

Allen Overy Shearman Sterling

Serrano 73,
28006 Madrid, España
+34 91 782 98 00

riskcompliance_spain@aoshearman.com

INTERNAL INFORMATION SYSTEM POLICY (A&O SHEARMAN MADRID)

1. INTRODUCTION

- 1.1 The global Whistleblowing and Speaking Up (Crime and Malpractice) Policy of A&O Shearman Grouping¹ (hereinafter, “A&O Shearman Global Whistleblowing Policy”) contains the set of guiding principles, guarantees, and operating rules of the channels enabled by the Firm to communicate possible breaches of legal, professional, and ethical regulations (both external and internal) that apply to us both collectively as a global law firm and individually to each of the professionals who make it up, in the various countries and jurisdictions in which we are present.
- 1.2 A&O Shearman Grouping carries out its legal and tax advisory activities in Spain through its Madrid Office, comprised of its Partners, other legal professionals (including students and trainees), and the rest of the support and operations staff (all of them, indistinctly, professionals of “A&O Shearman Madrid”)².
- 1.3 Act 2/2023, of February 20, regulating the protection of persons who report legal breaches and the fight against corruption (“Act 2/2023” or “Whistleblower Protection Act”, interchangeably, hereinafter), transposed into Spanish Law the Directive (EU) 2019/1937 of the European Parliament and of the Council, of October 23, 2019, on the protection of persons who report breaches of Union law (hereinafter, “Directive (EU) 2019/1937”). As indicated in its article 1, the Whistleblower Protection Act aims to (i) provide adequate protection against retaliation that may be suffered by natural persons who report, through any of the procedures described in said Act, any of the actions or omissions included within its material scope of application, and (ii) strengthen the culture of reporting, the integrity infrastructures of organizations, and the promotion of the culture of reporting or communication as a mechanism to prevent and detect threats to the public interest.
- 1.4 Based on the guiding principles, guarantees, and operating rules of the Whistleblowing and Speaking-Up System contained in the aforementioned Global Policy of A&O Shearman Grouping and considering the specific requirements that derive for A&O Shearman Madrid from the application of the aforementioned Whistleblower Protection Act and its implementing regulations³, this local Policy includes the set of principles, guarantees, protection mechanisms, and procedural rules that govern

¹ A&O Shearman Group means Allen Overy Shearman Sterling LLP, its Subsidiaries, and the other companies, businesses, and entities that are authorized to operate using a name that includes "Allen Overy Shearman Sterling" or "A&O Shearman," and a member of the A&O Shearman Group has the corresponding meaning. Allen Overy Shearman Sterling LLP is a limited liability partnership incorporated in England and Wales with registration number OC 306763 and registered office at One Bishops Square, London E1 6AD, United Kingdom.

² Specifically, under the name Allen Overy Shearman Sterling, an entity in a revenue attribution regime with a presence in Spanish territory, in accordance with the provisions of Article 38 of Royal Legislative Decree 5/2024, of March 5, which approves the revised text of the Non-Resident Income Tax Act, with an address at Calle Serrano 73, 28006, Madrid (Spain) and Tax number N00675003C.

³ Namely: Royal Decree 1101/2024 of 29 October approving the Statute of the Independent Authority for Whistleblower Protection (A.A.I.); Order PJC/908/2025 of 8 August determining the date on which the Independent Authority for Whistleblower Protection (A.A.I.) shall commence operations; as well as any Circulars and Recommendations that the Independent Authority for Whistleblower Protection (A.A.I.) may issue.

communications received through the Whistleblowing and Speaking-Up System of A&O Shearman Grouping when the Whistleblower Protection Act applies to the reporting person (and/or other persons related to the communication in question as provided in this Policy).

- 1.5 This local Policy is issued in both Spanish and English. In the event of any conflict, inconsistency or ambiguity between the two versions, the Spanish version shall prevail to the extent of such inconsistency. This local Policy shall be governed by, and construed in accordance with, the laws of Spain.

2. OBJECTIVE

- 2.1 This Policy aims to establish, in accordance with the provisions of the Global Whistleblowing and Speaking-Up (Crime and Malpractice) Policy and the legal requirements derived from Act 2/2023 and its implementing regulations, the general principles and procedural rules that govern the operation of the Whistleblowing and Speaking-Up System of A&O Shearman Grouping, as the preferred channel for receiving communications related to breaches, when the Whistleblower Protection Act applies, the identification of the Responsible for said System and their obligations and attributions, as well as the guarantees and protection measures for Whistleblowers provided in Act 2/2023 when the conditions and requirements provided in said Whistleblower Protection Act are met.
- 2.2 Regarding those communications of infringements or breaches that refer to matters that, according to Spanish legal regulations, must be processed following specific internal policies, procedures, or protocols (for example, the *Protocol for action against workplace harassment, sexual harassment, harassment based on sex, or violence against LGBTQ people and sexual violence of the Madrid office of A&O Shearman*), the provisions of said specific internal policies, procedures, or protocols will preferably apply, with this local Policy being supplementary.

