



# WHISTLEBLOWING CHANNEL REGULATIONS

## AUDAX RENOVABLES, S.A. AND ITS GROUP OF COMPANIES

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
		Audit Committee	Approval of the Regulations

Related regulations		
Name	Last version	Link/Appendix
Criminal Compliance Policy	10 September 2019	
Code of Ethics	28 February 2019	
Compliance and Criminal Risk Prevention Handbook	10 September 2019	

## Table of contents

<b>1. Introduction and Objective</b> .....	3
<b>2. Subjective scope of the Whistleblowing Channel</b> .....	4
<b>2.1 Who should report and who may use the Whistleblowing Channel?</b> .....	4
<b>2.2 Who may be reported through the Whistleblowing Channel?</b> .....	4
<b>3. Objective scope of the Whistleblowing Channel</b> .....	4
<b>4. Mechanism for filing enquiries and reports. How should or how could an enquiry or a report be made? Who handles them?</b> .....	5
<b>5. Requirements for the report to be accepted for processing and reasons for its dismissal</b> .....	5
<b>6. Protection of the whistleblower and of the reported person. Personal data protection. Whistleblowing Channel Guarantees</b> .....	6
<b>6.1 Prohibition of retaliation</b> .....	6
<b>6.2 Personal data protection. Confidentiality and possible anonymity of the whistleblower</b> .....	6
<b>6.3 Incompatibility and/or conflict of interest</b> .....	7
<b>6.4 Rights and obligations of the whistleblower</b> .....	7
<b>6.5 Rights of the reported person</b> .....	8
<b>7. Procedure for the handling of enquiries and reports</b> .....	8
<b>7.1 Procedure for handling enquiries</b> .....	8
<b>7.2 Procedure for handling reports Lodging a report Receipt and acceptance. Follow-up</b> .....	8
<b>A) Lodging a report</b> .....	8
<b>B) Receipt and acceptance of the report</b> .....	9
<b>C) Monitoring of the report by the reporting person</b> .....	9
<b>7.3 Investigation of the reported issues</b> .....	10
<b>7.4 Motion for a resolution</b> .....	11
<b>7.5 Decision on the measures to be taken</b> .....	12
<b>7.7 Special procedure for the handling of reports on moral harassment (mobbing), sexual harassment or gender-based harassment</b> .....	12
<b>7.8 Special procedure for the case of a report affecting a member of the Criminal Compliance Committee</b> .....	13
<b>8. Registering and filing</b> .....	14
<b>9. Principles of action and security measures</b> .....	14
<b>Appendix I - Issues which may be reported through Whistleblowing Channel</b> .....	15
<b>Appendix II - Privacy Policy</b> .....	19

## 1. Introduction and Objective

The need to protect the good reputation and prestige of Audax Renovables, S.A. ("**Audax**") as the parent company of the Audax Group<sup>1</sup> (the "**Group**" or the "**Audax Group**") requires that all its employees and partners, when acting on behalf of Audax, comply at all times with (i) applicable legislation, (ii) the Code of Ethics and (iii) applicable internal policies and procedures. In addition to that, a Whistleblowing Channel is made available to the employees and partners who, upon discovery of any behaviour contrary to the aforementioned policies and procedures, are required to use it.

For the purpose of detecting improper conduct it is also important to be able to rely on the cooperation of all the suppliers, and therefore they are also encouraged to use the Whistleblowing Channel.

The objective of the Whistleblowing Channel Regulations (hereinafter: the "**Regulations**") is to regulate the actions and steps undertaken by the Criminal Compliance Committee as the body responsible for the management of the Whistleblowing Channel when processing the enquiries and reports received, as well as the management of the rights and obligations of the persons who use it.

Therefore, in line with the ethical and compliance culture existing in Audax, we make available to our stakeholders (internal<sup>2</sup> and external<sup>3</sup>) the Channel which allows two types of communications:

- **Reports:** understood as communications of possible irregularities or breaches which might constitute an infringement of the regulations, especially of a criminal nature, 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.

Audax has been scrupulous in meeting all the legal requirements, especially those regarding privacy and data protection, while designing the Whistleblowing Channel. It has also taken into account the guidelines of Directive 2019/1937 on the protection of persons who report breaches of Union law.

These Regulations apply to the Audax Group in any country and/or region, and have been drawn up in compliance with the Spanish and European regulations on data protection. In the case of domestic or foreign subsidiaries, the Compliance delegate or the person appointed for that purpose shall be responsible for the appropriate

---

<sup>1</sup> Audax Group refers to the group of investee companies where Audax Renovables, S.A. holds a majority stake and/or exercises direct or indirect control.

<sup>2</sup> Internal stakeholders refer to all the employees of the Audax Group, its directors, senior management, legal representatives as well as executives in law or in fact.

<sup>3</sup> External stakeholders refer to business partners and suppliers.

adaptation of these Regulations. If necessary, it shall be done by means of an amendment containing all the applicable differences.

## 2. Subjective scope of the Whistleblowing Channel

The Whistleblowing Channel is a tool made available to certain groups specified in the following subsection, in order to enable them to make enquiries or report any irregularity of which they may be aware and which falls within the objective scope.

### 2.1 Who should report and who may use the Whistleblowing Channel?

All the employees, directors, managers, legal representatives and executives (hereinafter, and unless otherwise indicated, all of them shall be referred to as the "**Personnel**") can make enquiries and must report through the Whistleblowing Channel any irregularity of which they are aware and which falls within the objective scope of the Regulations, without fear of being subject to retaliation.

Moreover, Audax makes the Channel available to providers of goods and services and/or business partners of the Group, so that they can use it to make enquiries as well as to report breaches ("**Third Parties**").

Both groups, when necessary, will be referred to as "**Users**".

