Policy on the Internal Information System

MARK'ENNOVY GROUP

December 1st 2023

TABLE OF CONTENTS

1. WHAT IS THE GROUP'S INTERNAL INFORMATION SYSTEM? 3

2. WAYS OF SUBMITTING A COMMUNICATION 4

3. ESSENTIAL PRINCIPLES OF THE INTERNAL INFORMATION SYSTEM 5

3.1 CONFIDENTIALITY 5

3.2 RIGHT TO ANONYMITY 6

3.3 PROHIBITION OF RETALIATION 6

3.4 RIGHT OF THE PERSON UNDER INVESTIGATION 6

3.5 ACTUAL PROCESSING OF COMMUNICATIONS RECEIVED 7

4. PROTECTION OF PERSONAL DATA 8

4.1 DATA CONTROLLER 8

4.2 CATEGORIES OF PERSONAL DATA AND ORIGIN OF THE DATA 8

4.3 PROCESSING OF PERSONAL DATA (PURPOSES, LEGAL BASES AND RETENTION PERIODS) ... 9

5. LOG-BOOK 12

6. TRAINING AND DISSEMINATION 12

7. APPLICABLE LOCAL REGULATIONS 12

8. DISCIPLINARY REGIME 12

1. WHAT IS THE GROUP'S INTERNAL INFORMATION SYSTEM?[1]

Mark'ennovy Personalized Care, S.L. and its subsidiaries (collectively, the "**Group**") are firmly committed to regulatory compliance and business ethics in the conduct of their business.

For this reason, the Group has established an internal information system, articulated around a channel through which the Group's professionals or any third party can report the possible existence of a criminal or administrative offence or any other unlawful conduct committed within the framework of the activity carried out by the Group that has become known in a work or professional context.

The term **"Professionals"** encompasses all persons who make up the Group, including their directors or administrators, managers, employees or trainees. In any case, as indicated above, any other natural person who, in an employment or professional context, has information about the possible commission of the corresponding infringement may make use of the communication channel provided for in this Policy. An, or all persons making a report in accordance with this policy will hereinafter be referred to as "**Reporting Person"** or **"Reporting Persons"**, respectively.

This Policy on the Internal Information System (the **"Policy"**) sets out the main principles of the Communication Management Procedure (the details of which are provided in a separate document) (the **"Procedure"**), which is applicable to the Group in accordance with the provisions of Law 2/2023 of 20 February on the Protection of Persons Reporting Regulatory Violations and Anti-Corruption (the **"Whistleblower Protection Act").**

As established in article 4 of the Whistleblower Protection Act, the internal information system regulated in this Policy is the preferred channel for reporting the actions or omissions provided for in article 2 of such act[2]. However, the Whistleblower Protection Act also establishes an external channel to communicate with the Independent Authority for the Protection of Whistleblowers, AAI ("**AIPI"**), or the competent authorities that may be created at the regional level, to directly

[1] This is an English translation of the original document, which is drafted in Spanish. In case of any inconsistency or doubt on the meaning of the terms used in this Policy, the Spanish version should prevail.

[2] The infringements that may constitute the object of the information are (i) breaches of European Union law when they fall within the scope set out in Annex I of Directive (EU) 2019/1937 of the Parliament and of the Council of 23 October 2019, affect the financial interests of the Union or have an impact on the internal market; (ii) serious or very serious administrative infringements in accordance with the Spanish legal system; and (iii) criminal offenses.

formulate the corresponding communication, without prejudice to the possibility of also contacting the other competent authorities depending on the nature of the offence in question, including the competent institutions, bodies or agencies of the European Union. Thus, the implementation of the internal information system should not be interpreted as an indication by the Group that its Professionals should not directly contact such authorities to report the potential existence of regulatory breaches[3].

In any case, the whistleblowing channel must not be used as a channel for general complaints or to share personal opinions that do not involve a well-founded suspicion of non-compliance with legal regulations or an internal Group rule or policy, nor to transmit information linked to mere interpersonal conflicts or that only affect the Reporting Person and the persons affected by the communication in relation to facts that do not involve a breach of applicable legislation or internal Group rules and policies. All other matters that do not constitute a matter of communication under the terms of this Policy shall be channelled through the communication channels established for this purpose by the Group in accordance with its internal rules and regulations.

2. WAYS OF SUBMITTING A COMMUNICATION

The internal channel of the Group includes the following channels for the submission of communications:

(i). In writing:

a. Through the **digital whistleblowing channel** made available to the Group by Whistleblower Software ApS, which allows for written communications. This channel can be accessed via the following link https://whistleblowersoftware.com/secure/euclidvisiongroupemea .

