POLICY ON THE ALMIRALL GROUP IN SPAIN'S INTERNAL WHISTLEBLOWING SYSTEM AND ESSENTIAL PRINCIPLES OF THE REPORT MANAGEMENT PROCEDURE

1. THE ALMIRALL GROUP'S ETHICAL COMMITMENT

The Almirall Group, headed by Almirall, S.A., maintains a firm and unwavering ethical commitment in the conduct of all its corporate activities. This policy is the result of that ethical commitment and also the guarantee that all those who form part of the Almirall Group and who interact with it in a work or professional context can submit reports, safely and in good faith, about potential risks or breaches that they believe they have identified or detected.

2. THE POLICY

In line with this ethical commitment, this policy aims to provide clear and understandable information to those who form part of the Almirall Group and who interact with it in an employment or professional context on the functioning of the Almirall Group in Spain's Internal Whistleblower Channel (the '**Internal Channel**'), on the essential principles governing the management of reports received through the Internal Channel and on the rights of both those who submit reports ('**Whistleblowers**') and those who are affected by the report.

This policy, which will be posted on the Almirall Group in Spain's website, complies with the requirements under sections 5(2)(h) and 25 of the Spanish Whistleblower Protection Act 2/2023, of 20 February [*Ley de la protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción*], which incorporated Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 into Spanish law.

3. THE INTERNAL CHANNEL AND REPORTABLE FACTS

The Almirall Group in Spain has the 'SpeakUp!' Internal Channel, which is part of the Group's Internal Whistleblower System.

This Internal Channel may be used to report facts that may constitute breaches of European Union Law, very serious or serious criminal or administrative offences under Spanish law and breaches of the Code of Ethics and of the internal policies of the Almirall Group that occur within the framework of the activities of the Almirall Group in Spain.

Facts strictly linked to complaints relating to interpersonal conflicts or affecting only the Whistleblower and those to whom the report refers should not be communicated through the Internal Channel. The Almirall *People and Culture* department should be addressed to manage these issues.

4. WHO MANAGES THESE REPORTS? THE SYSTEM MANAGER

The Board of Directors of Almirall, S.A. has appointed Isabel Cristina Gomes, General Counsel of the Almirall Group, as Head of the Internal Information System of the Almirall Group in Spain (the '**System**

Manager'). The System Manager is the person in charge of managing and processing the reports received through the Internal Channel and supervising the investigations that are opened, always with the help of the persons (internal or external) who may be appointed in each case to assist the System Manager.

The Almirall Group will ensure the absence of conflicts of interest in the person of the System Manager in relation to the facts that are the subject of the reports managed and processed.

5. HOW CAN A REPORT BE MADE?

Reports may be filed in three different ways.

5.1 IN WRITING

Reports may be submitted in writing by accessing the SpeakUp platform! (https://almirall.integrityline.com/frontpage) published on the website and on the intranet of the Almirall Group in Spain.

After accessing the website, the Whistleblower must fill in a form with different information fields relating to the facts that are the subject of the report. The Whistleblower will have the option of attaching the documents supporting the report made. The Whistleblower has the choice between providing their contact details (name, telephone number and email address) or remaining anonymous.

In any case, the Whistleblower will be asked to open a secure mailbox (Secure MailBox) on the platform associated with a unique, password-protected case number that will allow the System Manager to maintain subsequent communication with the Whistleblower, even if the Whistleblower decides to remain anonymous.

Reports filed through this channel will generate an acknowledgement of receipt that will be sent, within a maximum of seven (7) calendar days, to the Whistleblower via their secure mailbox on the platform (and, where appropriate, by email if the Whistleblower has designated one).

5.2 BY VOICE MESSAGE

Reports may also be filed by calling the following telephone number: +34 900 963 436

In all cases, the following company code must be indicated: 25672.

Reports may only be submitted through this channel if the Whistleblower agrees to recording of the verbal communication, which will be in a secure, durable and accessible format. The voice message will be received by the System Manager.

After the report submitted by voice message is received, the Whistleblower will be informed of the processing of their personal data in accordance with Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (the '**GDPR**') and the applicable Spanish legislation.

Within a maximum of seven (7) calendar days following receipt of this report, an acknowledgement of receipt will be sent to the Whistleblower, provided that they have indicated an address, email or any other means to receive this acknowledgement of receipt.

