INTERNAL INFORMATION SYSTEM AND MANAGEMENT OF THE WHISTLEBLOWING CHANNEL PROCEDURE

AUDAX RENOVABLES, S.A.

Y SU GRUPO DE SOCIEDADES.

Version control			
Version	**Date**	**Controller**	**Action**
1.0	28 July 2020	Criminal Compliance Committee (author)	Design and preliminary implementation of the Whistleblowing Channel as a key element of the Compliance and Criminal Risk Prevention Model
2.0	18 July 2023	Criminal Compliance Committee	Update in accordance with the requirements of Law 2/2023 of 20 February, on the protection of persons who report breaches of law and on fight against corruption.
3.0	25 November 2024	Group Compliance Officer	Update regarding the new governance system in the Internal Information System

Approvals			
Version	**Date**	**Controller**	**Action**
1.0	28 July 2020	Audit Committee	Approval of the Regulations
2.0	27 September 2023	Board of Directors of AUDAX RENOVABLES, S.A.	Approval of the Internal Information System and Management of the Whistleblowing Channel Procedure
3.0	17 December 2024	Board of Directors of AUDAX RENOVABLES, S.A.	Update regarding the new governance system in the Internal Information System

Related internal regulations	
Name	**Last version**
Compliance and Criminal Risk Prevention Policy	17 December 2024
Corporate Code of Ethics and Conduct	10 November 2020
Compliance and Criminal Risk Prevention Handbook	17 December 2024
Corporate Policy on Internal Information System and Informant Protection	17 December 2024

Explanatory notes

- Throughout this document the masculine gender may be used as well to refer to the feminine gender or others in the spirit of inclusivity and solely for the purpose of economy of language and facilitating the reading.
- For the purpose of this document the terms "informant" and "whistleblower"; affected person" and "reported person"; and "communication", "information" or "complaint" are used interchangeably.

INDEX

1. Introduction and Object

The object of this Internal Information System and Management of the Whistleblowing Channel Procedure of Audax Renovables, S.A. and the companies belonging to the Audax Group (hereinafter referred to as the "**Procedure**") is to establish the principles and operational guidelines of the Internal Information System (hereinafter interchangeably referred to as "**Internal Information System**", "**IIS**" or the "**System**") pursuant to the underlying Corporate Policy on Internal Information System and Informant Protection (hereinafter, the "**Policy**").

On 16 December 2019, Directive (EU) 2019/1937 (hereinafter 'Directive') entered into force, which aims to encourage whistleblowing and protect whistleblowers from retaliation by establishing effective, confidential and secure whistleblowing channels. This Directive is implemented in the different Member States of the European Union through the national legislation of each State.

In the case of Spain, the Law 2/2023 of 20 February, on the protection of persons who report breaches of law and on fight against corruption (hereinafter, "**Law 2/2023**"), which incorporates to the Spanish law Directive its main purpose is to protect persons who, generally in a work or professional context, have obtained information on certain regulatory infringements and communicate it through internal and/or external information channels or, where appropriate, disclose it publicly, providing adequate protection against any type of reprisals. The formal and secure mechanism used within the Audax Group for the purpose of reporting irregularities is the Whistleblowing Channel (hereinafter also referred to as the "**Channel**"), regulated by the Policy and by this Procedure.

In accordance with our Corporate Code of Ethics and Conduct (hereinafter also referred to as the "Code of Ethics"), our Compliance and Criminal Risk Prevention Model, and especially with the Policy, the Audax Group strives to develop its business activity with integrity, while promoting ethical conduct, respect for human dignity and compliance with applicable laws.

And with the aim of maximising the efficiency of the prevention of irregular conduct, the key role lies with the collaboration of all the persons comprising the Group making use of the Channel System for the purpose of reporting unethical conduct and/or cases of non-compliance with internal and/or external regulations, without fear of suffering any kind of negative consequences or retaliation for the report they made in good faith.

2. Scope of application

2.1 Corporate scope of application

This Procedure is applicable to all the companies comprising the Audax Group, subject to the Directive and/or to Law 2/2023, independently of their line of business, geographical location and corporate structure.

This is without prejudice to the fact that the companies that make up the Audax Group must comply, in all cases, with the regulations corresponding to the country in which they are located, in accordance with the transposition of the Directive and applying the particularities foreseen locally.

The governing bodies of these companies shall make appropriate decisions in order to integrate the provisions of the Policy and of the corresponding Procedure in accordance with the applicable legislation, the structure of the governing bodies, commissions and departments, among other factors. This may entail adherence to and/or incorporation by means of an annex to this Procedure of the particularities that may be applicable.

