workers' Statute and the applicable collective bargaining agreements, establish effective, proportionate and deterrent penalties applicable to any members of ALUDIUM who:

1. Prevent or attempt to prevent communications being submitted or frustrate or attempt to frustrate the pursuit thereof.

2. Adopt retaliatory measures against whistleblowers.

3. Promote abusive proceedings against whistleblowers.

4. Breach their duty to maintain confidentiality with regard to the identity of the whistleblower or the persons involved in the communication, and the duty of secrecy regarding any information connected with the communication submitted.

5. Communicate or publicly disclose information being aware that it is false.

12. NON-DISCLOSURE

Without prejudice to the provisions of other subsections of this Policy, ALUDIUM guarantees the confidentiality of the identity of the whistleblower and of any third party mentioned in the communication, of the actions taken in the administration and processing thereof, as well as the protection of data, preventing access by unauthorized personnel.

In accordance with the above, access to data concerning the complaint is restricted to members specifically authorized by ALUDIUM to receive, pursue or rule on the communications received, and those third parties (such as a court authority, the State Prosecution Service or the competent administrative authority) where this would constitute a necessary and proportionate obligation imposed by the applicable regulations, within the context of an investigation conducted by the national authorities or within the context of court proceedings, and in particular where the disclosure is intended to safeguard the right of defense of the person affected.

In any event, except in the established cases, ALUDIUM guarantees that no authorized person will learn the identity of the whistleblower nor any other information that could directly or indirectly help to deduce their identity. ALUDIUM specifically guarantees that the person referred to in the events recounted will not under any circumstances be informed of the identity of the whistleblower nor, as applicable, the person who made the public disclosure.

ALUDIUM likewise guarantees the confidentiality of the data and facts submitted if the communication is sent via complaint channels other than those established, or to members of staff who are not responsible for the processing thereof. To this end, ALUDIUM has provided its staff with adequate training in this regard and has warned them of violations of the duty of confidentiality, and likewise the obligation established on the recipient of the communication immediately to refer it to the system supervisor.

In fulfilment of all the above, ALUDIUM has implemented technical and organizational measures within the internal channel to preserve the identity and guarantee the confidentiality of the data corresponding to the persons affected, and any third party mentioned in the information provided, in particular the identity of the whistleblower, if that person was identified.

With regard to the persons affected by the complaint, ALUDIUM guarantees that during the investigation conducted, the persons affected by the communication will enjoy the same right of protection as established for whistleblowers, concealing their identity and guaranteeing the confidentiality of events and data in the proceedings.

Meanwhile, those receiving public disclosures are subject to the same obligations as described above and will under no circumstances obtain data that would serve to identify the whistleblower and must have appropriate technical and organizational measures in place.

Disclosures made under the terms of this subsection will be subject to the safeguards established in the applicable regulations, and the whistleblower will in particular be informed before their identity is disclosed, unless such information could compromise the investigation or the court proceedings. Whenever the competent authority communicates with the whistleblower, it will write to them explaining the reasons for the disclosure of the confidential data in question.

ALUDIUM will in all cases ensure that the competent authorities receiving information as to infringements that include trade secrets do not use or disclose them for purposes that go beyond the necessary measures in order properly to pursue the proceedings.

13. PROCESSING OF PERSONAL DATA

The personal data processed under the terms of this Policy and the AIR Procedure, including the exchange or transfer of personal data with the competent authorities, will be processed by ALUDIUM, at the address Amorebieta, Barrio Ibarguren s/n, 48340, Vizcaya, Spain, in its capacity as data controller, as provided in personal data protection regulations.

The Data Protection Officer may be contacted via the following email address: info@aludium.com.

The personal data provided via the internal system will be processed for the purpose of receiving and analyzing the actions or omissions reported, and where applicable, deciding as to whether or not an investigation should begin of the acts reported. In addition, certain information may be processed to provide evidence of the functioning of the system. In this last case, ALUDIUM guarantees that the information stored as evidence will be anonymized.