### 2.2 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.

## 3. Objective scope of the Whistleblowing Channel

The objective scope of application of the Whistleblowing Channel covers the following acts, which nevertheless are specified in **Appendix I**:

- Breach of any applicable external law, especially all kinds of conduct susceptible of being considered as moral harassment (mobbing), sexual harassment and/or gender-based harassment, as specified in Appendix I, and in any case in accordance with the applicable laws of the country where the breach has allegedly taken place.
- Types of conduct specified in the Criminal Code and offences indicated in other special laws, which may expose Audax to criminal liability under applicable law of the country where the breach has allegedly taken place.
- Acts 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 according to the country and/or region.

The reported facts may refer to instances occurring in the past, present or future. In order to file a report it is not necessary to provide evidence, but a well-founded suspicion should suffice, provided that the report is made in good faith.

#### **4. Mechanism for filing enquiries and reports. How should or how could an enquiry or a report be made? Who handles them?**

The enquiries and reports may preferably be submitted through a platform designed for that purpose and accessible through:

- Employee Portal
- <https://audax.whistleblowernetwork.net>

The platform has been developed by an external provider and therefore guarantees the highest levels of confidentiality and independence, since the user may be absolutely sure that all communications received will be processed.

The Criminal Compliance Committee is the body responsible for receiving and handling the enquiries and reports through the platform and in accordance with these Regulations, and, if necessary, may be assisted in this duty by the Compliance managers in each entity of the Audax Group.

Moreover, the Committee is responsible for handling and managing any other issues about which it may come to know by other means, with legal advice and assistance from an external adviser.

#### **5. Requirements for the report to be accepted for processing and reasons for its dismissal**

A report shall be accepted only when it meets all the following requirements:

- The report is filed by any of the persons specified in section 2.
- The reported person is one of the persons specified in section 2.
- The reported act is one of the acts specified in section 3.

Likewise, a report may be dismissed for one of the following reasons:

- Reports made by, or concerning, groups other than those determined as users of the Whistleblowing Channel (e.g. complaints made by clients or concerning clients will not be accepted).
- Reports filed by an intermediary (e.g. a report filed by a union member on behalf of an employee).
- Reports on non-reportable issues, which do not imply any unlawful or unethical act (e.g. I'm unhappy with my job).

- Reports made evidently in bad faith<sup>4</sup>.
- Reports without basis in suspicions or particular or specified indications (e.g. I have a distrust of X's conduct).

## **6. Protection of the whistleblower and of the reported person. Personal data protection. Whistleblowing Channel Guarantees**

### **6.1 Prohibition of retaliation**

Users who make any kind of enquiry or report, provided that they act in good faith, are protected against any form of retaliation, threat, extortion, discrimination or punishment in connection with the reports they made. Audax will punish any form of retaliation against the user acting in good faith.

The prohibition of retaliation referred to in the preceding paragraph shall not prevent the adoption of appropriate disciplinary measures if internal investigation shows that the report is false and that the user who made it was aware of its falsehood and, therefore, acted in bad faith.

### **6.2 Personal data protection. Confidentiality and possible anonymity of the whistleblower**

This Whistleblowing Channel is designed in full compliance with diverse legal requirements concerning data protection in order to duly protect the privacy and secrecy of the persons concerned, and particularly in order to guarantee the confidentiality of the reporting person.

Thus, Audax fully complies with the following regulations:

- (i) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (hereinafter: "General Data Protection Regulation"),
- (ii) Spanish Organic Law 3/2018 of 5 December 2018, on the Protection of Personal Data or equivalent regulation in the case of foreign countries, and
- (iii) other implementing regulations which may be applicable.

Likewise, for the purpose of designing this Channel, Audax has also taken into account certain aspects specified 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 Union law.

With respect to the above, this Channel allows the reporting persons to make their reports anonymously or under their real name, so the reporting person may freely choose between anonymity and identification. In such case Audax will ensure the confidentiality of the whistleblower, and for that purpose, among other measures, the exercise of the right of access by the reported person will not involve access to the

---

<sup>4</sup>In this respect, it should be stated that, according to the provisions of article 456 et seq. of the Spanish Criminal Code, an accusation, false report and fraudulent deception of a criminal offence are considered crimes and are punishable by imprisonment of up to two years.

identity of the whistleblower. Therefore, and with the exception of cases expressly regulated, the reported person shall not know the identity of the whistleblower.

However, whistleblowers are encouraged to identify themselves and thus help the organisation obtain more information about the reported issues. At all events, maximum confidentiality regarding identity must be guaranteed to the person making the report until any such time as they choose to identify themselves.

Moreover, (i) the persons who, because of the position they hold in Audax, have knowledge of the reports made, as well as (ii) members of the Criminal Compliance Committee, or (iii) external advisers - are all expressly required to keep secret the identity of the whistleblower as well as any other information they may obtain through the Channel.

Privacy rules applicable to the Channel are specified in the «**Whistleblowing Channel Privacy Policy**», attached to these Regulations as **Appendix II**.

### 6.3 Incompatibility and/or conflict of interest

If any of the persons involved in a report are related by kinship or by marriage to any of the persons involved in the management, investigation or resolution of the reported issue, the latter shall be excluded from the process in accordance with the provision of section 7.8.

### 6.4 Rights and obligations of the whistleblower

The **whistleblower** has the following **rights**:

- The right to be protected from retaliation, providing that the whistleblower acts in good faith as stated in section 6.1.
- The right to confidentiality and anonymity as stated in section 6.2.
- The right to be informed about acceptance or dismissal of the report and the result of possible investigation.
- Lastly, any and all rights concerning personal data legally guaranteed in the Privacy Policy of the Whistleblowing Channel.

On the other hand, the **whistleblower** has the following **obligations**:

- To act in good faith.
- To provide the data and the documents which are in their disposal and are connected with the reported issues.
- Duty of confidentiality: as far as possible, maximum confidentiality is required throughout the processing of the report.

## 6.5 Rights of the reported person

- The right to be informed about the report filed against them, as soon as appropriate verification has been carried out and the document has been accepted for processing; if the report has been dismissed, revealing the information to the reported person is optional.

As a general rule, Audax will inform the reported person about the report filed against them within one month from receiving the communication. However, exceptionally, and only if it is justified, such information may be withheld for another two months (therefore, for a maximum time of 3 months) or even not be given at all if revealing it could seriously jeopardise the success of the investigation.

