

WHISTLEBLOWING CHANNEL POLICY

OF

IQANA TECHNOLOGIES, S.L.U.

June 2026

Version and Modification History

Version	Type of revision	Description of the modification	Approving body	Date
V 1.0	Initial approval	N/A	Board of Directors	30/06/2026

Table of Contents

1. Introduction	3
2. Scope of application	3
2.1 Subjective scope: who can report and who can be reported	3
2.2 Objective scope: what can be reported	3
3. General principles	3
4. Whistleblowing channel procedure	4
4.1 Access to the whistleblowing channel	4
4.2 Receipt of reports	4
4.3 Handling of reports	5
4.4 Completion of the investigation	5
5. Whistleblower protection measures	5
6. Protection measures for those reported and affected by the report	5
7. Review of policy and procedure, and entry into force	6
7.1 Approval and supervision	6
7.2 Periodic review and version control	6
7.3 Entry into force	6
8. Protection of personal data	6
9. Glossary	6
Annex. Access to the whistleblowing channel and external channels	7

1. Introduction

Iqana Technologies, S.L.U. ("**Iqana**") is an entity authorised to provide crypto-asset services in accordance with Regulation (EU) 2023/1114 (MiCA), which provides the service of discretionary and individualised management of crypto-asset portfolios under a non-custodial model, and is subject to the supervision of the National Securities Market Commission (CNMV).

Law 2/2023, of 20 February, regulating the protection of persons who report regulatory infringements and the fight against corruption (the "**Law 2/2023**"), which transposes Directive (EU) 2019/1937 into Spanish law, requires the establishment of an internal reporting channel and of protection measures in favour of those who report the actions or omissions referred to in Article 2 thereof. Iqana is obliged to have this channel by virtue of Article 10.1.b) of Law 2/2023, as it falls within the scope of application of European Union acts on financial services and the prevention of money laundering and terrorist financing, regardless of the number of workers it employs.

In compliance with this obligation, Iqana has implemented a **whistleblowing channel**, which constitutes part of its Internal Information System and through which any person within the scope of application of this policy can report infringements of which they become aware. The whistleblowing channel is managed through the "**Ethics Channel**" tool, operated by the specialist provider Whistleblower Software.

The purpose of this Whistleblowing Channel Policy (the "**Policy**") is to set out the general principles and describe the operation of the whistleblowing channel and the whistleblower protection measures, in compliance with Articles 5.2.h) and 25 of Law 2/2023, and to make its existence known so that any interested party can consult it. The Policy has been approved by Iqana's Board of Directors and is published in an accessible manner.

2. Scope of application

2.1 Subjective scope: who can report and who can be reported

In accordance with Article 3 of Law 2/2023, persons who maintain or have maintained an employment or professional relationship with Iqana may file a report through the channel, and in particular:

- a) Persons who have the status of Iqana employees, as well as those who are self-employed providing services for the Entity;
- b) Shareholders and persons belonging to the administrative, management or supervisory body, including non-executive members;
- c) Any person working for or under the supervision and direction of contractors, subcontractors, and suppliers; and
- d) Persons whose employment or professional relationship has not yet begun, when the information has been obtained during the selection process or pre-contractual negotiation, as well as those whose relationship has already ended, volunteers and trainees.

The protection also extends to the legal representatives of the workers, to those who assist the whistleblower, to natural persons related to them who may suffer retaliation (such as co-workers or family members) and to legal persons linked to the whistleblower. Any natural or legal person to whom the actions or omissions reported in the exercise of their activity for Iqana or in relation to it are attributed may be the subject of a report.

2.2 Objective scope: what can be reported

The actions or omissions included in Article 2 of Law 2/2023, i.e. the infringements of European Union law listed therein and the actions or omissions that may constitute a criminal offence or a serious or very serious administrative offence, may be reported through the whistleblowing channel. Especially included, due to the activity of the Entity, are possible infringements in the field of financial services and crypto-assets, prevention of money laundering and terrorist financing, data protection and Iqana's internal regulations.

3. General principles

Iqana's whistleblowing channel is governed by the following general principles:

- **Accessibility:** The channel is accessible to all persons within the scope of application, from any device, and allows reports to be filed anonymously.
- **Transparency:** Iqana makes known the existence and operation of the channel, publishes this Policy and keeps the whistleblower informed of the processing of their report in the terms provided for in the regulations.
- **Good faith:** The channel is directed to those who communicate information with reasonable grounds to believe that it is true at the time of communication, even if they do not provide conclusive evidence; the deliberate communication of false information is excluded.
- **Whistleblower protection:** Those who use the channel in good faith are protected from retaliation and any adverse consequences arising from their reporting.
- **Confidentiality:** The identity of the whistleblower, the reported person and any third party mentioned is safeguarded, as well as the confidentiality of the information provided and the actions carried out, preventing access by unauthorised personnel.
- **Objectivity and impartiality:** Reports are processed objectively and impartially and with the full independence of the System Manager.
- **Conflict of interest:** Persons or areas in respect of which there are present or potential conflicts of interest will not intervene in the processing.
- **Prohibition of retaliation:** Retaliation against those who report in good faith is expressly prohibited; its adoption or attempted adoption may result in disciplinary action.
- **Right of defence:** Throughout the proceedings, the presumption of innocence, honour and the right of defence of the reported person are guaranteed.