For this purpose, the governing bodies of the companies, acting through the Compliance Officers of each of the subsidiaries, shall coordinate their actions with the Information System Manager. At all events, the guarantees of the System are applicable at the level of the Audax Group, and any conduct which may be construed as retaliation against the informant acting in good faith shall be punished.

2.2 Who may report irregularities through the Whistleblowing Channel?

The following persons may submit complaints and queries through the Whistleblowing Channel:

- Members of the governing, managing and supervisory bodies of the Audax Group
- Shareholders or partners of the Audax Group
- Employees
- Employees made available by temporary employment agencies ("**ETT**")
- Interns and trainees
- Volunteers
- Candidates who are in the selection process
- Former employees
- Legal representatives of the employees

All of them together, and unless otherwise indicated, shall be referred to as the "**Personnel**", and have the obligation to report any detected irregularities and offences, whether present, past or future.

Moreover, the Audax Group makes the Channel available to:

- External collaborators, natural or legal persons (suppliers, business partners, contractors, agents, etc.)
- Any person working for (or under the supervision or direction of) the above.

Hereinafter all of them together will be referred to as "**Third Parties**".

The Whistleblowing Channel is not designed to be used by clients, who have a special channel, without prejudice to the applicable regulations.

2.3 Who may be reported through the Whistleblowing Channel?

Any member of the Personnel of the Audax Group who has committed, is committing or is going to commit a breach or has been involved in an act included within the objective scope outlined in the next section may be reported.

Although the investigative capacity and sanctioning authority of the Audax Group is limited to its Personnel, irregularities committed by the Third Parties may be reported in order to verify the facts (however to a limited extent), and pertinent measures may be applied including, where appropriate, the termination of the contract and any legal actions necessary

in order to protect the interest of the Group, the Personnel, the Third Parties themselves, and of the company.

2.4 Objective scope of application of the Whistleblowing Channel

In line with the ethical and compliance culture existing in the Audax Group, we make available to our stakeholders (the Personnel and Third Parties) the Channel which allows two types of communications:

Complaints: understood as communications of possible irregularities or breaches which might constitute an infringement of the regulations, a violation of the Code of Ethics, of its implementing provisions or of other Audax's applicable internal regulations.

Enquiries: understood as requests to clarify specific doubts raised by the implementation or interpretation of applicable regulations, both external and internal, including doubts regarding the operation of the Channel or any other applicable rules.

The objective scope of application of the Whistleblowing Channel includes:

- All kinds of conduct contrary to the principles and rules of conduct established by the Code of Ethics and other internal regulations of the Audax Group applicable to the Personnel.

- Actions or omissions, which imply non-compliance with any external regulations, especially those, which may constitute serious or very serious criminal or administrative offences, implying an economic damage to the Public Treasury and to the Social Security.

- Actions or omissions, which may constitute infringements of the Law of the European Union, and particularly those, which:

> Meet the scope of application of the European Union acts specified in the appendix to Directive (EU) 2019/1937 of the European Parliament and of the Council, of 23 October 2019, on the protection of persons who report breaches of Union law;

> Enter within the scope of application of Law 2/2023 or other local regulations applicable to companies belonging to the Audax Group;

> Affect the financial interests of the European Union, as outlined in article 325 of the Treaty on the Functioning of the European Union (TFEU); or

> Have an impact on the internal market, as outlined in article 26 point 2 TFEU, including the infringements of the regulations of the European Union regarding competition and aid granted by the States, as well as infringements related to the internal market in relation with the acts which infringe the regulations on corporate income tax or with practices aimed at obtaining tax advantage distorting the objective or aim of the legislation applicable to the corporate income tax.

Any form of retaliation, including threat of retaliation and attempts of retaliation.

Conduct susceptible of being considered as mobbing, sexual harassment and/or discrimination based on gender or any other motive, in accordance, at any event, with the applicable legislation and specific regulations.

The Whistleblowing Channel should not be used to inform about interpersonal conflicts, which do not imply any infringement and/or which concern only the informant and the persons to whom the information refers, nor to inform about issues, which are already fully known to the public, or which are merely gossip.

Likewise, it is strictly prohibited to knowingly communicate false information and gossip.

3. Mechanisms or channels for filing enquiries and complaints

The complaints should be submitted in good faith and without knowingly giving false information and without any fear of retaliation for reporting irregularities or infringements, as long as the complaint is made in good faith.

3.1 Internal Information System of the Audax Group

The Audax Group promotes making enquiries or reporting of concerns, irregularities and breaches by any means, however, it makes available to the Personnel and Third Parties the following **formal lines, which make up the Internal Information System** and comprise the **Whistleblowing Channel**:

- **Whistleblowing Channel Platform** of the Audax Group, in writing or by voice recording. The platform belongs to an external provider and is accessible from the corporate website, the Employee Portal of those companies which have it, as well as through the following link: https://audax.whistleblowernetwork.net

- **Personal meeting**: the reporting person may request, through the Whistleblowing Channel, a personal meeting with the Information System Manager, which shall take place within seven (7) calendar days from the date of the request.