3. SCOPE OF APPLICATION

- 3.1 This Policy will apply to all A&O Shearman Madrid Personnel who report possible infringements or breaches (hereinafter, whistleblower/s or informant/s), through the channels provided therein, on any of the following matters:
- (a) Actions or omissions that may constitute violations of European Union law, provided they fall within the scope of the acts of the European Union listed in the annex to Directive (EU) 2019/1937, provided they affect the financial interests of the European Union and have an impact on the internal market (including competition violations).
 - (b) Actions or omissions that may constitute a serious or very serious criminal or administrative offense under Spanish law⁴.
 - (c) Actions or omissions that may constitute a breach of the internal policies (global or local) of A&O Shearman Grouping by a professional of the Madrid Office in the performance of their duties or professional obligations.

⁴ In accordance with the provisions of Article 26 bis of Act 10/2010, of April 28, on the prevention of money laundering and terrorist financing ("Act 10/2010"), communications of possible non-compliance with this Act (and its regulatory development), as well as the internal policies on this matter of A&O Shearman Grouping, are subject to the provisions of this Policy, in addition to what is already provided in relation to the internal procedures for communicating potential non-compliance in the field of money laundering and terrorist financing prevention in the Global and Local Policy of Prevention of Money Laundering and Terrorist Financing of A&O Shearman Grouping, as an obligated entity under the aforementioned Act 10/2010. In this regard, in accordance with the provisions of Article 65.5 of Act 10/2010, persons exposed to threats, hostile actions, or adverse labour measures for reporting both internally and externally on activities related to money laundering or terrorist financing may file a claim with the Independent Authority for the Protection of Whistleblowers A.A.I., under the terms provided in Title III of the Whistleblower Protection Law and in accordance with the Statute of the said Independent Authority for the Protection of Whistleblowers, A.A.I., approved by Royal Decree 1101/2024, of October 29.

- 3.2 “A&O Shearman Madrid Personnel” means all members, non-member partners, partners and members of staff of A&O Shearman Madrid, including employees and consultants with equivalent standing to partners, employees, self-employed individuals, consultants, agency staff, independent contractors and temporary workers and any other individual who is engaged by A&O Shearman Madrid.
- 3.3 This Policy will also apply to persons who, not being professionals of the Madrid Office of A&O Shearman at the time of submitting their communication:
- (a) They are working for or under the supervision and direction of a professional from A&O Shearman Madrid, its contractors, subcontractors, or suppliers.
 - (b) They have been professionals of A&O Shearman Madrid in the past, having already ended their employment or commercial relationship with the Madrid Office.
 - (c) Volunteers and interns of the Madrid Office, regardless of whether they receive remuneration or not.
 - (d) Persons whose employment relationship with A&O Shearman Madrid has not yet begun, in the event that information about breaches was obtained during the selection process or pre-contractual negotiation.
- 3.4 The application of the guarantees and protection measures contained in this Policy will also be applicable, under the requirements and scope set forth in Act 2/2023, to:
- (a) The legal representatives of the workers in the exercise of their advisory and support functions to the whistleblower.
 - (b) Individuals who, being part of A&O Shearman Madrid, assist the whistleblower in the process of reporting violations referred to in this Policy.
 - (c) Individuals who are related to the whistleblower and may suffer retaliation, such as coworkers or family members of the whistleblower.
 - (d) Entities for which the whistleblower works or with which they maintain any other type of relationship in a work context or in which they hold a significant participation⁵.

4. RESPONSIBLE FOR THE INTERNAL INFORMATION SYSTEM OF A&O SHEARMAN MADRID

- 4.1 The governing body of A&O Shearman Grouping has appointed the Partner and Global Compliance Officer for Legal Practice , as responsible for the Whistleblowing & Speaking-Up (Crime & Malpractice) System of A&O Shearman Grouping globally (configured as a single-person body), including the supervision of the Internal Information System of the Madrid Office (thus becoming, formally, the Responsible for the Internal Information System of A&O Shearman Madrid).
- 4.2 Both the appointment and the dismissal of the Responsible for the Internal Information System of A&O Shearman Madrid are the responsibility of the governing body of A&O Shearman Grouping. Such appointment and dismissal will be notified, in the manner and form determined in the development regulations of Act 2/2023 and Royal Decree 1101/2024, of October 29, which approves the Statute of the Independent Authority for Whistleblower Protection A.A.I., to said Independent Authority or, where appropriate, to the competent authorities or bodies of the autonomous

⁵ For these purposes, participation in the capital or voting rights corresponding to shares or participations is considered significant when, due to its proportion, it allows the person who owns it to have the capacity to influence the participated legal entity.

communities, within their respective competencies, within ten (10) business days following the event, specifying, in the case of dismissal, the reasons that justified it⁶.