- The reported person has also the right of access to their personal data and to the information about the subject of the report, except for the identity of the whistleblower and of other persons affected by the report.
- The right to be informed about the resolution of the case if the report was accepted and investigated.
- Lastly, any and all rights concerning personal data legally guaranteed in the Privacy Policy of the Whistleblowing Channel.

## 7. Procedure for the handling of enquiries and reports

### 7.1 Procedure for handling enquiries

Upon receiving an enquiry through the platform, the Criminal Compliance Committee shall resolve it in writing, as far as possible, within 4 working days. In order to resolve the enquiry, the Criminal Compliance Committee shall be assisted or advised by other departments of Audax or by external experts, whose assistance they may consider necessary to achieve an accurate and appropriate resolution in reasonable time.

### 7.2 Procedure for handling reports. Lodging a report. Receipt and acceptance. Follow-up

#### A) Lodging a report

Once the form has been filled in by the reporting person in writing or by voice recording, the report is created.

If the reporting person, in order to register their report, 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.

The reporting person, when submitting the report to the platform, may set up an **email account** in case of future wish to send further communications or add information and/or documents.



A **PIN** code associated with the report will also be created. It is necessary for the reporting person to memorise or save the PIN code for an appropriate follow-up of the report.

### **B) Receipt and acceptance of the report**

When a report is registered, the Criminal Compliance Committee receives an email informing about a new report with a file number assigned, regardless of whether the case might be later dismissed or closed.

Subsequently, the Criminal Compliance Committee accesses the Channel platform in order to carry out a preliminary analysis of the reported issues. For this purpose, the Committee shall be assisted by other departments of Audax or by external experts. The Committee decides then whether to initiate the investigation or to dismiss the report accordingly, and therefore the following options are possible:

- **The report is dismissed:** if the report does not meet the established formal requirements or there exists one of the reasons for its dismissal specified in section 5.
- **The report is accepted for processing and investigation is initiated:** when the report meets the established formal requirements and the reported issues are of necessary importance, the Criminal Compliance Committee decides to accept the report for processing and to initiate the investigation.

In any case, the Criminal Compliance Committee shall, within **7 working days**, send an acknowledgement of receipt to the reporting person, unless a longer period is required for justified reasons.

Likewise, every person who has been the subject of a report, except for the reports that have been dismissed, shall receive the following information:

- the receipt of the report;
- the act of which they are accused;
- the handling of the report by the Criminal Compliance Committee;
- the processing of their data, its purpose and the persons who have access to that data.

Exceptionally, if the Criminal Compliance Committee considers that by notifying the reported person they could compromise the investigation, such notification may be postponed until that risk disappears. In any event, the reported person must be notified within **one month** from the receipt of the report, with the possibility of extending this time limit to a maximum of **three months** if 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.

### **C) Monitoring of the report by the reporting person**

As it has been mentioned in section A, for the purpose of monitoring of the report, the whistleblower may access the platform in order to check the processing stage the report. For that purpose it will be necessary to enter the PIN code in the corresponding section. The processing stage includes the acknowledgement of receipt referred to in the previous subsection, unless the reporting person has provided an email address to which such communication can be made.

### 7.3 Investigation of the reported issues

If an investigation is initiated, the Criminal Compliance Committee shall delegate to one of its members (who must not be involved in the reported issues, in which case see section 7.8 below) the carrying out of necessary verification in order to confirm the veracity and reality of the reported conduct, being authorised to delegate these and other responsibilities to an external adviser for the purpose of achieving a higher level of confidentiality and independence. The investigation shall seek to answer the following questions:

- What is the reported conduct;
- Who are the persons responsible for that conduct;
- The time when the conduct took place;
- To what extent that conduct is connected with a breach of internal regulations;
- What are the consequences of the irregular conduct and, in particular, whether it may be a cause of criminal liability for Audax;

For this purpose, the procedure for the handling of reports, regardless of their nature, shall be governed by the following principles which must be observed and respected at all times by the Criminal Compliance Committee, as well as by any external person involved in the investigation:

- Guarantee of the integrity of the evidence and respect for the law, in particular, respect for the rights of the person under investigation.
- Guarantee of the confidentiality and protection of the privacy and dignity of the persons involved, ensuring at all events the protection of the identity and personal data of the whistleblower.
- Priority and urgent processing, if necessary.
- Thorough investigation of the facts and, if needed, led by specialised professionals.
- Guarantee of action by taking the necessary steps including, where appropriate, disciplinary measures against the person or persons whose offensive behaviour is proven, as well as against those who make false allegations or reports acting in bad faith.
- Protection from retaliation ensuring that no adverse treatment or negative effect on a person will take place as a consequence of their reporting in any way their concern in order to prevent an offensive situation and initiate these proceedings (without prejudice to the disciplinary measures which might be taken in case of false reports).
- Guarantee that the harassed person may remain in their post on the same conditions, if that is what they wish.

In any event, 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.

In compliance with the above principles and guarantees, the Criminal Compliance Committee shall carry out the investigative measures it deems necessary to confirm the veracity and reality of the reported conduct. For that purpose the Committee may use, always with respect to the rights of the persons involved, the necessary means and, in particular, the following:

- Interview with the reporting person: it is advisable, whenever possible and when the report is not anonymous, to meet with the reporting person in a secluded place and explain the investigation process highlighting the absence of retaliation for reports made in good faith. Minutes shall be taken of each meeting, and shall be signed by all the persons in attendance at the meeting.
- Interview with the reported person: such meeting shall take place as soon as possible after necessary information from other sources has been gathered. Minutes shall be taken of each meeting, and shall be signed by all the persons in attendance at the meeting.
- Interview with the witnesses: those who may have reliable information about the facts which are being investigated. Minutes shall be taken of each meeting, and shall be signed by all the persons in attendance at the meeting.
- Documents and electronic records: including emails, agendas and files, only if they are in the corporate electronic media owned by Audax and made available to the employees for work-related use (e.g. corporate e-mail, corporate telephone, etc.), all in accordance with the applicable policy of ICT systems and media.
- Paper documents: must be referenced with a unique number and stored securely in physical or electronic form. They may include: company policies and procedures, invoices, reports, expense settlements, performance appraisals, etc. If such documents are kept in places for exclusive use of the reported person within the workplace (such as lockers, personal belongings, etc.), the search shall take place during working hours and in the presence of a workplace representative or, if not available, another employee.
- Security system logs: such as video surveillance recordings, in accordance with ICT systems and media policy and, in particular, video surveillance in the workplace.