Regardless of the way the offences are reported, the Audax Group shall conduct an independent, impartial and efficient investigation, ensuring the rights of the parties involved and informing the reporting person about the progress and the result of such investigation in a confidential manner, always in accordance with the Policy and this Procedure.

If the Internal Information System Manager receives an enquiry or a complaint by any means other than the Channel, they shall formalise such communication on the Whistleblowing Channel Platform, expressly indicating that such communication was made verbally, by post or in any other way and, as far as possible, giving evidence of the communication.

If a person other than the Manager receives by any means information about an irregularity or breach as outlined in the personal and material scope of this Procedure, they shall immediately transfer such information to the Manager through the Whistleblowing Channel Platform, indicating the way in which they received the information and, as far as possible, giving evidence of the communication. At any event, the person who receives such information has the duty of confidentiality regarding the entirety of the information, especially with regard to the identity of the persons directly or indirectly affected and/or involved, including expressly the informant and the reported person.

An infringement of this duty, especially with regard to the confidentiality, is considered to be a very serious offence and may result in the application of relevant disciplinary and legal consequences.

Without prejudice to the means outlined above, the Internal Information System Manager or other persons or entities/bodies may also obtain information about infringements or irregularities in connection with the scope of application of the Policy through other means while performing their ordinary duties (e.g. risk updates and controls, certification processes, audit procedures, etc.), and if so, it may be necessary to conduct investigation of the information disclosed applying the principles and guarantees of this Procedure and, in any case, those outlined in the Policy.

3.2. IIS management at Group level: coordination between the IIS Manager at the head entity of the Audax Group and the Compliance Officers of the Group companies.

The IIS is unique in the Audax Group, however, for regulatory, efficiency and proximity reasons and in order to provide maximum protection to the informant, Audax has chosen a mixed management model in the sense that the different Compliance Officers of each of the companies that form part of the Group also participate in the management of the communications received through the IIS in a coordinated manner.

By virtue of the foregoing, in those cases in which a communication is received in the IIS from any of the Group companies, the Internal Information System Manager shall delegate such communication to the Compliance Officer of the company from which it originates so that he/she may process and resolve it, thus adopting the role of Instructor in its management and following the provisions of section IV of point 6.2 of this Procedure. To this end, the corresponding communications shall be sent through the Whistleblowing channel Platform itself.

In the event that the report is received by alternative means, the Internal Information System Manager must manually enter the report in the Platform and proceed in the same way, sending the report to the corresponding Compliance Officer. Similarly, in the event that the report is received by alternative means, the Compliance Officer of any of the companies that make up the Audax Group must enter it manually in the Whistleblowing channel Platform so that it can be duly processed with all the guarantees.

For these purposes, there is a single Internal Information System Manager for the entire Audax Group, without prejudice to the fact that he/she must subsequently coordinate with the Compliance Officers of the Group's subsidiaries in order to properly manage the irregularities and breaches reported.

3.3 External channels. Independent Administrative Authority

Pursuant to the Directive, the Internal Information System is the means of preference for the purpose of submitting information about an irregularity. And, apart from the aforementioned mechanisms, the government or public administration of each country where the Audax Group is present may have **external channels made available to the public**. In the case of the European Union, the Member States have appointed competent authorities (Independent Administrative Authority) to whom cases of non-compliance may

be reported either directly or through previous complaint in the Whistleblowing Channel of the Audax Group.

Information is clearly stated and easily accessible through the Whistleblowing Channel Platform and the website of the Audax Group about such external channels (alongside their implementation information is made available about their existence and/or their means of operation). The Compliance Officers of each company will be responsible for keeping this information updated through the means they deem appropriate and, in any case, on the website of the corresponding Audax companies.

4. Board of Directors and Internal Information System Manager. Competence and responsibility

1. In accordance with the provisions of the Internal Information System Policy of the Audax Group, the responsibility to guarantee its correct operation lies with the Board of Directors of the parent company of the Audax Group.

2. The Board of Directors of the parent company of the Audax Group delegates to the Group Compliance Officer (hereinafter referred to as '**GCO'**), as the Internal Information System Manager, the management of the IIS and, therefore, the processing of information about irregularities and infringements of all the Group. This is without prejudice to the fact that the Compliance Officer of each company that makes up the Group will also be the local Information System Manager. Consequently, all obligations relating to the GCO in its capacity as Information System Manager are also applicable to the local Compliance Officers, in their capacity as Local Manager.