- 4.3 The Responsible for the Internal Information System of A&O Shearman Madrid, as Partner and Global Compliance Officer for Legal Practice (COLP), is a managerial position of A&O Shearman Grouping that acts independently and without undue interference from the governing bodies of the Firm and has the necessary material and personal resources for the proper development of its functions, which it will carry out autonomously with respect to the rest of the firm's bodies, with neutrality, honesty, and objectivity.
- 4.4 In the absence of a conflict of interest, the Responsible for the Internal Information System of A&O Shearman Madrid will diligently assume the resolution of the procedures initiated as a result of the communications and information received through the Internal Information System and will ensure that in their processing the provisions of the Global Policy and this local Policy are respected. In the event of a conflict of interest in relation to a Case, they will abstain from intervening in it, with the Global Risk Management and Compliance Partner for the A&O Shearman Grouping proceeding to appoint another person in charge of resolving said Case.

5. COMMUNICATION CHANNELS ENABLED IN THE INTERNAL INFORMATION SYSTEM OF A&O SHEARMAN MADRID

- 5.1 Communications to the Internal Information System of A&O Shearman Madrid can be made through any of the following channels:
- (a) Preferably and unless there is a material or technical impossibility for the whistleblower, communications will be made through the independent whistleblowing reception service **Safecall** (<https://www.safecall.co.uk/file-a-report/>), available 24 hours a day, 365 days a year. The whistleblower can choose to submit their communication in writing or verbally by calling the local **Safecall** number for Spain 00 800 72332255, or both. The communication can be submitted in the whistleblower's own language and, if preferred, anonymously. The information provided will be securely forwarded via a report to the Responsible for the Internal Information System of A&O Shearman Madrid (Partner and Global Compliance Officer for Legal Practice) who will process it according to the procedural rules provided in the Global Policy and this local Policy.
 - (b) By email (vanessa.morgan@aoshearman.com) addressed to the Responsible for the Internal Information System of A&O Shearman Madrid (Partner and Global Compliance Officer for Legal Practice), who will process it according to the procedural rules provided in the Global Policy and this local Policy.
 - (c) By email (riskcompliance_spain@aoshearman.com), phone call (+34 91 782 98 00) or letter addressed to the Head of Risk & Compliance of the Madrid Office at Calle Serrano 73, 28006 (Madrid), who will limit themselves to receiving the communications they receive (written or verbal, or both) and forwarding them in the form of a report to the Responsible for the Internal Information System of A&O Shearman Madrid (Partner and Global Compliance Officer for Legal Practice) who will process it according to the procedural rules provided in the Global Policy and this local Policy.

⁶ In accordance with the Sole Transitional Provision of Royal Decree 1101/2024 of 29 October, approving the Statute of the Independent Authority for Whistleblower Protection (A.A.I.), the appointments and removals, both of natural persons and of the members of the collegiate body who have been designated as Responsible Persons of the Internal Information System since the entry into force of Law 2/2023 of 20 February, must be notified to the Independent Authority for Whistleblower Protection (A.A.I.) within two months from the date on which the Authority becomes operational, in accordance with Article 8.3 of said Law. In accordance with Order PJC/908/2025 of 8 August, determining the date on which the Independent Authority for Whistleblower Protection (A.A.I.) shall commence operations, the said Authority became fully operational on 1 September 2025.

- (d) At the request of the whistleblower made through any of the enabled communication channels mentioned above, the communication may also be presented through an in-person meeting (or via videoconference, as appropriate and feasible) within a maximum period of seven (7) days.
- 5.2 Verbal communications, including those made through in-person meetings, must be documented in one of the following ways, with the prior consent of the whistleblower:
- (a) By recording the conversation in a secure, durable, and accessible format; or
 - (b) Through a complete and accurate transcription of the conversation made by the responsible personnel.
- 5.3 Without prejudice to the rights granted under applicable personal data protection regulations, the whistleblower will be offered the opportunity to review, correct, and accept by signature the transcription of the conversation mentioned in the previous section. If the whistleblower disagrees with the content of the transcript, they shall inform the interviewer accordingly. Should the interviewer accept the proposed amendments, these shall be incorporated into the transcript. If the interviewer does not accept them, the proposed amendments shall be recorded at the end of the transcript, together with a note stating that they were not accepted. In any event, if the whistleblower refuses to sign the transcript, the interviewer shall record such refusal at the end of the transcript by means of an appropriate note.
- 5.4 **Communications may be made anonymously by sending a communication through any of the enabled written communication channels, without identifying the sender.**
- 5.5 When submitting the communication, the informant may indicate an address, email, or secure location for receiving notifications, and may also expressly waive the receipt of any communication regarding actions taken as a result of the submitted communication.
- 5.6 Communications received through any of the enabled communication channels that, due to their content and nature, refer to facts subject to the provisions of the *Protocol of Action against workplace harassment, sexual harassment, gender-based harassment, or violence against LGBTQ people and sexual violence of the A&O Shearman Office in Madrid*, will be processed as expressly provided in said Protocol, and their subsequent processing will occur as provided therein.
- 6. PRINCIPLES, GUARANTEES, AND PROTECTION MEASURES OF THE INTERNAL INFORMATION SYSTEM OF A&O SHEARMAN MADRID**
- 6.1 The Internal Information System of A&O Shearman Madrid is designed, established, and managed in a secure manner, ensuring the confidentiality of the identity of the informant and any third party mentioned in the communication, and of the actions taken in the management and processing of the same, as well as the rights to privacy, honour, defence, and presumption of innocence of the persons involved in the investigation processes that may arise, and the protection of their personal data, preventing access by unauthorized personnel.
- 6.2 The identity of the informant, if known, as well as that of the third parties mentioned in the communication, in addition to the third parties who must justifiably intervene in the processing and resolution of the procedures that are substantiated, may only be communicated to the judicial authority, the Public Prosecutor's Office, or the competent administrative authorities within the framework of a criminal, disciplinary, or sanctioning investigation, after informing the informant or the affected third