#### **7.4 Motion for a resolution**

Once the investigation has been completed within a maximum period of 30 calendar days, the member of the Criminal Compliance Committee in charge of the investigation shall inform the remaining members of the results obtained so that the Criminal Compliance Committee can decide by majority of its votes the motion for final decision to be made by the Audit Committee, which may consist in the closure of the proceedings or, otherwise, the measures to be applied in each case. The motion for

resolution shall be drawn up within 15 calendar days from the completion of the investigation.

The Criminal Compliance Committee shall decide on closing the proceedings if the reported issues have not been sufficiently confirmed or if such issues are finally considered not to constitute a breach included within the objective scope of the Whistleblowing Channel.

Otherwise, if the Criminal Compliance Committee considers that the reported issues have been sufficiently confirmed, it will issue a justified decision indicating the legal measures of any kind to be taken (including corrective actions, improvements in the system to prevent similar situations in the future, and others).

At any point of the procedure the Criminal Compliance Committee 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).

#### 7.5 Decision on the measures to be taken

In order to ensure the objectivity and independence of the decision, the body authorised and empowered to make the decision is the Audit Committee of Audax Renovables, S.A., which shall be duly informed by the Criminal Compliance Committee about the issue, the result of the investigation and the proposed resolution, whether the issue is a minor breach, a serious breach or a very serious breach, as set out in the previous paragraph.

In the case of a report concerning a minor breach, the Criminal Compliance Committee, in cooperation with the area of Human Resources, may decide what measure shall be taken.

#### 7.6 Implementation of the measures

The sanctions and disciplinary measures will be implemented by the department of Human Resources, and the Criminal Compliance Committee shall keep record of the measures implemented.

#### 7.7 Special procedure for the handling of reports on moral harassment (mobbing), sexual harassment or gender-based harassment

If a report on any kind of harassment is received and accepted in accordance with the provisions of section 7.2 above, the procedure specified in sections 7.3 to 7.6 above shall be initiated with the special procedural features described below, and shall be carried out under the direction of the Human Resources Manager assisted by a member of the Criminal Compliance Committee:

- a) **Preliminary procedure:** Upon receipt of information on a situation of harassment, a preliminary procedure shall be initiated automatically with the aim to resolve the problem immediately.

At this stage, the Criminal Compliance Committee shall interview the parties in order to clarify the facts and find a solution accepted by both parties, taking minutes of each meeting, which must be then signed by the persons in attendance. In the event that, after 10 working days from the beginning of the preliminary procedure, no solution has been reached, the preliminary procedure shall be closed with due closing report and the formal procedure will be initiated.

- b) **Formal procedure:** It shall begin with the opening by the Human Resources manager of an inquiry, during which all the evidence deemed necessary may be examined for the purpose of clarifying the reported facts using among others the means expressly referred to in section 7.3 above.

Within 30 calendar days, which is the time limit of the investigation, the Human Resources Manager shall draw up a written account containing the description of the reported facts, their circumstances and intensity, the repetitiveness of the conduct and the degree to which the situation affected the professional duties and working environment of the alleged victim. At all events, the account must contain the opinion of the investigating party about the veracity of the allegations, and an explanation of the facts which have been objectively confirmed through the actions carried out within the procedure.

- c) **Precautionary measures:** During the proceedings, the Criminal Compliance Committee together with the Human Resources Department and at the request of the Human Resources Manager may, at their discretion, take necessary precautionary measures in order to achieve immediate cessation of the situation of harassment, if such measures do not imply any deterioration of the working conditions of the persons involved.
- d) **Assistance to the parties:** During the proceedings, the parties involved may be assisted and accompanied by a trusted person, who must keep in secret the information obtained in the process. Such person may be present at statement taking and at the communications made by the investigating party to the persons involved. A workplace representative, if there is any, shall also be present at the proceedings.
- e) **Completion of the proceedings:** Within a maximum period of 15 calendar days from the end of the investigation, the Criminal Compliance Committee together with the Human Resources Department shall take the necessary corrective measures, depending on the seriousness and importance of the verified facts, of which it shall give account to the Audit Committee. At all events, if any kind of harassment or an act of bad faith is confirmed, appropriate disciplinary measures provided for in applicable regulations shall be applied.

### 7.8 Special procedure for the case of a report affecting a member of the Criminal Compliance Committee

If, after reading the report or the preliminary analysis of the report, it is concluded that it concerns a member of the Criminal Compliance Committee as a participant or collaborator in any way in the reported issues, as well as in the cases referred to in section 6.3, the special procedure shall be activated. This procedure differs from the ordinary one only in terms of who is involved in the handling of reports:

- **In the case when one of the members of the Criminal Compliance Committee is involved:** the report shall be handled by some other member of the Criminal Compliance Committee, and the member involved in the issues shall be removed from the proceedings, and the access to the Channel in connection with that specific report shall be blocked for that specific member throughout the investigation process of the case.
- **In the event when all the members of the Criminal Compliance Committee are involved:** the report shall be immediately transferred to the Human Resources Management as the body responsible for handling the report with the assistance of an external and impartial third party.

Later on, the process will follow the same guidelines as in the case of reports in which no member of the Criminal Compliance Committee is involved, in accordance with the previous provisions.

## 8. Registering and filing

All the communications (enquiries and reports) received, as well as the responses and related documents must be duly registered and filed. The aforementioned documentation must be kept for a minimum 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 Criminal Compliance Committee 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 this Channel.