3. In order to provide more security to the Whistleblowing Channel implemented in the Audax Group, there is an external platform (the Whistleblowing Channel Platform), which guarantees independence and traceability of the information at any time and throughout the process. This Platform will be available in the languages necessary for any person linked to the Audax Group to be able to communicate in the language corresponding to the country in which the Group operates.

4. The Information System Manager shall perform their duties in an independent way from the rest of the bodies of the Audax Group, may not receive any kind of instructions while carrying out their duties (including from the supreme governing body and by their express mandate), and shall have at their disposal all the human and material resources necessary to perform those duties. Moreover, they shall respect the principles, rules of conduct and guarantees outlined in the legislation, the Policy, the Code of Ethics and other internal regulations, ensuring especially the prohibition of any kind of retaliation, whether direct or indirect, against the members of the Personnel or Third Parties who, in good faith and in compliance with this Procedure, have made a complaint.

5. The Information System Manager shall ensure the confidential character of the identity of the person who submitted the enquiry or reported irregularities and infringements, be it through the whistleblowing Channel or by any other means, and chose to identify themselves. The identity of the whistleblower may be communicated to the judicial Authority, the Public Prosecutor or the competent administrative authority within the framework of a

criminal, disciplinary or penalty investigation, without prejudice to other regulations which may be applicable. The disclosures thus made shall be subject to appropriate protections established in the applicable regulations. In particular, the whistleblower shall be informed about it before they reveal their identity, unless such information should compromise the ongoing or future investigation or administrative or legal proceedings, or should not meet the criteria established by the competent judicial or administrative authority or by legal regulations.

6. The Information System Manager shall maintain a secure communication path with the whistleblower, using for this purpose the secure mailbox of the platform or any other means which may be made available for such purpose according to the circumstances.

7. The Information System Manager shall include in their annual report the basic and statistical information about the management and operation of the Whistleblowing Channel in the previous year, safeguarding at any event the confidentiality of the identity of the whistleblowers. Moreover, they shall put down in a record book (the "Record Book") the complaints received and the internal investigations based on them. The platform shall automatically register the complaints in a way which will allow to keep updated the Record Book. Likewise, the Manager shall manually incorporate into the platform the complaints received by other means. The Record Book shall contain the file number of the complaint, its date, state of the internal investigations carried out, guaranteeing at all events that the requirements of confidentiality are met according to the applicable regulations. The Record Book is not public, as the only persons with the right to access it are the Information System Manager and the persons appointed by the Information System Manager, and access to the entirety or part of it may be granted on justified request of the competent legal Authority, by a judicial decision, and in the framework of legal proceedings and under the care of such authority; without prejudice to any other regulation which may be applicable.

5. Whistleblower protection. Principles and guarantees of the Internal System.

The guarantees applicable to the Internal Information System and particularly to the management and processing of the complaints, independently of the means of communication used, are outlined in the Internal Information System Policy of the Audax Group. The following principles and guarantees are expressly specified below:

5.1 Prohibition of retaliation

It is expressly prohibited to undertake actions which may constitute retaliation, including threat of retaliation and attempts of retaliation against persons who, in good faith, reported information in accordance with the rules of this Procedure.

For the purpose of this Procedure, and by way of example and without it being considered as a complete list, the following actions are considered as retaliation:

- Dismissal or suspension of the employment agreement;
- Early termination of a temporary employment agreement, after the conclusion of the trial period;
- Refusal to employ an applicant who is a whistleblower;

- Imposition of any disciplinary measure, demotion or withholding of promotion and any other substantial change in the terms of employment (except when such measures are adopted in accordance with labour legislation and because of proven circumstances, facts or infringements, which are not connected with the complaint filed);
- Withholding of training, which would have been granted had not the complaint been made, or without apparent reason;
- Denial of due variable remuneration or its significant and unjustified reduction;
- Early termination or cancellation of a contract for purchase and sale or lease of goods or services;
- Coercion, intimidation, harassment or ostracism;
- Exclusion from meetings and/or group messaging;
- Harm, including that done to the reputation or resulting in economic losses;
- Harmful changes done to duties and work responsibilities;
- Change of location of the place of work or unjustified relocation;
- Unjustified negative evaluation or references concerning work or professional performance or which result in sudden and baseless changes;
- Blacklisting or disseminating information within a sector of industry, which impede or block access to employment or to contracts for performance of work or provision of services;
- Cancellation of a licence or permit;
- Psychiatric or medical referrals made to the whistleblower; or
- Discrimination or unfavourable or unjust treatment.