party, provided that this circumstance does not compromise the investigation or the ongoing judicial procedure.

- 6.3 Actions carried out within the framework of an internal investigation aimed at verifying and clarifying the facts contained in the received communications must be carried out with the greatest diligence, agility, and effectiveness possible, considering the complexity of the facts.
- 6.4 Actions resulting from a communication received through the Internal Information System must be developed under criteria of proportionality and objectivity, with the utmost respect for the current legislation.
- 6.5 The person affected by the communication (i.e., the one to whom the commission of a breach included within the scope and reach of this local Policy is attributed, by action or omission) has the right to be informed of the facts attributed to them and to be heard at any time. Once informed, they may request to review the information and documentation held in the ongoing internal investigation, although necessary measures must be taken to ensure that no information is revealed that would allow the identity of the informant to be known.
- 6.6 The necessary information for informants to use the Internal Information System is provided clearly and accessibly both on the A&O Shearman Group's intranet and on its corporate website: <https://www.aoshearman.com/en/legal-notices/country-specific-legal-notices/spain>
- 6.7 The various internal training programs of A&O Shearman Grouping (both in-person and/or through the 'Learning Portal' of the Intranet) will include adequate information on the existence and use of the firm's Internal Information System.
- 6.8 In the event that the facts reported could potentially constitute a crime, they must be brought to the attention of the Public Prosecutor's Office or the European Public Prosecutor's Office, as appropriate, all in accordance with the internal procedures provided for this purpose by A&O Shearman Grouping.
- 6.9 In line with the provisions of Act 2/2023, acts constituting retaliation, including threats of retaliation and attempts at retaliation against persons who submit a communication through the A&O Shearman Madrid Internal Information System as provided in this local Policy, are expressly prohibited. For these purposes, retaliation will be understood as any acts or omissions that are prohibited by law, or that, directly or indirectly, result in unfavourable treatment that places the persons suffering them at a particular disadvantage compared to others in the work or professional context, solely because of their status as whistleblowers or informants, or for having made a public disclosure. In particular, A&O Shearman Grouping will take measures to ensure that employees, managers, or agents who report

violations committed in the field of money laundering prevention and terrorist financing are protected against retaliation, discrimination, and any other type of unfair treatment for that reason⁷.

- 6.10 The Whistleblower Protection Act recognizes a set of support⁸ and protection measures against retaliation⁹ for the whistleblower who reports actions or omissions included within its material scope of application (Section 3 of this Policy), which will be facilitated by the Independent Whistleblower Protection Authority, A.A.I., or another competent authority or body, without prejudice to the specific support and assistance measures that may be articulated by A&O Shearman Madrid.
- 6.11 Whistleblowers must act in good faith and with an honest belief that serious harmful events have occurred or may occur, observe the criteria of truthfulness and proportionality in their communications, and refer only to facts that have some relation to A&O Shearman Grouping. False or malicious communications or information may result in the imposition of disciplinary, professional, or contractual sanctions, depending on the nature of the legal relationship with the bad faith whistleblower.
- 6.12 Persons who report or disclose violations covered by the scope of this Policy will be entitled to the protection measures described herein provided the following circumstances are met:
- (a) They have reasonable grounds to believe that the information referred to is true at the time of communication or public disclosure, even if they do not provide conclusive evidence, and that the said information falls within the scope of this local Policy.
 - (b) The communication or disclosure has been made in accordance with the provisions and requirements contained in this local Policy.

⁷ By way of example, the following will be considered forms of retaliation: (i) Suspension of the employment contract, dismissal, or termination of the employment or professional relationship, including non-renewal or early termination of a temporary employment contract once the probation period has been passed, or early termination or cancellation of goods or services contracts, imposition of any disciplinary measure, demotion or denial of promotions, and any other substantial modification of working conditions and non-conversion of a temporary employment contract into a permanent one, if the worker had legitimate expectations of being offered a permanent job, all unless the measures are carried out within the regular exercise of the power of direction, in accordance with applicable labour or professional regulations, due to circumstances, facts, or proven violations unrelated to the submission of a communication; (ii) Damages, including reputational damage, or economic losses, coercion, intimidation, harassment, or ostracism; (iii) Negative evaluation or references regarding work or professional performance; (iv) Inclusion in blacklists or dissemination of information in a specific sectoral field, which hinders or prevents the person from accessing employment or contracting works or services; (v) Denial or cancellation of a license or permit; (vi) Denial of training; or, finally, (vi) any form of discrimination, or unfavourable or unfair treatment motivated by the submission of a communication.