## 9. Principles of action and security measures

The validity of the evidence obtained and the actions of the Criminal Compliance Committee and other departments and persons involved in the investigation shall be in line with the following constitutional principles and rights:

- The right to an effective remedy before a court.
- The principle of presumption of innocence.
- The right to due process.

The Criminal Compliance Committee shall be in charge of the safekeeping and filing of the reports received, and will ensure that all the necessary technical and organisational measures are taken in order to maintain the confidentiality and security of the data collected and prevent unauthorised disclosure or access to the data, in accordance with the provisions of Title VIII of the Regulation implementing the Organic Law on Data Protection.

## Appendix I - Issues which may be reported through Whistleblowing Channel

The issues which may be reported through the Whistleblowing Channel of the Audax Group include:

1. Any breach of applicable law. Specifically, any conduct which may constitute moral harassment (mobbing), sexual harassment or gender-based harassment, defined as followed:

- **Moral harassment (mobbing):** Any abusive conduct or psychological violence carried out for a prolong period of time towards a person in the workplace, manifested through repeated behaviour, acts, orders or words whose purpose is to discredit, offend or isolate the person in order to provoke job abandonment and causing progressive and continuous damage to the person's dignity or psychological integrity. Aggravating circumstance is considered to be the fact that the harassing person has some form of hierarchical authority in the structure of the company over the harassed person.
- **Sexual harassment:** According to the provisions of article 2.1.d) of Directive 2006/54/EC of the European Parliament and of the Council of 5 July 2006 on the implementation of the principle of equal opportunities and equal treatment of men and women in matters of employment and occupation (hereinafter: "**Directive 2006/54/EC**") and article 7 of Organic Law 3/2007 of 22 March 2007 on effective equality of women and men (hereinafter: "**OL 3/2007**"), sexual harassment is defined as a situation in which any any verbal, non-verbal or physical behaviour of sexual nature occurs for the purpose or with the effect of violating the dignity of a person, especially when an intimidating, hostile, degrading, humiliating or offensive environment is created.
- **Gender-based harassment:** In accordance with article 2.1 c) of Directive 2006/54/EC and article 7 of OL 3/2007, gender-based harassment is defined as any conduct related to the sex of a person occurs with the purpose of the effect of violating the dignity of that person and creating an intimidating, degrading or offensive environment.

2. Any breach of the principles and standards of conduct established in the Code of Ethics.

3. Offences legally typified in the Criminal Code and crimes specified in other special laws, which may result in criminal liability for Audax, such as:

**Bribery:** Offering or giving to officials, authorities, agencies and public administrations a gift or compensation, economical or of any kind, with the intention of obtaining a benefit for Audax, whether lawful or unlawful.

**Influence peddling:** Influencing by taking advantage of any situation arising from a personal relationship, in order to obtain a decision which might generate, directly or indirectly, an economic benefit for Audax.

**Corruption in business:** When a member of the management, a director, an employee or a business partner of Audax, either themselves or through intermediaries, receives, requests or accepts an unjustified benefit or advantage of any nature, for themselves or for a third party, as a consideration in order to give an unfair advantage to another party in the purchase or sale of goods or services or in business relations. Otherwise, promising or granting a benefit to a third party for the purchase or sale of goods in business relations.

**Corruption in international transactions:** Offering or granting undue benefit or advantage to a public officer in order to secure favourable treatment in carrying out international business activity.

**Embezzlement:** disloyal management and misappropriation of public funds. Fraudulent accounting of a public entity, of the documents which should reflect the financial situation or of the information contained in such documents. Providing false information about the financial situation of a public entity.

**Scam:** Deceiving another for profit, persuading them to dispose of property to the detriment of themselves or of third party.

**Misleading advertising:** Offering or advertising products or services with false claims made regarding their features, so that they may cause serious and manifest harm to consumers.

**Discovery and disclosure of trade secrets:** Appropriation, by any means, of data, written or electronic documents, digital media or other items which constitute confidential information of another company, entity, etc., in order to use, publish, disclose or transfer such information.

**Subsidy fraud:** Obtaining subsidies or aid from Public Administration of an amount or worth more than €120,000 by distorting the conditions required, through concealing the circumstances which would impede the granting of the subsidy or aid.

**Public Treasury Fraud:** Defrauding the Public Treasury (state, autonomous, regional or local) in the amount greater than €120,000; by evading the payment of taxes, amounts withheld or which should have been withheld or income on account of remuneration in kind, improperly obtaining refunds or enjoying tax benefits in the same way.

**Social Security Fraud:** Avoiding the payment of Social Security fees by improperly obtaining returns or by unfairly enjoying deductions.

**Non-compliance with financial reporting obligations, and false accounting:** Serious breach of the obligation to keep commercial accounts and/or accounting records. This type of offence usually is associated with other fraudulent conduct, as it is usually perpetrated through double counting and false accounting entries.

**Offences against natural resources and the environment:** Causing or facilitating, directly or indirectly, emissions, spills, radiation, extractions, excavations, burying, noises, vibrations, injections or dumps, into the atmosphere, soil, subsoil or into inland waters, subterranean waters, seas or oceans; creating tanks or dumping sites for any refuse or liquid or solid waste which may be toxic or dangerous and may seriously damage the balance of natural ecosystems or be detrimental to human health.

**Frustration of enforcement:** Performing any act of disposal of property or liability-creating transaction, which hinders or prevents the carrying out of seizure and confiscation or monetary claim proceedings. Concealing property in judicial or administrative enforcement proceedings. Using without authorisation of the receiver the goods seized by authorities.



**Punishable insolvency:** On the assumption that Audax went to administration, this offence would be committed by carrying out a transaction of disposal of assets in order to unduly reduce the equity, which secured the payment of the liabilities, or by hindering or preventing the creditor from getting information about the true financial situation of the debtor.