In addition to whistleblowers, these protective measures will be likewise applicable:

- If the whistleblower is a worker, to the persons within the organisation who assist them and/or support them in the process of presentation, managing and investigation of the complaint.

- To the natural persons related to the informant and who may suffer retaliation, such as their friends and relatives, especially those who may influence or condition the whistleblower at the time of filing a complaint and provide information and possible evidence or aid them.

To the legal persons for whom the whistleblower works or with whom he or she maintains any kind of relationship in a work context or holds a stake in such legal person. In order to protect the persons against possible retaliation, the Audax Group will apply (and will make the rest of the Group apply) the **protective measures** appropriate for the case. For this purpose periodical monitoring will be carried out in accordance with the "Non-Retaliation Internal Protocol". On the other hand, besides the support measures established in the regulations, the Audax Group will ensure (and will make the rest of the Group ensure) that, as far as possible, a series of **support measures** be made available to the whistleblower in accordance with the "Non-Retaliation Internal Protocol".

5.2 Guarantee of confidentiality and anonymity

The whistleblowers may identify themselves, or make the complaint anonymously if they so prefer, in which case the Audax Group will not attempt to uncover their identity. However, although it is not necessary, the whistleblowers are encouraged to identify themselves or, at least, to provide a means of contact other than the Secure Mailbox (as defined below) in order to enable more effective communication with them in case more information about

the reported incidents is required. Should they identify themselves, they shall be guaranteed the utmost confidentiality of their identity and any other identifying data in accordance with applicable legislation.

Should they choose to use the Whistleblowing Channel platform, this platform has a "Secure Mailbox", which allows to maintain communication with the anonymous whistleblower, therefore it is crucial to save the unique PIN number provided by the platform during the registration of the complaint, in order to be able to track the complaint and access the request for additional information from the Internal Information System Manager. The Audax Group guarantees at all times the confidentiality of both the whistleblower's identity and the facts, data and information provided with regard to the natural and legal persons affected and to any third party mentioned in the submitted complaint, regardless of the means of relaying the irregularity, including expressly the complaint made to a person other than the Internal Information System Manager. As a means of guaranteeing the confidentiality of the identity of the whistleblower who has chosen to identify themselves, their identifying data will not be included in the scope of the right of access available to the reported person.

The identity of the informant may be communicated to the judicial Authority, the Public Prosecutor or the competent administrative authority within the framework of a criminal, disciplinary or penalty investigation, without prejudice to other regulations which may be applicable. The disclosures thus made shall be subject to appropriate protections established in the applicable regulations. In particular, the information shall be transmitted to the whistleblower before they reveal their identity, unless such information should compromise the ongoing or future investigation or proceedings, or should not meet the criteria established by the competent judicial or administrative authority or by any applicable regulations.

5.3 Conditions of protection

The protection system outlined in this Procedure will be applied to the whistleblowers and/or directly or indirectly involved persons as long as:

a) The communication or disclosure has been made in accordance with the requirements established in the applicable legislation, the Policy and this Procedure;
b) The informant has reasonable grounds to think that the reported information is true at the moment of the communication or disclosure, even if they do not provide conclusive evidence, and that such information belongs to the scope of application of Law 2/2023 or the equivalent local legislation in force in the companies belonging to the Group.

Otherwise, no protection under this Procedure (regardless of any other system of protection being applicable) shall be granted to the informants who file the following complaints:

a) Information which already is fully available to the public;
b) Complaints which are dismissed;
c) Information about interpersonal conflicts, or which concerns only the informant and the persons to whom the information or disclosure refers;
d) Mere gossip;
e) Information beyond the scope of application of this Procedure.

6. Procedure for the handling of Enquiries and Complaints

6.1 Procedure for handling Enquiries

Upon receiving an enquiry through the Whistleblowing Channel, the Group Compliance Officer as the Manager of the system shall resolve it giving their response in writing, as far as possible, within seven (7) working days. As mentioned above, if the enquiry comes from a Group company, the GCO will receive it and then delegate its management to the Compliance Officer of the company in question through the Platform itself or by any other appropriate alternative means.

In order to resolve the enquiry, the Manager shall be assisted or advised by other departments of the Audax Group or by external experts, whose assistance they may consider necessary to achieve an accurate and appropriate resolution in reasonable time.

6.2. Procedure for handling Complaints.

I. Submission of the complaint

Once the form has been filled in by the whistleblower **in writing** or by **voice recording** through the Whistleblowing Channel platform, the complaint is created.

- **By voice recording**: if the whistleblower, in order to register their complaint, opts for the voice recording system made available on the platform, it should be noted that the recording will be played back using a special format so as to make the voice unrecognisable and impossible to associate it with any person, and thus protect the anonymity.