⁸ These support measures include: (i) Complete and independent information and advice, which are easily accessible to the public and free of charge, on available procedures and resources, protection against retaliation, and the rights of the affected person; (ii) Effective assistance from the competent authorities before any relevant authority involved in their protection against retaliation, including certification that they can avail themselves of protection under Act 2/2023; (iii) Legal assistance in criminal proceedings and cross-border civil proceedings in accordance with European Union regulations; and (iv) Financial and psychological support, exceptionally, if so decided by the Independent Whistleblower Protection Authority, A.A.I., after assessing the circumstances arising from the submission of the communication.

⁹ The legally recognized protection measures against retaliation are: (i) It will not be considered that the whistleblower has violated any restriction on the disclosure of information and, therefore, will not incur any liability in relation to such communication (except for criminal liabilities), provided that they had reasonable grounds to believe that the communication was necessary to disclose a breach, in accordance with the definition included in Act 2/2023, extending this protection also to information made by workers' representatives, even if they are subject to legal obligations of confidentiality or non-disclosure of confidential information; (ii) The whistleblower will not incur liability regarding the acquisition or access to the information that is communicated, provided that such acquisition or access does not constitute a crime. Any other possible liability of the whistleblowers arising from acts or omissions not related to the communication or not necessary to disclose a breach under this local Policy will be enforceable in accordance with the applicable regulations; (iii) In proceedings before a judicial body or other authority related to the damages suffered by the whistleblowers, once the whistleblower has reasonably demonstrated that they made a communication and suffered harm, it will be presumed that the harm occurred as retaliation for reporting. In such cases, it will be up to the person who took the harmful measure to prove that the measure was based on duly justified reasons not related to the communication; and (iv) In judicial proceedings, including those related to defamation, copyright infringement, breach of secrecy, violation of data protection rules, disclosure of trade secrets, or compensation claims based on labour or commercial law, the whistleblower and those legally extended whistleblower protections will not incur any liability as a result of communications protected by the Whistleblower Protection Law. Such persons will have the right to argue in their defence and within the framework of the aforementioned judicial proceedings that they communicated, provided they had reasonable grounds to believe that the communication was necessary to disclose a breach under the aforementioned Act.

6.13 The following persons are expressly excluded from the protection measures provided herein:

- (a) Information contained in communications that have been rejected by any of the internal information channels enabled or for any of the following reasons:
 - (i) When the reported facts lack all credibility.
 - (ii) When the reported facts do not constitute a breach of applicable laws and regulations included within the scope of this local Policy.
 - (iii) When the communication is manifestly unfounded or there are rational indications that it was obtained through the commission of a crime.
 - (iv) When the communication does not contain new and significant information about breaches compared to a previous communication regarding which the corresponding internal investigations or procedures have been concluded, unless new factual or legal circumstances justify a different follow-up.
- (b) Information related to claims about interpersonal conflicts or that only affect the whistleblower and the persons referred to in the communication or disclosure.
- (c) Information that is already fully available to the public or that constitutes mere rumours.
- (d) Information affecting classified information, or obligations arising from the protection of professional secrecy of legal professionals in the scope of their actions.
- (e) Information related to infringements in the processing of public procurement procedures that contain classified information or have been declared secret or reserved, or those whose execution must be accompanied by special security measures in accordance with current legislation, or where the protection of essential interests for state security requires it.

7. PROCESSING AND MANAGEMENT OF COMMUNICATIONS RECEIVED THROUGH THE INTERNAL INFORMATION SYSTEM

7.1 Acknowledgment of receipt and registration of the communication

- (a) Once the communication is received, an acknowledgment of receipt must be issued to the whistleblower within a maximum period of seven (7) calendar days from its receipt, unless this could jeopardize the confidentiality of the communication, it is not possible due to the anonymous nature of the communication, or the whistleblower has expressly waived receiving communications related to the investigation.
- (b) Likewise, within the aforementioned period of seven (7) calendar days, the said communication will be incorporated into the A&O Shearman Madrid Internal Information System Register (referenced below), assigning it an entry number and indicating a date of receipt, and its receipt and registration will be reported, if not already known, to the Responsible for the Internal Information System of A&O Shearman Madrid.

7.2 Admission of the communication

- (a) Once the communication is registered, the Responsible for the Internal Information System of A&O Shearman Madrid (or the person to whom they may delegate the receipt and registration of the communications received) must verify whether it falls within the scope of this Policy.

- (b) After the analysis of admission or not provided for in the previous letter, the Responsible for the Internal Information System of A&O Shearman Madrid will decide, within a period not exceeding ten (10) calendar days from the date of entry of the communication in the Register:
- (i) To reject (not admission for processing) the communication, when: (i) The reported facts lack all credibility; (ii) The reported facts do not constitute a breach of the laws and regulations as stated in Act 2/2023 or the internal policies included within the scope of this Policy; (iii) The communication is manifestly unfounded or there are rational indications that the information was obtained through the commission of a crime; or (iv) The communication does not contain new and significant information about breaches or infringements compared to a previous communication regarding which the corresponding investigations have already been concluded.