5.3 BY FACE-TO-FACE MEETING, VIDEO CONFERENCE OR TELEPHONE CALL

Reports may also be submitted via a face-to-face meeting, videoconference or telephone call with the System Manager, always at the Whistleblower's request. The meeting (face-to-face, electronic or telephone) must be held within seven (7) calendar days of the request.

In this case, at the option of the Whistleblower, the report must be documented (i) by recording the conversation in a secure, durable and accessible format; or, where appropriate, (ii) by means of a subsequent complete and accurate transcription of the conversation. Without prejudice to their rights under data protection legislation, the Whistleblowers will be offered the opportunity to check, rectify and accept the report by signing the transcription of the conversation.

After receiving a report submitted through a face-to-face meeting, videoconference or telephone call with the System Manager, the Whistleblower will be informed of the processing of their personal data in accordance with GDPR and the applicable Spanish regulations.

6. CAN REPORTS BE SUBMITTED ANONYMOUSLY?

Yes, regardless of whether the report is submitted in writing or by voice message.

In any case, we encourage all potential Whistleblowers to identify themselves to facilitate the investigation of the reported event by the System Manager.

7. DO I HAVE AN OBLIGATION TO REPORT?

If you are part of the Almirall Group in Spain, yes. All directors, managers and employees of the Almirall Group in Spain are obliged, without exception, to report to the System Manager, through the Internal Channel, any breach of the legislation described in section 3 that may occur within the framework of the activities of the Almirall Group in Spain.

When in doubt, a report should be filed.

8. OTHER CHANNELS AVAILABLE

The Internal Channel of the Almirall Group in Spain is the preferred channel for submitting reports covered by this policy. We encourage all potential Whistleblowers to use the Internal Channel as a primary means of ensuring that potential risks or breaches reported can be properly investigated, addressed and resolved by the Almirall Group.

Whistleblowers may also use the external channels established by the competent authorities (the Independent Whistleblower Protection Authority and/or the corresponding regional authorities) to submit reports under the terms established in the respective legislation.

9. MANAGEMENT OF REPORTS

Once a report has been received, an acknowledgement of receipt will be sent to the Whistleblower within seven (7) calendar days of receipt, unless this could jeopardise the confidentiality of the report.

The System Manager will subsequently decide on whether to admit it for processing. The report will be admissible unless (i) the facts reported are not at all plausible or do not relate to the possible commission of any of the infringements that may be reported through the Internal Channel; (ii) the report is manifestly unfounded, has been submitted in bad faith or there is rational evidence that the underlying information was obtained by committing an offence; or (iii) the report relates to facts that are the subject of a previous report and does not contain significant new information that justifies its processing or is a matter of well-known facts that are publicly known.

After admission for processing, the System Manager will carry out the relevant investigative actions to clarify the facts depending on the circumstances. As a result of the investigation, appropriate measures may be taken.

As a general rule, a response to the investigative actions will be given within three (3) months. In cases of particular complexity, this period may be extended by an additional three (3) months.

10. CONFIDENTIALITY GUARANTEE

The guarantee of confidentiality of the identity (and, where appropriate, anonymity) of the Whistleblower is a guiding principle in the management of reports. The identity of the Whistleblower may not be disclosed to anyone other than those involved in the analysis of the report, in the eventual investigation carried out and in the analysis and implementation of the results of the investigation. All these persons must keep the identity of the Whistleblower strictly confidential.

Under no circumstances will the identity of the Whistleblower or specific personal data allowing the identification of the Whistleblower be communicated to those who are investigated or affected by the report; nor will they be given access to the report, without prejudice to their recognised rights.

The identity of the Whistleblower may be communicated to the competent authorities in the context of a criminal, disciplinary or sanctioning investigation. The Whistleblower will be informed of this communication requirement before their identity is disclosed, unless this information could jeopardise the investigation or the judicial proceedings.

11. PROHIBITION AGAINST RETALIATION

No Whistleblower who has made a report in good faith and in compliance with the requirements of the Whistleblower Protection Act may be penalised or suffer any negative consequences or retaliation (including threats of retaliation and attempted retaliation) for the mere fact of having filed a report.