- **Mailbox**: the whistleblower, when submitting the complaint to the Whistleblowing Channel platform, may use the "Secure Mailbox" in case of future wish to send further communications or add information and/or documents. For this purpose a PIN code associated with the complaint will be created. It is necessary for the reporting person to memorise or save the PIN code for an appropriate follow-up of the report.

- **Holding a personal meeting to file the complaint:** Should the whistleblower wish to make the complaint personally, a meeting shall be held within seven (7) days from the request, in a neutral and secure place, and in order to guarantee adequate confidentiality of the investigation the persons attending the meeting shall be informed in writing about their obligation of secrecy and confidentiality, as well as shall be given all the legal information concerning data protection. Moreover, the whistleblower may attend the meeting, if they so desire, in the presence of a lawyer or a trusted person of their choosing. In such cases the complaint shall be documented by a complete and exact transcription of the conversation, made available to the whistleblower for the purpose of verification, rectification and acceptance by their signature, or shall be recorded on a secure medium. If for any reason the whistleblower or any of the attending persons do not want to sign the transcription, such information shall be stated and the investigation shall proceed. In the case of a complaint made in a personal meeting, the Information System Manager shall include the transcription or recording of the conversation in the platform.

II. Receipt, Record Book, Acknowledgement of Receipt and Acceptance/Dismissal of the complaint for processing

- **Receipt**: when a complaint is submitted to the Platform, the Information System Manager receives an email informing them about a new complaint with a file number assigned.
- **Record Book**: the complaint with its file number is immediately registered in the Record Book.
- **Acknowledgement of Receipt**: when a complaint is submitted, an acknowledgement of receipt is automatically generated and will be sent to the informant at any event within seven (7) calendar days from the receipt of the complaint. The acknowledgement of receipt is sent to the whistleblower in order to inform them of the receipt of the complaint and of the file number assigned to it.
- **Decision about acceptance for processing**: later the Information System Manager decides about the commencement of the relevant investigation or dismissal of the complaint, with appropriate justification included in the file and in the Record Book.

III. Information for the parties: notification of the whistleblower / reported person

After the complaint has been accepted for processing, the whistleblower and the reported person will be informed about it:

- **Notification of the whistleblower**: the decision about the acceptance for processing or dismissal of the complaint will be communicated to the whistleblower who identified themselves and/or indicated any means of communication (email, telephone number, etc.) or through the Whistleblowing Channel Platform **within**

seven (7) calendar days from the receipt of the complaint or as soon as possible, as long as such notification does not compromise the investigation or jeopardise the confidentiality of the communication.

- **Notification of the reported person or affected person**: likewise, the person being the object of the complaint, if such complaint is accepted for processing, will be informed by the Information System Manager **within a maximum of thirty (30) calendar days** from the receipt of the complaint about **(i)** the receipt of the complaint, **(ii)** the summary of actions or omissions attributed to them, **(iii)** the departments and third parties who, if applicable, may be addressees of the complaint and **(iv)** how to exercise their right of access, rectification, erasure, restriction, objection, and portability of their personal data, in accordance with the internal and external regulations on data protection. However, the right of access of the reported person shall be limited to their own personal data processing, therefore, and given the confidential nature of the complaints, the reported person will not be able to exercise this right for the purpose of learning the identity and personal data of the whistleblower provided, as the case may be, by the latter. The notification to the reported person will be sent to their business email address or by any other means available to the Information System Manager.
  Exceptionally, if the Information System Manager considers that by notifying the reported person they could compromise the investigation, such notification may be postponed until that risk disappears. At any event, the notification shall be sent within a maximum of three (3) months, as long as there are justified reasons to do so. All that without prejudice to the fact that other express and binding time limits may be established by law, in which case they will necessarily be complied with.

When applicable, bearing in mind the shortness of the limitation period of labour offences, the Information System Manager shall provide the Human Resources Management with information about a preliminary estimate time of the investigation so as to enable them to decide whether they should initiate simultaneously any disciplinary proceedings in order to avoid the expiration of the limitation period, which would make it impossible to apply any relevant disciplinary measures.

I.V. Opening of the Proceedings. Investigator and Investigation of the Reported Incidents

Investigator: in the case of opening the investigation stage, the Information System Manager will appoint an Investigator (usually themselves or an appointed manager), without prejudice to the support and help from any members of the Personnel or external experts that may be required. In the event of a complaint from one of the Group's companies, the Compliance Officer of the company in question shall be responsible for investigating the complaint by delegation of the GCO.