The rejection will be communicated to the whistleblower within five (5) calendar days following the adoption of the decision, indicating the reasons, unless the communication was anonymous, or the whistleblower had waived receiving communications.
 - (ii) Admit the communication for processing, which will be communicated to the informant within the next five (5) calendar days, unless the communication was anonymous, or the informant had waived receiving communications. In these cases, the Responsible for the Internal Information System of A&O Shearman Madrid will designate a Case Instructor who will be in charge of carrying out the appropriate internal investigation.
 - (iii) Immediately forward the information to the Public Prosecutor's Office or the European Public Prosecutor's Office, as appropriate, when the facts could potentially constitute a crime.
 - (iv) Forward the communication to the authority, entity, or organization deemed competent for its processing.
- (c) If, after the initial analysis of whether to admit a communication, there are doubts about the decision to be made, and provided it is possible to contact the informant, within a maximum period of three (3) calendar days from the date of registration of the communication, the informant will be required to clarify or supplement their communication within the next three (3) calendar days, providing any necessary documentation and data. In these cases, the decision on whether to admit the communication must be made within a maximum period of seven (7) calendar days from the conclusion of the aforementioned three-day period granted to the informant to supplement their communication (whether or not the required information has been provided).

7.3 Case Instruction

- (a) The Case Instructor will carry out the appropriate internal investigation, conducting the necessary, suitable, and proportional investigative actions to promptly and adequately determine the facts subject to communication. The Instructor will verify the truthfulness and accuracy of the provided information and, in particular, the reported conduct, respecting the rights of the affected parties, especially the presumption of innocence and the dignity of the involved persons, as well as their right to defense and to be heard.
- (b) All members of A&O Shearman Grouping are obliged to cooperate with the Case Instructor in their investigation, with the involvement of witnesses and affected parties being strictly confidential.

- (c) During the instruction, all affected parties will be informed about the processing of their personal data, unless they have been previously informed, as well as complying with any other duty required by personal data protection legislation.
- (d) The instruction should not extend beyond thirty (30) calendar days from the admission of the communication, unless justified circumstances, based on the complexity or number of actions to be taken, justify the extension of this period.
- (e) It will be ensured that the person affected by the information is informed of it, as well as the facts succinctly reported. Additionally, they will be informed of their right to submit written allegations and the processing of their personal data, unless they have been previously informed. However, this information may be provided during the hearing process if it is considered that providing it earlier could facilitate the concealment, destruction, or alteration of evidence. In no case will the identity of the informant be communicated to the affected parties, nor will access to the communication be granted. Only a brief summary of the facts will be provided to the investigated person.
- (f) Without prejudice to the right to submit written allegations, the instruction will include, whenever possible, an interview with the affected person in which, always with absolute respect for the presumption of innocence, they will be invited to present their version of the facts and provide any evidence they consider appropriate and relevant. To guarantee the right of defence of the affected person, they will have access to the Case documentation without revealing information that could identify the informant.
- (g) The Case Instructor may seek the support of the relevant Human Resources department within the A&O Shearman Grouping, solely and exclusively when the reported fact could lead to the adoption of disciplinary measures against a professional of A&O Shearman Grouping and/or as provided by the applicable regulations.

7.4 Resolution

- (a) Upon completion of the internal investigation (instruction), within a maximum period of fifteen (15) calendar days, the Case Instructor will submit a Proposal for Case Resolution, in the form of a written report, to the Responsible for the Internal Information System of A&O Shearman Madrid. This Proposal will include at least:
 - (i) A statement of the reported facts along with the identification code of the communication and the registration date.
 - (ii) The actions taken to verify the credibility of the facts.
 - (iii) The conclusions reached during the instruction and the assessment of the actions and evidence supporting them.
- (b) Within a maximum period of ten (10) calendar days from the receipt of the report on the Proposal for Case Resolution, the Responsible for the Internal Information System of A&O Shearman Madrid will issue the appropriate final Resolution of the Case, which may decide:
 - (i) The dismissal with prejudice and closing of the Case, due to the lack of evidence of the reported breaches, which will be notified to the informant (unless it is not possible, due to the anonymous nature of the communication or because they have waived receiving communications related to the investigation) and, if applicable, to the affected person. In these cases, the informant will have the right to the protection provided in this Policy, unless, as a result of the actions carried out during the

instruction phase, it is concluded that the information, in light of the gathered information, should have been rejected (not admitted for processing).