This prohibition against retaliation covers a wide range of actions from which the Whistleblower is protected. Suspension of the employment contract, dismissal or termination of the employment relationship (including non-renewal or early termination of a temporary employment contract), imposition of any disciplinary measure or demotion or denial of promotion are considered retaliation for these purposes. Of course, this protection does not extend to cases where these measures are motivated by matters unrelated to having submitted the report (e.g. an employment offence leading to dismissal).

The guarantee of freedom from retaliation also extends the Whistleblower's relations (such as co-workers or family members), any individuals who assisted the Whistleblower during the submission and processing of the report and to the legal representatives of the employees in the exercise of their functions of advising and supporting the Whistleblower.

12. RIGHTS OF THE PERSON UNDER INVESTIGATION

The mere submission of a report that affects or incriminates a specific person does not imply that this person has actually committed any irregularity, nor does it imply that the Almirall Group considers from the outset that this person has committed the alleged irregularity. Those under investigation have a series of rights that the Whistleblower Protection Act confers on them and that the Almirall Group respects.

On the one hand, those under investigation have the right to be informed of the actions or omissions attributed to them and to be heard, although this right must be exercised at the time and in the manner deemed appropriate to ensure the proper conduct of the investigation.

Furthermore, during the processing of the case file, those under investigation have the right to the presumption of innocence, the right to honour, the right to defence and the right of access to the case file as required under the Whistleblower Protection Act, the exercise of which must always be adapted as far as possible to the principle of confidentiality of the Whistleblower's identity and of the facts and data of the proceedings.

13. HOW WILL THE PERSONAL DATA BE PROCESSED?

The Almirall Group in Spain is firmly committed to full compliance with the GDPR and the applicable Spanish legislation. Detailed information on the processing of personal data in the Internal Channel and in the processing of internal investigations that may occur (the '**Personal Data**') is set out below.

13.1 DATA CONTROLLER

Personal Data will at all times be processed in accordance with this policy and applicable data protection legislation.

The data controller will be the company of the Almirall Group in Spain that is affected by the reported facts. The identifying data for each of them are detailed below:

(i) **Almirall, S.A.**, with tax identification number A-58869389 and address at Ronda General Mitre, 151, 08022, Barcelona, Spain.

(ii) **Industrias Farmacéuticas Almirall, S.A.**, with tax identification number A-61158408 and address at Ronda General Mitre, 151, 08022, Barcelona, Spain.

(iii) **Laboratorios Almirall, S.L.**, with tax identification number B-60249331 and address at Carretera de Martorell, 41, 08740, Sant Andreu de la Barca, Spain.

(iv) **Ranke Química, S.L.**, with NIF A-61040705 and address at Carretera de Martorell, 41, 08740, Sant Andreu de la Barca, Spain.

These companies' Data Protection Officer, who can be contacted at dpo.global@almirall.com, is the point of contact for questions relating to the processing of Personal Data.

13.2 CATEGORIES OF PERSONAL DATA PROCESSED

The Personal Data will be identification, contact, financial, professional and employment data, as well as any other personal data deriving from the use and operation of the Internal Channel and from any investigations that may be carried out. On some occasions, as a result of the content of the facts reported through the channel, the Personal Data may also include special categories of data (for example, data relating to criminal or administrative offences, health data, data on sexual orientation or ethnic or racial origin).

13.3 SOURCE OF THE PERSONAL DATA

The Personal Data processed by the data controller will be those provided directly by the data subjects or, as the case may be, by Whistleblowers, as well as by employees and third parties from whom information is requested within the scope of the Internal Channel.

13.4 INTERNATIONAL DATA TRANSFERS

If it is necessary to make international transfers of the Personal Data (for example, to other entities of the Almirall Group outside the European Union), the transfers will be carried out in accordance with this policy and in compliance with all the guarantees required by the applicable data protection legislation.

13.5 PURPOSE OF PROCESSING AND STORAGE PERIODS

Personal Data will be processed for the following purposes and for the following retention periods:

A. Internal Channel Management

   The Personal Data will be processed to process the report and to take a decision on whether to admit it. The legal basis for this processing will be compliance with the legal obligations of the Almirall Group in Spain (article 6[1][c] GDPR) or, where applicable, the public interest (article 6[1][e] GDPR). Personal Data will only be processed in the Internal Channel for the time necessary and proportionate to decide on the admissibility or inadmissibility of the communication and will only be disclosed to third parties in those cases where it is necessary to (i) take a decision on the admissibility or inadmissibility of the communication (e.g. to external advisors supporting the System Manager); or (ii) ensure the proper functioning of the Internal Channel (e.g. to external providers).