In any case, the Manager will supervise the processing and investigation of the complaints examined by the Investigator, and will offer them support, assistance and advice at all times. With this regard, any written communication maintained by the Investigator with the whistleblower or the reported person shall be made or registered on the Whistleblowing Channel Platform, in order for the Manager to have access to it. Once the proceedings have

been opened, the identity of the Investigator and the investigation measures applied shall be registered in the Record Book.

The Investigator will conduct preliminary enquiry (through the analysis of the documents, files, or by interviewing the parties, witnesses or others) deemed necessary in order to confirm the veracity and reality of the reported conduct, or may delegate these and other duties to an external advisor, in order to apply informed criteria to the management of the proceedings and improve the guarantees of confidentiality and independence. The investigation shall seek to answer the following questions:

- What are the reported actions or omissions (the "Conduct");
- To whom the Conduct is attributed
- The time when the Conduct took place;
- To what extent that Conduct is connected with a breach of internal and/or external regulations;
- What are the consequences of the Conduct and, in particular, whether it may be a cause of criminal liability for the Audax Group.

For this purpose, the investigation of the complaints, regardless of their nature, shall be governed by the principles, rights and guarantees of the parties, outlined in the Internal Information System Policy of the Group, as well as, particularly, by the following:

- **Proportionality**. The process of gathering data and information during the investigation of a complaint (including personal data) must comply with this principle. This means that (i) the data collected shall be limited to those strictly and objectively necessary for the purpose of processing the complaints and to verify the reality of the reported issues; (ii) the data shall be treated at all times in accordance with the applicable regulations on data protection, for lawful and specific purposes in connection with the investigation, which may be initiated as a consequence of the complaint, and may not be used for incompatible purposes; and (iii) shall be adequate and not excessive in relation with the aforementioned purposes.

  In the process of gathering information and documentation related to the incidents, the Investigator shall guarantee at all times the respect of the data protection regulations, applicable Workers' Statute and Collective Agreements, as well as of the relevant business agreements.

- **The right to an impartial Investigator.** The investigation shall be conducted according to the rules of equality, independence and honesty.

- **Equality of the parties.** Any unjust situations of privilege of one of the parties at the expense of the other party must be prevented.

- **Right to a defence.** The right of the reported person to be heard, to request and bring evidence, as well as to refute the evidence presented against them, in order to challenge the allegations made against them.

- **Right of reply.** Construed as the recognition of the right of the parties to present their respective claims from the point of view of examination of evidence, as well as the right to be heard before being punished. In this regard, the whistleblowers and the reported persons or persons involved may be assisted by a trusted person of their choosing.

- **Right to privacy, place and time protection.** All the investigations must respect the right of the participants to confidentiality of their personal data and private information. Moreover, personal interviews shall be conducted at times and in places which do not jeopardise their necessary discreet and confidential nature. If the Investigator deems it appropriate and there is no objection from the parties, the interviews may be conducted online, by videoconference.

- **Right to the presumption of innocence of the investigated persons and right to honour.** Every person is presumed innocent and shall be treated as such during the investigation proceedings, until they are proved responsible for the reported incidents. Likewise, the right to honour of the investigated persons shall be guaranteed.

- **Right of information**: should the whistleblower choose to identify themselves and/or provide a means of communication, the communication with them shall be maintained at all times in order to clarify any doubts which may arise or to request any additional information. Moreover, the reported person has the right to be informed in accordance with the provisions of section 2 above.

- **Secrecy**: all persons involved in the investigation are bound by obligation to maintain professional secrecy regarding the information to which they have access while processing the files. Failure to comply with this obligation may result in sanctions.

At any point of the procedure the Information System Manager may seek legal assistance and advice from external adviser about aspects related to the issues or the investigation (e.g. the initial classification of the acts, their categorisation, investigation steps to be taken, conducting inquiries or taking the most appropriate disciplinary action in each case).

V. Investigation report and draft resolution

Once the investigation has been completed, the Investigator conducting it shall draw up an **Investigation Report**, which will include a **Draft Resolution**. The Draft shall be drawn up within five (5) calendar days from the completion of the investigation.

The Report shall be communicated to the Information System Manager (if they have not been appointed as the Investigator of the case, who at any event will have the obligation of drawing up the Report).

For this purpose it should be taken into account that the process of conducting the investigation and drawing up the Report and Draft Resolution and, eventually, transmitting it to the interested parties, must be completed within **three (3) months, extendable by other three (3) months in cases of particular complexity**.