[3] Depending on the information in question, the communication may be addressed to different authorities, such as the National Markets and Competition Commission, the State Administration of the Tax Agency, the National Securities Market Commission, the Spanish Data Protection Agency, etc. or, where appropriate, the competent criminal authorities (Court of Instruction or Peace, the State Security Forces or Bodies, the Autonomous Communities or the Local Corporations, as well as the Public Prosecutor's Office or, when the facts potentially constituting crime affecting the financial interests of the European Union, the European Public Prosecutor's Office).

b. By **post** addressed to the System Manager (as defined in Section 3.5), sending it to the following address: Avenida Ada Lovelace 12, 28906 Getafe, Madrid, Spain.

(ii). Verbally:

a. Through the **digital whistleblowing channel** made available to the Group by Whistleblower Software ApS, which allows communications to be made, in addition to in writing, verbally by recording a voice message. This channel can be accessed via the following link https://whistleblowersoftware.com/secure/euclidvisiongroupemea.

b. By **telephone call** to the System Manager.

c. At the request of the Reporting Person, by means of a **face-to-face meeting** with the System Manager, within a maximum period of seven days from the request.

3. ESSENTIAL PRINCIPLES OF THE INTERNAL INFORMATION SYSTEM

3.1 CONFIDENTIALITY

Any person who participates directly or indirectly in the processing of the communications and in the corresponding internal investigations must respect the confidentiality of the communications received and of the investigation carried out in accordance with the provisions of the applicable regulations. In the event that a communication is made through a channel other than the channel regulated in this Policy to any Professional of the Group, the recipient of the communication shall also be subject to the aforementioned obligation of confidentiality and shall immediately forward the communication to the System Manager.

The guarantee of confidentiality of the identity of the Reporting Person constitutes one of the guiding principles of the operation of the internal information system, so that this information shall not be disclosed to any person other than those who participate in the receipt and processing of the communication or, where appropriate, in the assessment and implementation of corrective, legal or disciplinary measures that may be relevant. Under no circumstances will the identity of the Reporting Person be communicated to the person under investigation or

affected by the report, nor any personal data that indirectly allows for his or her identification.

3.2 RIGHT TO ANONYMITY

The channel regulated in this Policy admits the possibility of making anonymous communications, regardless of the form in which the communication is made (verbal or written). However, the Group encourages Reporting Persons to identify themselves, as this facilitates the processing of communications.

3.3 PROHIBITION OF RETALIATION

The Reporting Person may not be penalised or suffer any negative consequences or reprisals[4] (including threats or attempts thereof) as a result of having made a report. This guarantee of freedom from retaliation extends to natural and legal persons related to the Reporting Person[5], to natural persons who, within the organisation in which the Reporting Person works, assist the Reporting Person in the process and to the legal representatives of the employees in the exercise of their functions of advising and supporting the Reporting Person. Furthermore, the mere fact of collaborating with the investigation shall never be grounds for a sanction, reprisal or any other negative consequence.

However, any communication made knowing it to be false or without reasonable grounds to believe that the information referred to is true at the time the communication is made is strictly forbidden.

3.4 RIGHT OF THE PERSON UNDER INVESTIGATION

The person under investigation has the right to be informed of the actions or omissions attributed to him/her and to be heard by the investigator of the internal investigation as often as he/she reasonably requests. However, the communication

[4] In accordance with the provisions of section 2 of article 36 of the Whistleblower Protection Law, retaliation is understood to be "any acts or omissions that are prohibited by law, or that, directly or indirectly, involve unfavorable treatment that places the people who suffer from them at a particular disadvantage with respect to others in the work or professional context, solely because of their status as informants, or for having made a public disclosure."

Likewise, in accordance with section 1 of article 36 of the Law on the Protection of Whistleblowers, all acts constituting retaliation are prohibited, including both threats and attempts at retaliation.

[5] Specifically: (a) natural persons who are related to the Reporting Person and who may suffer retaliation, such as co-workers or family members of the Reporting Person; and (b) legal entities, for which you work or with which you maintain any other type of relationship in a work context or in which you have a significant participation. For these purposes, it is understood that the participation in the capital or in the voting rights corresponding to shares or participations is significant when, due to its proportion, it allows the person who owns it to have the capacity to influence the invested legal entity.

to the person under investigation shall take place at the time and in the manner deemed appropriate to ensure the proper conduct of the investigation and shall comply with the principle of confidentiality of the identity of the Reporting Person. During the processing of the investigation, the person under investigation shall have the right to the presumption of innocence, the right to honour and the other rights provided for in the applicable regulations.

3.5 ACTUAL PROCESSING OF COMMUNICATIONS RECEIVED

The Human Resources Director of Mark'ennovy Personalized Care, S.L. is the person responsible for the management of the internal information system regulated by the Procedure, in accordance with the provisions of Article 8 of the Whistleblower Protection Act (hereinafter, the "**System Manager**").