**Offences against intellectual property:** Reproducing, plagiarising or publishing, whether in whole or in part, a literary work (a book), an artistic work (a picture or a photography) or scientific work (a specific theory, computer software) or its transformation, interpretation or artistic performance fixed on any kind of medium or published through any kind of medium, without authorisation of the owner of the rights. For instance, this offence is applicable to the cases when computer software is used without due licence.

**Offences against industrial property:** Reproducing, imitating, etc. a distinctive sign without permission of the owner, so that other sign, identical or similar, is achieved, in order to distinguish the same or similar products, services, activities or establishments.

**Cybercrime:** Erasing, damaging, deteriorating, suppressing or making inaccessible data, computer programmes or electronic documents of others, without permission and when the result produced is of a serious nature. Impeding or hindering the operation of computer systems of others.

**Planning breach:** Carrying out infrastructure construction works or building construction works without permission, on the land intended for roads, greenery, public property or places of officially recognised natural, ecological, artistic, historical or cultural value, or places which have been given special protection for the above reasons.

**Offences against personal and family privacy:** Appropriating, using or modifying, without permission and to the detriment of others, private personal or family data of others, recorded in computer, electronic or telematic files or media or in any other public or private archive or register. Accessing illicitly computer systems in order to appropriate personal data contained therein.

**Against the rights of foreign citizens:** Promoting, encouraging or facilitating illegal trafficking or illegal immigration.

**Money laundering:** Accepting funds, deposits, etc. of criminal origin, or acting in any other way to conceal such illicit origin, or to assist a person who participated in the offence. May be committed recklessly due to acting without due diligence, meaning that it is not necessary for the perpetrator to act willingly and knowingly for the crime to be committed.

**Financing of terrorism:** Providing, collecting or accepting funds to be used to commit crimes related to terrorist organisations and groups.

**Offences against public health:** Offering on the market products which are harmful to health and/or do not meet the expiration or composition requirements established by laws or regulations. Also, developing substances which are harmful to health, dispatching, supplying or trading such substances.

**Against workers' rights:** Seriously endangering the workers' life, health and safety due to violation of occupational risk prevention rules. This criminal offence may be committed recklessly. Using deception or abusing a situation of necessity in order to impose working conditions or Social Security terms which harm, suppress or restrict the workers' rights. Enforcing working conditions which are inadequate or contrary to health and safety in the workplace; treating workers on terms of inequality and discrimination; preventing or limiting the freedom of association.

**Stock fraud:** Using or providing any information significant to the quotation of any kind of financial instruments. Disseminating information or rumours about persons or businesses while being aware of their falsehood, with the aim of altering or preserving the price of securities or financial instruments. Falsifying economic and financial information presented in the issue prospectus of any financial instrument.

**Handling of toxic, corrosive or other substances:** Contravening safety regulations established for the manufacture, handling, transport, possession or trading of explosive materials, substances which are flammable, corrosive, toxic or asphyxiating, by exposing life, bodily integrity or health of persons or the natural environment to real and present danger.

**Forgery of credit card, debit card or travel cheque:** Altering, copying, reproducing or falsifying credit cards, debit cards and travel cheques.

**Illegal funding of political parties:** Making illegal donations or contributions to a political party, federation, coalition or group of electors.

**Fraudulent invoicing:** Altering or tweaking automatic devices for measuring the cost of goods sold or services offered (meters, taximeters, etc.) with the aim of invoicing higher amounts to the detriment of the consumer.

**Prostitution and corruption of minors:** Forcing an adult person to practice or continue to practice prostitution by using violence, intimidation or deception, or by abusing a situation of authority, or necessity, or vulnerability. Inducing to, promoting, supporting or facilitating the prostitution of a minor or of a person with disability in need of special protection, or profiting from that, or exploiting in any way a minor or a person with disability for such purpose. Requesting, accepting or obtaining, in return for a remuneration or promise, a sexual intercourse with a minor or with a person with disability in need of special protection. Producing, selling, distributing etc. child pornography.

**Price alteration in competitions and public tenders:** Requesting a benefit in return for not taking part in a competition or public tender, trying to remove other bidders from such competition or tender by using threats, gifts, promises or any other artifice, colluding with other bidder to change the amount of the bid, or fraudulently abandoning a tender after winning it.

**Piracy of broadcasting or interactive services:** Acceding or facilitating access (without permission of the service provider) to a sound or television broadcasting service or interactive service provided remotely and electronically. Changing or duplicating the identification number of telecommunications devices, or selling devices which have been fraudulently tweaked. Using devices or programmes which allow unauthorised access to conditional access services or telecommunications equipment.

## Appendix II - Privacy Policy

---

### *Basic Legal Information (first layer information)*

The personal information collected through this Whistleblowing Channel shall be processed by «Audax Renovables, S.A.», as the entity legally responsible, for reasons of public interest, with the intention of avoiding any possible breach or illicit act.

Unless legally required, the information will not be disclosed to any third party outside the Company nor to any person inside the organisation who is not duly authorised to know or access the information.

The parties involved in the reports or enquiries received may exercise their legal rights with regard to Privacy, as well as learn in due detail all the additional legal information by accessing [dpo@audaxrenovables.com](mailto:dpo@audaxrenovables.com), or through this [Privacy Policy](#).

### *Additional Legal Information (second layer information)*

#### *Privacy Policy*

#### 1. OBJECTIVE

The objective of this Privacy Policy is to inform about legal terms of processing the personal data collected as a consequence of the reports and enquiries submitted through the Whistleblowing Channel of Audax Renovables.

For the purpose of correct configuration and design of this Whistleblowing Channel, Audax Renovables fully adheres to the applicable laws concerning personal data protection; and in particular:

- (iv) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (hereinafter: "General Data Protection Regulation"),
- (v) Spanish Organic Law 3/2018 of 5 December 2018, on the Protection of Personal Data, and
- (vi) other implementing regulations which may be applicable.

Although it has not yet been transposed to the national legislation, Audax has also taken into account certain aspects specified 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 Union law.