(ii) That the commission of some infringement is substantiated, with a proposal to adopt disciplinary sanction or the exercise of legal actions that, if applicable, may correspond. In the case of professionals with a labour relationship, the applicable disciplinary sanction will be applied according to the labour regulations in force. The Resolution will be forwarded to the person responsible for the Human Resources department of the office where the offending person provides their services. In the event that the exercise of some legal action is appropriate, it will be forwarded to the relevant legal department – such as the Regulation and Conduct team or Office of the General Counsel - for examination and action as appropriate. For the rest of the regimes or professional, contractual, or service provision relationships that may exist, the possible sanctions or penalties (including the extinction of the relationship) will be as agreed in each case in the corresponding contractual document in which said relationship has been materialized and in the applicable Law. Whatever the decision, it will be communicated to the informant, unless they have waived it or the communication is anonymous.

(c) The period to finalize the actions and respond to the informant, if applicable, shall not exceed three (3) months from the receipt of the communication, except in cases of special complexity that require an extension of the period, in which case, it may be extended for a maximum of another three (3) additional months, up to a total maximum of six (6).

8. REGISTER OF THE INTERNAL INFORMATION SYSTEM OF A&O SHEARMAN MADRID

8.1 The Responsible for the Internal Information System of A&O Shearman Madrid (or the person to whom they delegate) will keep a Register of the communications received and the internal investigations that have resulted in the instruction and resolution of the Case, ensuring due confidentiality and compliance with personal data protection regulations.

8.2 In said Register, which will be kept in digital format, the following information must be recorded in relation to each of the communications received: (i) Date of receipt; (ii) Identification code; (iii) Actions taken; (iv) Measures adopted; and (v) Closing date.

8.3 As provided in Act 2/2023, this Register of the Internal Information System of A&O Shearman Madrid will not be publicly accessible and only upon a reasoned request from the competent Judicial Authority, by order or warrant, and within the framework of a judicial procedure and under its supervision, can its content be accessed in whole or in part.

9. PROTECTION OF PERSONAL DATA AND CONFIDENTIALITY

9.1 Information on personal data protection for users of the System

(a) The personal data processing activities that occur within the Internal Information System of the A&O Shearman Madrid will be carried out respecting the general principles and obligations established in European personal data protection regulations (Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data – GDPR) and Spanish regulations (Organic Act 3/2018, of December 5, on the Protection of Personal Data and guarantee of digital rights – LOPDGDD), as well as in Act 2/2023 itself.

- (b) The personal data collected in the Internal Information System will be processed by Allen Overy Shearman Sterling LLP (hereinafter and for the purposes of this Section, A&O Shearman LLP), acting as Data Controller¹⁰.
- (c) The purpose of the processing is the management and processing of the communications and information received in the Internal Information System of A&O Shearman Madrid, as provided in this Policy.
- (d) The personal data that could be processed depending on the content of the communications that may be received could include the following categories: identifying data, data related to personal characteristics and social circumstances, contact data, academic and professional data, economic, financial and insurance data, and/or specially protected data. The personal data processed may have been provided both by the informant themselves and by third parties during the internal investigation that may take place.
- (e) The legal basis for the processing of personal data by the Controller is the fulfilment of legal obligations derived from Act 2/2023. In the case of processing specially protected data (such as health data, sexual life, union affiliation, political opinions, religious beliefs, etc.), they will be processed, in addition to fulfilling the aforementioned legal obligations, because it is necessary for the formulation or defence of claims by the Controller or the entity to which the person to whom the alleged infractions refer belongs. Persons making a communication through the Internal Information System must ensure that the personal data provided are true, accurate, complete, and up-to-date.
- (f) Legal service providers, IT systems, and technological tools of the Controller may access the personal data processed by the Controller during the provision of said services, although such data processing will always be carried out under the Controller's guidelines, following the signing of the appropriate data processing agreement and will be returned or duly destroyed at the end of the contracted service.
- (g) Regarding the transfer of personal data, in the event that the communications received may result in a procedure that requires the adoption of disciplinary measures by the entity of A&O Shearman Grouping to which the affected person belongs, the Controller will transfer their personal data to said entity based on the legitimate interest of said entity and the Controller to apply the corresponding disciplinary measures. Likewise, personal data may be transferred to the Public Prosecutor's Office to fulfil the obligations established in Act 2/2023 or, in the event that the communication presented results in the initiation of a judicial procedure, personal data will be transferred to the Judges and Courts based on the legitimate interest of the Controller linked to the right to effective judicial protection. If during the investigation process it has been necessary to collect specially protected personal data, they will be transferred, in addition to the legitimate interest of the Controller, based on the necessity of the processing for the formulation or defence of claims.
- (h) No international transfers of the personal data will be made (that is, to countries that do not offer an adequate level of protection for the purposes of Article 45 of the GDPR). If, in any case, due to the type of information and the circumstances of the case, it is necessary to make some type of international transfer, the interested party will be informed of all the circumstances of the transfer, including the identification of the recipient, the destination country, and the guarantee mechanism in accordance with the provisions of the GDPR.

¹⁰ Allen Overy Shearman Sterling LLP is a limited liability partnership registered in England and Wales with registration number OC306763 and registered office at One Bishops Square, London E1 6AD, United Kingdom.