The System Manager shall be responsible for ensuring the effective implementation of the internal informationsystem of the Group and for the diligent processing of reports, acting independently and autonomously and having at his or her disposal all necessary personal and material means for this purpose.

In this regard, all communications submitted through the channel regulated in this Policy shall be admitted for processing, except in the following cases:

(i). when the facts reported lack all plausibility;

(ii). when the facts do not refer to the possible commission of a criminal or administrative offence or any other unlawful conduct or conduct contrary to the applicable legal regulations or the Group's internal policies;

(iii). when the communication is manifestly unfounded (for example, when it is based on mere personal opinions without any indication of veracity) or there is evidence that the information supporting it has been obtained through the commission of a criminal offence; and

(iv). where the communication relates to facts that are the subject of a previous communication and does not contain significant new information that would justify its processing.

Without prejudice to the decision on the admissibility of the communication, an acknowledgement of receipt of the communication shall be sent to the Reporting Person within seven calendar days of its receipt, unless this could jeopardise the confidentiality of the information.

The possibility of maintaining communication with the Reporting Person and, if deemed necessary, of requesting additional information on the facts reported are

permitted. Thus, the Reporting Person may indicate an address, e-mail address or safe place for the purpose of receiving the corresponding communications.

Communications admitted for processing shall be investigated effectively and studied in detail in order to adopt the measures that, where appropriate, are deemed pertinent.

The System Manager shall ensure that no situation of conflict of interest, real or potential, arises in the processing of communications in order to guarantee that they are handled with maximum impartiality and objectivity.

The maximum time limit for replying to the Reporting Person on the investigative actions is set at three months from the date of receipt, except in cases of special complexity that require an extension of the time limit, in which case this may be extended up to a maximum of a further three months.

4. PROTECTION OF PERSONAL DATA

4.1 DATA CONTROLLER

Each company of the Group with which the Reporting Persons or any other third party involved in the development of internal investigations have an employment, contractual or any other type of relationship shall be considered responsible for the processing of personal data arising from the use of the internal information system and the processing of internal investigations (the "**Personal Data**") in accordance with this Policy and with the provisions of the regulations on the protection of personal data.

The "**Data Protection Officer**" is the point of contact with the various companies of the Group as the entities responsible for the processing of Personal Data for questions relating to the processing of Personal Data. For the Group, the Data Protection Officer may be contacted by the data subject at the following e-mail address: privacy@auratechlegal.es.

4.2 CATEGORIES OF PERSONAL DATA AND ORIGIN OF THE DATA

The Personal Data that will be processed within the scope of the internal information system will be identification, contact, economic, professional and employment data, data relating to the facts that are reported, and, on exceptional occasions, when necessary in the context and according to the nature of the investigation, special category data (such as data relating to criminal or administrative offences, health

data, data on sexual orientation or life or ethnic or racial origin) as well as any other data derived from the use and operation of the channel regulated in this Policy.

The Personal Data processed within the scope of the internal information system shall be those provided directly by the data subjects or, as the case may be, by the Reporting Person, as well as by the employees and third parties from whom information is requested in the course of the investigation, if any, and which shall in all cases be related to the facts under investigation.

4.3 PROCESSING OF PERSONAL DATA (PURPOSES, LEGAL BASES AND RETENTION PERIODS)

4.3.1 Purposes of processing and basis for legitimising the internal information system

Personal Data will be processed for the purpose of processing the communication and deciding on its admission or inadmissibility and, in the event of admission, carrying out the corresponding investigation and adopting the corrective and disciplinary measures that may be applicable.

These data processing operations will be carried out on the basis of (a) for those entities of the Group obliged to have an internal information system by Whistleblower Protection Act and all other applicable regulations (the "**Whistleblower Protection Regulations**"), compliance with legal obligations; and (b) for those entities of the Group that are not obliged to maintain an internal information system by the Regulations, the fulfilment of a mission in the public interest. Similarly, and only when strictly necessary for these purposes, special categories of data may be processed for reasons of substantial public interest in accordance with Article 9(2)(g) of the GDPR.

4.3.2 Retention of Personal Data in the internal information system

Personal Data will only be processed within the channel for receiving communications for the time necessary to take a decision on their admissibility and will not be disclosed to third parties unless necessary for the proper functioning of the system or for taking a decision on the admissibility of a communication.

In particular, where the means of submission of communications through the channel for receiving communications is oral, the Reporting Person is aware that oral communications will be documented (i) through a recording of the conversation in a secure, durable and accessible format; or (ii) through the subsequent complete and accurate transcription of the recording of the conversation, in which case the Reporting Person will be given the opportunity to verify, rectify and accept by signing the transcription of the conversation.

Once the decision on its admission or inadmissibility has been taken, the Personal Data shall be deleted from the communications reception channel and, in any case, if no decision has been taken in this respect, three months after its recording. However, limited information may be kept for a longer period of time in order to leave evidence of the functioning of the system.