#### 2. CONTROLLER OF THE COLLECTED PERSONAL DATA PROCESSING

The entity legally responsible for processing the data gathered through the Whistleblowing Channel is the company «Audax Renovables, S.A.» (hereinafter referred to as «the Company», «Audax», or «Audax Renovables», interchangeably).

Company contact details:

- Postal address: Av. Navarra, 14, 08911 Badalona (Barcelona).
- Tel. +34.93.240.53.06
- e-mail: [info@audaxrenovables.com](mailto:info@audaxrenovables.com)

### 3. ORIGIN OF THE PERSONAL DATA WHICH ARE SUBJECT TO PROCESSING

The Whistleblowing Channel may process personal information of the whistleblower and of the reported person as well as of third parties involved in the issues which are the subject of the enquiry or report (e.g. possible witnesses).

Audax may receive such personal data:

- a) directly from the data subject (for providing the data at the moment of filing their report or enquiry, when making possible claims or at any other moment during the investigation); and
- b) indirectly, by any other person, whether natural or legal, involved in the investigation, or by the companies belonging to the Audax Group, if the person works or provides services in any of them.

When Audax receives personal information indirectly, as a proof of transparency, the data subject is informed immediately about it, and especially about the origin of the data and the category of the information received.

### 4. PURPOSE AND LEGALITY

In compliance with the European General Data Protection Regulation, it is hereby stated that the Whistleblowing Channel has a triple purpose, each of them based on the relevant legal grounds:

#### a) Criminal risk prevention, as a mission of public interest

Firstly, the personal data gathered through the Whistleblowing Channel shall be processed with the aim of (a) handling and managing the enquiries and reports received, (b) investigating the reported issues, if necessary, (c) clarifying and obtaining evidence of the facts in order to pursue legal action, if applicable, (d) ensuring necessary protection of the whistleblower in order to prevent possible retaliation.

This data processing shall be carried out with the aim of fulfilling a mission of public interest, which is the prevention, detection and discovery of possible risks and violations of criminal laws within the organisation, which could result in criminal liability of Audax as a legal person.

#### b) Obtaining evidence of the correct operation of the Criminal Risk Prevention Model, in the legitimate interests of Audax

Moreover, personal data may be processed within the Whistleblowing Channel for the interest of Audax in obtaining evidence of the correct operation of its Criminal Risk Prevention Model.

This shall be carried out because of the concurrence of the legitimate interests of Audax, which do not cause any harm or damage to the privacy of the data subject, and of the latter, whose legitimate interest is for the Company where they work or provide services to have and implement an appropriate and efficient Criminal Risk Prevention Model.

#### c) Other possible purposes which may be legally binding:

Lastly, in some cases, personal data may also be processed for the purpose of complying with certain legal obligations which may be applicable to Audax. In such cases, as far as possible, the data subject will be notified and informed about the grounds of the legal obligation.

## 5. STORAGE PERIOD FOR THE COLLECTED PERSONAL DATA

The personal data of the reporting person, of the reported person and of other persons who may be named in the report or may be involved in the investigation (e.g. Suppliers, Clients or other employees) will be processed by Audax:

- a) for the time needed to establish whether the investigation should be launched into the reported issues,
- b) for the duration of the relevant investigation, if launched, and lastly,
- c) for the duration of the pertinent legal action.
- d) In the case of an individual enquiry, for the time needed to manage, process and respond to it.

Subsequently to that, Audax will store the data (i) duly secured, and solely and exclusively for the purpose of (ii) meeting any legal obligations which may apply, as well as (iii) addressing any complaints and responsibilities, still duly secured and for the maximum legally defined period, and made available to Mossos d'Esquadra, law enforcement agencies and forces, courts and tribunals, and competent public administration entities.

## 6. TO WHOM THE PERSONAL DATA COLLECTED WILL BE DISCLOSED?

As a general rule, Audax will not share with any third party the data collected through the Whistleblowing Channel. The data will be accessed only by the employees of Audax who, because of their duties, responsibilities and assignments within the Company, have been duly and previously authorised.

However, there are some exceptions to this general rule. Accordingly:

- a) Firstly, the data may be disclosed by Audax under legal obligation to third parties, e.g. to the courts and tribunals, to Mossos d'Esquadra, to law enforcement state agencies or any authorised public entity.
- b) If, as a consequence of an investigation carried out, a decision is made to take legal action against an **employee of the Audax Group**, the employer of the worker will be provided with the information strictly necessary for the implementation of pertinent measures.
- c) Moreover, Audax may be assisted by **third-party service providers**, who may have access to such personal data and shall process the data in their own name and on their own behalf.

With regard to the above, it is hereby stated that **Audax applies strict criteria for the selection of providers in order to fulfil its obligations concerning data protection**. Therefore, in order to regulate the privacy terms on which those possible third-party providers shall act, Audax undertakes to sign with them a pertinent agreement on data processing, under which they will acquire the following obligations: to apply appropriate technical and organisational measures; to process the personal data for the agreed purposes and following only the documented guidelines of Audax; and to erase or return the data when services are no longer being provided.

In accordance with the above, Audax may sign agreements on service provision with third-party service providers of the following areas, among others: legal services, multidisciplinary professional services, information technology services.

In such cases of engagement of third-party service providers, in the agreement signed with them the following obligations will be expressly established:

- The provider, as a data processing controller, shall follow strictly and punctually the instructions issued by Audax.
- The controller must not use the data for any other purpose.

- The controller shall implement the technical and organisational security measures in order to guarantee the confidentiality of the information to which they will have access.
- The controller must not disclose to third parties the data collected within the administration of the Whistleblowing Channel, not even for its maintenance.

The actions mentioned above will not involve the transfer of personal data outside the European Economic Area, therefore no international transfer of data will take place. However, if exceptionally it is necessary to carry out any action which could involve international transfer, Audax shall at any time fully and strictly comply with all the obligations of information and authorisation established by applicable law at the time, so that personal privacy is duly safeguarded and protected.