If information which is not necessary to process and investigate the actions or omissions referred to in subsection 2 of the Policy is received, the data controller will proceed immediately to erase it. Likewise, all personal data that may have been communicated and that refer to conduct not lying within the scope of application of the Whistleblower Protection Act and of this Policy, or any information or part thereof proven to be inaccurate, will be erased, unless such lack of accuracy could constitute a criminal offence.

The data controller will process the personal data provided by the whistleblower in fulfilment of a legal obligation, specifically to comply with the Whistleblower Protection Act. Furthermore, in the case of verbal communications, the consent of the whistleblower will be required in order to document the communication in question, including those conducted by means of an in-person meeting, by telephone or voice messaging. Meanwhile, the processing of specially protected data, if necessary for the purpose pursued, may be conducted by the controller for reasons of essential public interest, and may be performed in accordance with the provisions of Article 9.2(g) of Regulation (EU) 2016/679.

The personal data gathered via the internal channel will be stored in accordance with the provisions of the applicable legislation. Such data will specifically be stored only for as long as essential to decide as to whether or not an investigation should be conducted of the events reported and must under no circumstances last more than three months from receipt of the communication, other than for the purpose of providing evidence of the functioning of the system. Those communications that have not been acted upon may only be recorded in anonymous form. Nonetheless, should it prove necessary to process the personal data for longer in order to continue the investigation, or where applicable because it is deemed necessary to initiate the relevant legal action, the data will be stored in a different environment from the internal channel, for as long as necessary in order to conclude the investigation, or for ALUDIUM to bring the corresponding action.

To fulfil the purposes described above, the data controller may provide access to personal data on the part of:

- Third-party companies providing services, such as consultants and external partners providing administrative support, or where applicable, the investigation of the complaints received via the internal channel.
- Relevant areas or departments with a view to processing the complaint and, where applicable, for the investigation and possible measures to be adopted with regard to the conduct communicated, wherever necessary.

- Likewise, personal data may be transferred to Judges and Courts, the State Prosecution Service, and to the competent public authorities, as a consequence of any investigation that may be launched.

In connection with the above, ALUDIUM informs the data subjects that it does not perform international transfers of the personal data provided.

The data subject is furthermore informed that under the conditions established in the applicable regulations, they may exercise the rights recognized in the data protection regulations by writing to the data controller by conventional mail at its registered office, or by sending an email to the following address: info@aludium.com.

ALUDIUM nonetheless states that if the person to whom the events recounted in the communication refer, or to whom the public disclosure refers, were to exercise the right of objection, it will be presumed, absent evidence to the contrary, that there are overriding legitimate grounds for the processing of their personal data.

Without prejudice to the rights enjoyed by the whistleblower, in accordance with data protection regulations, if the communication was given verbally, the data subject may confirm, rectify and revoke consent via the following address: info@aludium.com.

The data subjects are likewise entitled to file a grievance with the Spanish Data Protection Agency (www.aepd.es).

The System Supervisor will periodically review the proper functioning of the internal reporting system and the provisions of this Policy.

14. REGISTER OF COMMUNICATIONS

ALUDIUM will maintain a register of all communications and consultations it may receive via the internal reporting system, compiled in what is known as the "register book", complying at all times with the established confidentiality requirements, and for as long as strictly necessary and proportionate in order to fulfil the legal and regulatory requirements issued by the European Union.

If the communication was performed verbally, ALUDIUM reserves the right to document the verbal complaint in one of the following manners:

1. By recording the conversation in a lasting and accessible format.

2. Through a complete and precise transcript of the conversation drawn up by the System Supervisor.

The whistleblower is in any event entitled to sign in confirmation, rectification and acceptance of the transcript made. These rights may be exercised at any time via the platform set up for whistleblowers on the Company website: https://aludium.com/en/aludium-information-channel/

If the whistleblower has requested a personal interview with the System Supervisor to make the communication, ALUDIUM will, subject to the consent of the whistleblower, ensure that full and precise records of the meeting held are kept in a lasting and accessible format.