4. Whistleblowing channel procedure

The whistleblowing channel is managed by the manager of the Internal Information System (the "System Manager"), a position that in Iqana falls to the Head of Regulatory Compliance, appointed by the Board of Directors. They carry out their functions autonomously and independently, without receiving instructions in the performance of their duties, and have the necessary means to do so. Their appointment and, where appropriate, removal are notified to the Independent Authority for the Protection of Whistleblowers, A.A.I., or to the competent regional authority, within ten working days, in accordance with Article 8.3 of Law 2/2023. The receipt of reports is outsourced to the provider Whistleblower Software, which is considered to be the data processor, without this altering the status of the System Manager. The reports management procedure is structured in the following phases:

4.1 Access to the whistleblowing channel

Reports are submitted through Iqana's whistleblowing channel, accessible at the link in the Annex and managed on the platform of the provider Whistleblower Software, by completing the electronic form provided for this purpose, to which the whistleblower can attach the documentation they deem appropriate. Reports are not addressed to general mailboxes or to individual addresses at Iqana: they are received through the channel, which is only accessed by the System Manager and authorised persons, which reinforces confidentiality and anonymity. The channel allows the submission and subsequent processing of **anonymous reports**, as well as secure and two-way communication between the whistleblower and the System Manager, even when the former remains anonymous. In addition, at the request of the whistleblower, the report may be presented orally through a face-to-face meeting, which will be held within a maximum period of seven days. When submitting the report, the whistleblower may indicate a postal address, an email address or a safe place for the purpose of receiving notifications. Instructions and the link to access the channel are set out in the Annex to this Policy.

4.2 Receipt of reports

An acknowledgement of receipt of the report shall be sent to the whistleblower within seven calendar days of receipt, unless this would jeopardise the confidentiality of the communication. Anyone who receives a report through any means other than the channel or without being responsible for its processing must immediately forward it to the System Manager, maintaining confidentiality.

4.3 Handling of reports

The System Manager shall analyse the report and promote the necessary investigative actions, collecting the relevant information and maintaining, where appropriate, communication with the whistleblower to request additional information. The reported person shall be informed of the actions or omissions attributed to him or her and shall have the right to be heard, in the time and manner deemed appropriate to ensure the successful completion of the investigation. The maximum period for responding to the investigation proceedings shall be three months from the acknowledgement of receipt or, if no acknowledgement has been sent, from the expiry of the seven-day period following the report; in cases of special complexity, it may be extended for up to another three months, in accordance with Article 9.2.d) of Law 2/2023. Where the facts may prima facie constitute a criminal offence, the information shall be sent immediately to the Public Prosecutor's Office and, if they affect the financial interests of the European Union, to the European Public Prosecutor's Office. Reports that are manifestly unfounded or that do not provide new and significant information with respect to a report already handled may be declared inadmissible.

4.4 Completion of the investigation

Once the investigation proceedings have been concluded, a reasoned decision shall be taken and the outcome thereof, as appropriate and without delay, shall be communicated to the whistleblower and the person concerned. Where the facts are substantiated, Iqana will adopt the corresponding corrective or disciplinary measures, without prejudice to the referral of the matter to the competent authorities when appropriate.

5. Whistleblower protection measures

Iqana guarantees the protection of those who report in good faith through the channel, in accordance with the following measures:

- **Prohibition of retaliation:** Those who report in good faith will not be subject to retaliation or suffer any other adverse consequences. Retaliation includes, but is not limited to, suspension or termination of employment, disciplinary measures, demotion or denial of promotions, substantial changes in working conditions, reputational or economic damage, intimidation, harassment, negative references, blacklisting, or any discriminatory or unfair treatment.
- **Confidentiality and anonymity:** The identity of the whistleblower is preserved and will only be shared with the areas whose collaboration is essential for the investigation, and anonymous reporting is allowed.
- **Absence of conflicts of interest:** Only persons and areas in respect of which there are no conflicts of interest will be involved in the processing.
- **Measures against retaliation:** The adoption or attempted adoption of retaliation may lead to the initiation of disciplinary measures in accordance with the applicable internal and labour regulations, without prejudice to other responsibilities.
- **Information on external channels:** Iqana provides the whistleblower with clear and accessible information on the external channels for reporting to the competent authorities, which is set out in the Annex to this Policy.