## 7. EXERCISING OF RIGHTS

The persons whose personal data may be processed within the framework and context of the Whistleblowing Channel shall have the following rights:

- a) The right to obtain information whether or not their personal data are being processed in Audax, within the framework of the Channel management, as well as to access, rectify, restrict the processing of their data or, if applicable, request the erasure or the data on legally established terms.
- b) Under certain circumstances, the right to object to processing of their personal data.
- c) They shall also have the right to lodge a complaint with the Data Protection Agency (as the competent supervisory authority for data protection), especially if they were not able to exercise satisfactorily their rights by:
  - a letter sent to the Data Protection Agency, c/Jorge Juan, 6 28001-Madrid,
  - or through the website <https://www.aepd.es>

If the person concerned does not reside in Spain or, in any event and for any reason, wishes to lodge their claim with any other national supervisory authority from among those of the European Union, they have also the right to do so. For information on the location and contact details of such national authorities, click [here](#) (see section «*Making a complaint*»).

## 8. DATA ACCESS RESTRICTION

The access to the data gathered in the Whistleblowing Channel shall be limited exclusively to the Criminal Compliance Committee, the Human Resources and the Audit Committee or other areas which might be strictly necessary for the investigation of the issues, only within the strict scope of their competences in accordance with Audax's Criminal Risk Prevention Model.

Moreover, as it has been already stated, access to the data shall also be granted to third-party professionals, to whom Audax may assign the provision of certain services connected with the management of the Whistleblowing Channel.

## 9. PRINCIPLE OF PROPORTIONALITY AND OF DATA MINIMISATION

The personal data collected within the Whistleblowing Channel:

- shall be limited to those which are **strictly and objectively necessary** for the purpose of handling the reports and, if appropriate, of verifying the reality of the reported issues;
- shall be processed at any time in accordance with the applicable regulations on data protection, **for legitimate and specific purposes** connected with the investigation which may arise as a consequence of the report; and
- shall be **adequate and not excessive**. No personal data will be collected which will not be evidently relevant to the handling of a specific report.

## 10. SECURITY AND CONFIDENTIALITY MEASURES. POSSIBLE ANONYMITY OF THE WHISTLEBLOWER

Audax shall ensure that all the necessary technical and organisational measures are taken to maintain the security of the data collected in order to protect them from unauthorised dissemination or access.

In this regard, whistleblowers may decide whether or not to identify themselves when making a report. However, whistleblowers are encouraged to identify themselves and thus help the organisation obtain more information about the reported issues. At all events, maximum confidentiality regarding identity must be guaranteed to the person making the report until any such time as they choose to identify themselves.

Moreover, and as a measure to ensure the confidentiality of the whistleblower, it is hereby expressly stated that the exercising of the right of access by the reported person will not imply automatically their access to the identity of the whistleblower.

However, as an exception to the above, provided that there is a reasonable justification of sufficient significance and it is necessary to the protection of the right of defence of the person concerned, or where it is legally appropriate, the reported person may be provided with the identity of the whistleblower (*as well as any other information which may directly or indirectly be used to deduce their identity*).

The disclosures made under the exception described in the previous paragraph shall be subject to appropriate protections. In particular, and among other measures which may be implemented, unless such notification could compromise the investigation or the court proceedings, the whistleblower will be notified before their identity is disclosed and will receive a written explanation of the reasons of such disclosure.

Accordingly, it is hereby stated that the identity of the whistleblower shall be known only to the Criminal Compliance Committee, the Audit Committee and the Managers of the areas strictly competent as participants of the investigation and resolution of the reports made. External experts may also have access to such information.

With regard to the above, it is hereby stated that all the persons who, because of their position and duties, have knowledge of the reports made, must maintain confidential the identity of the whistleblower.

## 11. OBLIGATION TO INFORM THE PARTIES INVOLVED

The parties involved in the enquiries or reports received shall be duly informed of the legal terms of privacy on which their personal data will be processed. In order to comply with the above, the Criminal Compliance Committee of Audax:

1. Will implement the necessary mechanism to ensure that the users of this Channel may know and avail - in a simple, accessible, comprehensible manner and of course free of charge - the privacy rules covered by this Policy. This, at all events, before they lodge any possible enquiry or report.

2. Moreover, additionally, each time an enquiry or report is made, the Criminal Compliance Committee shall notify it in particular to the persons involved. However, the above shall be carried out in a personalised manner. Therefore, in this regard, and apart from this Policy being accessible on the Audax employee portal, the following measures will be implemented in order to reinforce and ensure the compliance with such information obligation (with regard to the whistleblower, the reported person or a third party involved):
- **Whistleblower:** The whistleblowers who will identify themselves at the moment of making the report will be informed of the processing of their data in an email sent to confirm the receipt of the enquiry or report, with a link to this Privacy Policy. The above will be carried out within a maximum of 7 working days from the reception of the report.
  - **Reported person:** In the case of the reported person, it will be necessary to assess individually whether informing them about the report made against them might compromise the correct development and success of the investigation. Therefore, if the decision is made to not inform the person concerned in the initial stage of the investigation, such decision must be duly documented and justified.  
In this regard, as a general rule, the reported person will be informed about the report filed against them within a maximum of one month from receiving the communication. However, exceptionally, and only if it is justified, such information may be withheld for another two months (therefore, for a maximum time of 3 months overall) or even not be given at all if revealing it could seriously jeopardise the success of the investigation. This, without prejudice to the involvement which they may eventually have in the proceedings to be carried out.
  - **Any other person concerned, involved in the report or enquiry:** Lastly, the third parties involved in the report or enquiry made, shall be informed before their participation in the proceedings begins: for instance, a possible witness before their interview or hearing.

## 12. DATA PROTECTION OFFICER

Audax has appointed a person within the organisation in order to ensure, among other aspects, that the operation of the Whistleblowing Channel meets all the legal requirements of data protection established in the Spanish and European regulations.

That person is the Data Protection Officer, who shall attend to all the enquiries or claims made as a consequence of, and in connection with, the personal data processing within the Whistleblowing Channel. The email address of the Data Protection Officer is [dpo@audaxrenovables.com](mailto:dpo@audaxrenovables.com).