   In particular, where reports are submitted verbally through the Internal Channel, the Whistleblower is aware that verbal reports will be recorded and/or documented (i) by recording the conversation in a secure, durable and accessible format; or (ii) through the subsequent complete and accurate transcription of the conversation, in which case the Whistleblower will be given the opportunity to verify, rectify and agree by signing the transcript of the conversation.

The Personal Data will be deleted from the Internal Channel once a decision has been taken on whether to admit the report. If no such decision has been taken, the Personal Data will in any case be deleted three (3) months after it was registered.

However, a limited amount of information may be stored for longer to provide proof of the system's operation. Any reports that are inadmissible will only be stored anonymously.

B. Processing of the internal investigation

If the report is admitted and processed, the team responsible for the investigation may process the data outside the Internal Channel to carry out the internal investigation regulated in this Procedure. The legal basis for this procedure will be compliance with the legal obligations of the Almirall Group in Spain (article 6[1][c] GDPR) or, where applicable, the public interest (article 6[1][e] GDPR). The Personal Data will only be processed for the time necessary and proportionate to carry out the research and to comply with the legal obligations of the Almirall Group in Spain. The Personal Data will only be disclosed to third parties (i) where appropriate to carry out the investigation (e.g. external consultants or service providers); or (ii) to take corrective measures as a result of the investigation (e.g. the heads of the People and Culture department or the Legal department of the Almirall Group, if appropriate to adopt measures within their areas of competence in relation to the outcome of the investigation). In any case, and as indicated in section 10, the identity of the Whistleblower may only be communicated to the court, the Government Legal Service or the competent administrative authority within the framework of a criminal investigation, disciplinary or sanctioning proceedings, and Whistleblowers will be informed of this need for communication before revealing their identity, unless this information could compromise the investigation or the judicial proceedings.

If measures are taken after the conclusion of the Investigation, the Personal Data will only be retained for as long as necessary to carry out these measures, and after that for the maximum of limitation of any applicable legal or contractual actions. Conversely, if it is decided not to take measures, the Personal Data will be blocked for a maximum of three (3) years and subsequently deleted, unless they need to be held for longer to meet legal or contractual liabilities in accordance with the applicable statute of limitations. In no case will data be stored for more than ten (10) years.

13.6 LEGAL BASIS FOR PROCESSING

The legal basis for processing the Personal Data for the above purposes is to comply with the legal obligations of the Almirall Group in Spain (article 6[1][c] GDPR) or, where applicable, the public interest (article 6[1][e] GDPR).

13.7 RIGHTS OF DATA SUBJECTS

Data subjects may contact the System Manager or the Data Protection Officer at the email address dpo.global@almirall.com to exercise their rights of access, rectification, objection, erasure, portability, restriction or any other rights recognised by law in relation to the Personal Data appearing in the

corresponding file, in accordance with applicable law. However, exercising the right of access, whether by the person to whom the reported facts are attributed or by any third party, will in no case allow access to the Whistleblower's identifying data.

Data subjects may also file a claim or request related to the protection of their Personal Data with the corresponding data protection authority, which in Spain is the Spanish Data Protection Agency (*Agencia Española de Protección de Datos*) (https://www.aepd.es).

14. TRAINING AND AWARENESS-RAISING

The Almirall Group in Spain will include training on the operation of the Internal Channel and the essential principles of the Internal Whistleblower System in its ordinary training programme for its employees.

Appropriate awareness-raising actions will also be carried out for the workforce.

15. DISCIPLINARY REGIME

Failure to comply with this policy may result in disciplinary sanctions or other appropriate action.

* * *

The Board of Directors of Almirall, S.A., as the parent company of the group, approved this policy at its meeting held on 13 June 2023, which will be published both on the website and on the intranet of the Almirall Group in Spain. In accordance with section 11 Whistleblower Protection Act, this policy extends its effects to all the companies that are part of the Almirall Group in Spain.

This policy will enter into force automatically after it is approved. The policies in force in the Almirall Group before the approval of this policy must be adapted to it.