6. Protection measures for those reported and affected by the report

In the processing of reports, the rights of the reported and affected persons are respected in all cases:

- **Presumption of innocence, honour and defence:** The presumption of innocence, the right to honour and the right of defence of the reported person are guaranteed, preserving his or her good name at all times.
- **Right to information and to be heard:** The reported person shall have the right to be informed of the actions or omissions attributed to him or her and to be heard, in the time and manner deemed appropriate to prevent the destruction, concealment or alteration of evidence and to ensure the successful completion of the investigation.
- **Confidentiality of the identity of the whistleblower:** In no case will the reported person be provided with the identity of the whistleblower or information that allows their identification.

7. Review of policy and procedure, and entry into force

7.1 Approval and supervision

This Policy has been established and approved by the Board of Directors of Iqana, which is responsible for supervising its correct application. The System Manager oversees its application, promotes awareness and publicity of the Policy and adopts the necessary measures for its compliance.

7.2 Periodic review and version control

The Board of Directors reviews the effectiveness of the Policy and the procedure at least annually, or whenever any circumstance makes it advisable to do so (in particular, regulatory changes or changes in the organisation of the channel), and adopts the necessary measures to correct the deficiencies detected. Any material changes will be approved by the Board of Directors and will

be reflected in the version history. Failure to comply with the provisions of this Policy may result in the initiation of the corresponding disciplinary proceedings.

7.3 Entry into force

This Policy shall enter into force on the date of its approval by the Board of Directors, as indicated in the version history, and shall remain in force indefinitely until the Board agrees to amend it or to approve a new policy to replace it.

8. Protection of personal data

The processing of personal data derived from the receipt and management of reports is governed by Law 2/2023 (in particular Title VI), by Regulation (EU) 2016/679 (GDPR) and by Organic Law 3/2018, of 5 December (LOPDGDD), in accordance with the following criteria:

- the processing of personal data in the context of internal reports is lawful under Article 6(1)(c) of the GDPR;
- whistleblowers will be provided with the information required by Articles 13 of the GDPR and 11 of the LOPDGDD; personal data whose relevance is not manifest will not be collected and, if they are collected by accident, they will be deleted without delay;
- access to personal data is limited, within the scope of their competences, to the System Manager and whoever manages it directly; to the person in charge of human resources, when disciplinary measures could be adopted; to the legal services, where the adoption of legal measures is appropriate; to the designated processors; and to the Data Protection Officer, if applicable;
- the data will be kept only for the necessary time and, in no case, for a period exceeding ten years; if three months have elapsed since the receipt of the report without any investigation actions having been initiated, the data will be deleted, unless the purpose of the conservation is to leave evidence of the operation of the channel, in which case they will be recorded in anonymised form; and
- if the information contains special categories of data or data not necessary for the investigation, such data will be immediately deleted.

Iqana keeps a **register** of reports received and internal investigations carried out, which guarantees confidentiality and is not public. Its content may only be accessed at the reasoned request of the competent judicial authority, by court order and within the framework of judicial proceedings. Its retention will not exceed the maximum period of ten years.

9. Glossary

- **Whistleblowing channel:** Iqana's internal reporting channel, integrated into its Internal Information System, through which reports are received and processed.
- **Whistleblower:** A natural person who communicates, through the channel, information about infringements obtained in the context of an employment or professional relationship with Iqana.
- **Reported or affected person:** Natural or legal person to whom the actions or omissions that are the subject of the report are attributed or to which it refers.

- **System Manager:** Person designated by the Board of Directors as responsible for the management of the whistleblowing channel; in Iqana, the Head of Regulatory Compliance. They perform their functions with autonomy and independence.
- **Retaliation:** Any act or omission, direct or indirect, that takes place in the work or professional context, is prohibited by law and entails or may entail harm to the whistleblower as a result of their reporting.
- **A.A.I.:** Independent Authority for the Protection of Whistleblowers, the competent authority for the management of the external reporting channel and the protection of whistleblowers.

ANNEX

Access to the whistleblowing channel and external channels

Iqana whistleblowing channel (internal channel)

Reports may be submitted, even anonymously, through Iqana's whistleblowing channel (Ethics Channel), accessible at the following link:

<https://whistleblowersoftware.com/secure/Canal-etico-Iqana>

External reporting channels

As an alternative to the internal channel, the whistleblower may contact the external channels established by law, in particular the Independent Authority for the Protection of Whistleblowers, A.A.I., and, where appropriate, the competent authorities or bodies of the Autonomous Communities, as well as the institutions, bodies or agencies of the European Union authorised for this purpose.