The Report and the Draft Resolution shall contain a justified verdict about the possible existence or absence of an infringement of the internal and/or external regulations. In particular, the Draft Resolution shall include any of the following alternative proposals:

a) conducting complementary proceedings necessary in order to determine the existence or absence of an infringement
b) closing the proceedings if, after conducting the pertinent investigation, it is considered that the reported issues have not been sufficiently confirmed or if such issues are finally considered not to constitute an infringement.
c) the existence of an infringement of the internal and/or external regulations.
d) it shall include, if applicable, a proposal of measures to be taken when the reported issues have been sufficiently confirmed and, additionally, they constitute an infringement included in the objective scope of the System (e.g. legal measures of any kind to be taken including corrective actions, improvements in the system to prevent similar situations in the future, and others). With this regard, strictly necessary information about the complaint and the investigation of the facts shall be submitted to the Human Resources Management or to the competent body of the Audax Group responsible for deciding and adopting the specific disciplinary measures deemed necessary, and the Information System Manager shall keep a record of the implementation of the measures adopted.
e) the Internal Information System Manager, after the pertinent scrutiny, shall immediately submit the information to the Public Prosecutor when the facts indicate a criminal offence, after obtaining advice from the Legal Advisor and, if considered necessary, from an external consultant. If the investigated issues affect financial interests of the European Union, a notification shall be submitted to the European Public Prosecutor's Office.

VI. Application of appropriate disciplinary measures

Sanctions, disciplinary measures or legal consequences will be applied by the management or competent organisation (Human Resources Management, competent body, etc.). The Information System Manager shall keep a record of the implementation of the measures adopted.

7. Registering and filing

The Record Book as well as the communications and documents related to each investigated case shall be duly registered and filed. The aforementioned documentation must be kept for a period of 10 years in order to address any possible claims that may be made, or to comply with any legal obligations that may be imposed on the Audax Group. At all events, the storage, the protection of personal data and the applicable technical measures must comply with the provisions of the Privacy Policy of this Channel.

The platform stores all kinds of communications and tracks every report or enquiry. The Information System Manager shall collect such documentation and keep it in the systems always in compliance with the regulations and security measures for the protection of personal data in accordance with the Privacy Policy of the Channel.

8. Special case when the complaint affects the Internal Information System Manager -GCO-, Local System Managers -Local Compliance Officers-, or a member of the Board of Directors.

If the complaint refers to or affects the Information System Manager -GCO- or Local System Managers -Local Compliance Officers-, the person in question may not participate in the proceedings. Likewise, it will be understood that there is a conflict of interest preventing their participation in the following situations:

- family relationship with the whistleblower or the reported person;

- direct interest in the reported issues;

- clear animosity towards the whistleblower or the reported person;

- present or past situation of power disparity between them and the whistleblower or the reported person; or

- any other circumstances, which would prevent them from acting independently.

The decision about the existence of a conflict of interest of the person and, therefore, of their incapacity to participate in the proceedings, may be brought forward by the parties (whistleblower/reported person) or by the Manager themselves and/or Local Compliance Officers. In the situation of conflict of interest concerning the Manager -GCO-, the Group Chief Internal Auditor shall undertake the role of investigator and may cooperate with a third party.

If the complaint affects any member of the Board of Directors, the Information System Manager will inform the Secretary of the Board about such situation and together they will select an independent investigator.

Likewise, in the event that the conflict of interest affects the Local Compliance Officer of a subsidiary company of the Group, the GCO will assume the role of instructor and may be supported by a third party.

9. Personal Data Protection

The use of the Internal Information System, including the Whistleblowing Channel, by any person implies for the Audax Group the obligation to ensure confidentiality and protection of the data provided, therefore all the information and documentation obtained, as well as any updates thereof, shall be kept in a place of restricted access.

The Whistleblowing Channel has a confidential nature, guaranteeing at all times the utmost confidentiality of the data and information collected through the complaint (including data and information obtained during the investigation) and, in particular and among other issues, of the identity of the whistleblower. All the bodies and/or persons involved in the processing

of the complaint shall ensure the utmost confidentiality, without prejudice to the legal obligations or court orders.

The Internal Information System Manager will make sure that all the technical and organisational measures necessary to comply with the personal data protection regulations are applied.

The data of the person making the complaint or of other persons whose data are processed shall be retained solely for the time needed to establish whether the investigation should be launched into the reported issues, except when the purpose of data retention is to provide evidence of the operation of the criminal responsibility prevention model and of the Whistleblowing Channel comprised in it. The complaints, which have not been followed up may be stated only in an anonymous form, without being applicable in such cases the blocking of data obligation referred to in the Organic Law on Data Protection and Guarantees of Digital Rights in Spain, or other regulation on data protection, which may be locally applicable.

At any event, the special regulations applicable in matters of data protection in accordance with Spanish Law, are those specified in the «***Whistleblowing Channel Privacy Policy***». The parties concerned may exercise their rights of access, rectification, erasure, restriction or objection on legally established terms by accessing dpo@audaxrenewables.com.