- (i) The personal data included in the communications and those derived from the investigation procedure will be kept during the processing of the Case until the final decision is made and may be kept duly blocked during the statute of limitation period of legal actions against the Controller.
- (j) Users of the Internal Information System may at any time, in accordance with the applicable legislation in each case, exercise the rights of access, rectification, deletion, opposition, and limitation of the processing of their personal data by written communication addressed to the registered office of A&O Shearman LLP or to the A&O Shearman Madrid Office (Calle Serrano 73, 28006, Madrid, Spain) indicating the specific right they wish to exercise or through one of the following email addresses: DataPrivacy@aoshearman.com or RiskCompliance.Spain@aoshearman.com.
- (k) Measures will be taken to ensure the adequate security of the information and the identity of the informant, the person referred to in the communication, and any third party. Additionally, enhanced security measures may be established and precautions taken to ensure compliance with the duty of confidentiality.

9.2 **Principles of personal data protection and confidentiality governing the operation of the A&O Shearman Madrid Internal Information System**

- (a) Principle of transparency: The informant will be informed that their identity will in any case be kept confidential and will not be communicated to the affected person or third parties except, when appropriate under the terms established in Act 2/2023, to the Judicial Authority, the Public Prosecutor's Office, or the competent administrative authority within the framework of a criminal, disciplinary, or sanctioning investigation.
- (b) Principle of minimization: No more data will be collected than is strictly necessary and essential. If more data than strictly necessary is collected, it will be deleted as soon as possible.
- (c) Principle of purpose limitation: The personal data collected should not be processed for any purpose other than the management of the communication and processing of the Case.
- (d) Principle of storage limitation: Personal data should only be processed for the time strictly necessary. In any case, once three (3) months have passed since the receipt of the communication without having initiated investigation actions, the personal data must be deleted, unless the purpose of the storage is to provide evidence of the operation of the Internal Information System itself. Communications that have not been processed can only be kept in an anonymized form, without the obligation of blocking provided for in the LOPDGDD.
- (e) Principle of accuracy: All personal data included in the communicated information that is not accurate must be deleted. All this, unless the lack of accuracy may constitute a criminal offense, in which case the information will be stored for the necessary time during which the judicial procedure is processed.
- (f) Principle of integrity and confidentiality: The confidentiality of the informant and third parties will be guaranteed, as well as the establishment of all necessary technical and organizational security measures to protect the information against any unauthorized or illegal processing and against its accidental loss, destruction, or damage.

9.3 Limitations on access to personal data processed through the A&O Shearman Madrid Internal Information System

- (a) Only the Responsible Person of the Internal Information System (and those who directly manage the receipt of communications by delegation), third-party service providers considered data processors, and, where appropriate, the Data Protection Officer may access the personal data of a communication or a Case.
- (b) Additionally, the following may access personal data:
 - (i) The person responsible for the relevant Human Resources department within the A&O Shearman Grouping, who may access personal data only and exclusively when disciplinary measures against an employee may be taken.
 - (ii) The person responsible for the relevant legal department, who may access personal data only and exclusively if legal measures are to be taken in relation to the facts reported in the communication.
 - (iii) Other persons, exclusively when necessary for the adoption of corrective measures in the A&O Shearman Grouping or the processing of sanctioning or criminal procedures that may be appropriate.

10. EXTERNAL COMMUNICATION CHANNELS

- 10.1 Without prejudice to the preferred channel of this Internal Information System for the communication of possible breaches covered by Act 2/2023, informants and whistleblowers may also access the channels established by Public Administrations for these purposes ("External Channels"), either directly or after communication through this Internal Information System of A&O Shearman Madrid.
- 10.2 Act 2/2023 provides that any natural person may report to the Spanish Independent Authority for Whistleblower Protection [*"Autoridad Independiente de Protección del Informante (A.P.I.)"*] (Royal Decree 1101/2024, of October 29, approving its Statute), or to the corresponding Autonomous Community authorities or bodies, the commission of any actions or omissions included within the scope of application of said Act, either directly or after communication through the corresponding internal channel.
- 10.3 The members of A&O Shearman Madrid, as an obligated entity under Spanish regulations for the prevention of money laundering and terrorist financing (Act 10/2010 and its regulatory development), who become aware of facts or situations that may constitute violations in this matter, may report them to the Executive Service of the Commission for the Prevention of Money Laundering and Monetary Offenses ("SEPBLAC"). These communications will be sent to SEPBLAC in writing and will include all documents and information about the reported facts that justify the complaint. The communications will be confidential, and SEPBLAC cannot disclose the identifying data of the persons who made them.
- 10.4 There are other External Channels, including, but not limited to, the following: (i) External channel enabled by the Competition Directorate of the National Commission of Markets and Competition for communications related to violations of competition laws; (ii) Fraud Notification System of the European Anti-Fraud Office (OLAF); or (iii) External channels enabled by the National Securities Market Commission for reporting possible violations in the field of the securities market and investment services.

This Local Policy was approved by the Managing Partner of A&O Shearman Grouping on 7 April 2026. Any amendment to this Policy must likewise be approved by the said Managing Partner.