4.3.3 Processing for internal investigation and subsequent retention of Personal Data

In the event that the communication is admitted for processing, the Personal Data may be processed outside the channel for receiving communications for the purpose of carrying out the relevant internal investigation. This processing shall be carried out (i) for entities of the Group that are obliged to have an internal information system under the Whistleblower Protection Regulation (those entities with more than 49 employees), based on the fulfilment of legal obligations of such companies (art. 6.1.c) GDPR); and (ii) for entities of the Group that are not obliged to maintain an internal information system under the Whistleblower Protection Regulation to fulfil a mission in the public interest (art. 6.1.e) GDPR).

The Personal Data will be processed for the time necessary to carry out the investigation and comply with legal obligations.

If it is proven that the information provided or part of it is not true, it must be immediately deleted as soon as this circumstance comes to light, unless this lack of truthfulness may constitute a criminal offence, in which case the information will be kept for the time necessary during the processing of the corresponding legal proceedings.

Once the investigation has been concluded, the Personal Data will be kept for the time necessary to adopt and execute the corresponding measures and, after that, for the maximum period of prescription of any legal or contractual actions. In no case will the data be kept for a period of more than ten years.

4.3.4 Recipients of Personal Data and international transfers

Personal Data will be processed by the System Manager and those persons within the Group who, in accordance with the scope of their powers and duties, and in accordance with the Whistleblower Protection Act, are required to do so. They shall only be disclosed to third parties if this is appropriate for the purposes of the investigation (e.g., service providers or external advisors) or for corrective measures (e.g., the head of human resources —if disciplinary measures are to be taken against

an employee— or the head of legal services —if legal measures are to be taken in connection with the reported facts— of the Group).

The identity of the Reporting Person may be disclosed to the judicial authority, the public prosecutor's office or the competent administrative authority in the context of a criminal, disciplinary or disciplinary investigation. Disclosures made for these purposes shall be subject to safeguards set forth in the applicable regulations. In particular, the Reporting Person shall be informed of this circumstance before his or her identity is revealed unless such information could jeopardise the investigation or judicial proceedings.

If the facts reported or subsequently investigated contain circumstances that make the international transfer of Personal Data necessary, the appropriate measures will be adopted in accordance with the applicable regulations. Likewise, should the processing of data by any of the service providers assisting in the management of the communications reception channel regulated in this Policy or of the investigation involve international transfers, these will in any case be carried out in accordance with the applicable regulations. For example, standard contractual clauses approved by the European Commission will be adopted or personal data will be transferred to countries for which the European Commission has recognised that they provide an adequate level of protection for personal data. Information on the safeguards adopted by the Group may be obtained by contacting the Data Protection Officer.

4.3.5 Exercising personal data protection rights

Persons involved in the preliminary processing or investigation process may contact the System Manager or the Data Protection Officer for the purpose of exercising their rights of access, rectification, opposition, erasure, portability, limitation or any other rights recognised by the regulations in relation to the data contained in the corresponding file, under the terms provided for in the applicable legislation. However, when the person to whom the facts are attributed or any third party exercises his or her right of access, the Reporting Person's identification data shall not be communicated to him or her.

Likewise, the holders of Personal Data may file a complaint or request related to the protection of their Personal Data before the corresponding Data Protection Authority, in Spain, the Spanish Data Protection Agency (www.aepd.es).

5. LOG-BOOK

The System Manager is obliged to ensure that a logbook is kept of the communications received and the internal investigations to which they pertain, guaranteeing the confidentiality requirements and the data protection obligations provided for in this Policy and in the applicable regulations.

6. TRAINING AND DISSEMINATION

The content of this Policy shall be the subject of the training and dissemination actions determined from time to time by the System Manager.

Likewise, a copy of the Policy shall be sent to the Professionals of the Group when they join any of the companies of the Group. In addition, the Group's website shall include a specific section on the existence of the internal information system in which this Policy shall be published.

7. APPLICABLE LOCAL REGULATIONS

This Policy has been prepared on the basis of the applicable Spanish legislation (in particular, the Whistleblower Protection Act) as well as the principles and obligations recognised in 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 European Union law. However, in the event that the communication sent by the Reporting Person is subject to the legislation of another country, the Policy will be applicable without prejudice to compliance with legislation other than Spanish legislation (in its scope of application) to the extent that such legislation establishes additional protections or guarantees to those provided for therein. If any of the provisions included in this Policy are contrary to the applicable local regulations, the provisions of such regulations shall be complied with.

8. DISCIPLINARY REGIME

Failure to comply with the provisions of this Policy may result in the imposition of disciplinary sanctions or other appropriate action depending on the relationship between the offender and the Group.

* * *