rauva

RAUVA TECHNOLOGY
Whistleblowing Policy

Portugal, June 2025

Table of Contents

Abbreviations

Abbreviation	Full Form
BoD	Board of Directors
CEO	Chief Executive Officer
CRO	Chief Risk Officer
EU	European Union
HoC	Head of Compliance
HoP	Head of People
MENAC	Mecanismo Nacional Anticorrupção (Anti Corruption Nacional Mechanism)

1. Introduction

1.1 Rauva Technology is a technological services provider that offers, through Rauva App, an interface that allows and aggregates access to financial and enterprise services related to their partners, through APIs, in order to offer a “one-shop” digital solution, so that the client is able to start and manage their business, at the same time they are offered additional tools related to the company.

1.2 Rauva Technology is committed to maintain the highest standards of professional and ethical conduct. In order to achieve the same, Rauva Technology aims to develop a relationship of confidence and trust between itself and its stakeholders, including employees, suppliers and customers. Whistleblowing acts as a mechanism wherein stakeholders are enabled to report any violation or wrongdoing within the organization which may otherwise remain hidden.

1.3 This document is compatible with the local regulatory guidelines applicable to Rauva Technology. No other Rauva Technology policy or procedure shall contradict or supersede any of the statements contained in this policy. In all matters, relevant stakeholders shall follow the guidelines stated in this document along with the regulatory guidelines applicable.

1.4 The owner of this document is the Head of Compliance. Any changes to this document will be initiated by the Head of Compliance and approved by the Board of Directors.

1.5 Following BoD approval, relevant changes will be summarised in the version control table (Change Control) located at the start of this document and the document shall be circulated to all stakeholders by the HoC.

1.6 In case of rejection, reasons for rejection should be specified by the Board of Directors, which would be further taken up by the Head of Compliance for modifications and further re-submission.

1.7 As a minimum, the Whistleblowing Policy will be reviewed by the HoC annually. More frequent reviews can be triggered for various reasons, namely:

- Amendments / introduction of new regulations applicable to Rauva Technology.
- Amendments / introduction of new statutory legal provisions.
- Material change to the Rauva Technology business model and products.

1.8 An audit trail of the various versions of this Policy will be maintained.

2. Policy Statement

2.1 The Whistleblowing Policy (hereafter referred to as “the document” or “the policy”), establishes a framework for treatment (communication, receipt, analysis and conclusion) of any possible irregularity which has been committed, is being committed, or is about to be committed, without being negatively affected and communicated to Rauva Technology in the Whistleblowing Channel.

The purpose of the Whistleblowing Channel is to provide Rauva Technology with a reliable and efficient mechanism that enables adequate safeguards for the treatment of possible irregularities, including its detection, investigation and resolution.

2.2 This document aims to encourage employees and stakeholders to speak up and report, without the fear of retaliation, any possible irregularities which include acts or omissions, malicious or negligent, practiced in the scope of a professional activity, that any interested party identifies, has knowledge or unfounded doubts of non-compliance with the Code of Conduct, Conflict of Interest Policy or other internal policies of Rauva Technology, legislation or regulations. . This policy does not conflict with the use of regular channels to report suspicious cases to direct superiors, except in case of knowing or feeling that this channel will not be appropriate.

2.3 The basic principles of the Whistleblowing Policy include:

- Protection of Identity and Confidentiality
    - The whistleblowers may report any irregularities on an anonymous basis or by identifying themselves.
    - Rauva Technology management is responsible to ensure the existence and effectiveness of the measures necessary to maintain the confidentiality and anonymity of whistleblowers, of the information and also the data included in the disclosures and subsequent processing.
    - The communication of any irregularities is always treated as confidential information, and the access to it is restricted to competent and responsible persons for their treatment.
    - All employees with access to information that is part of a disclosure, and subsequent processes, are obliged to keep its confidentiality.
    - Any party or person mentioned in the communication of any irregularities ("disclosure") may not, under any circumstances, have access to the identity of the whistleblower.

- No retaliation
    - Rauva Technology, its management and other employees, will refrain from any prejudicial treatment, retaliatory action, harassment, intimidation or discrimination towards the whistleblower.
    - Rauva Technology will use all proportionate measures to ensure that retaliation does not occur.
    - Rauva Technology will develop investigation processes and decide about possible sanctions for all conduct carried out by employees, or other persons under their control, with the aim of threatening, harassing or discriminating against the author of the communication as a form of retaliation.

- Intentionality
    - All reports of possible irregularities must be made in good faith and with reasonable motives to be considered valid and truthful.
    - Failure to comply with the provisions of the previous paragraph constitutes an infraction that may lead to the initiation of disciplinary proceedings against the perpetrator of the action and possible sanction appropriate and proportional to the infraction.

- Communication duty
    - Whenever a Rauva Technology employee becomes aware that a possible irregularity has occurred, or is expected to occur, he/she is obliged to immediately report it in accordance with this policy.

- Protection of the Whistleblower
    - Whistleblowers are entitled to benefit of legal protection
    - Whistleblowers may benefit from measures for the protection of witnesses in criminal proceedings.

2.4 This policy applies to members of the Board of Directors and its committees, executives, permanent and contract employees, interns, consultants, employees working through a third party, customers, shareholders and any third party who has interest in Rauva Technology.

2.5 All employees are expected to adhere to this document. In the event any exceptions are required, the same should be suitably documented and will need to be approved by the BoD.

2.6 This policy does not override the requirement to report in the cases and under the terms determined by law.

3. Regulatory Guidelines Applicable

3.1 Rauva Technology operates in an environment in which it must have regard to the Portuguese laws and the rules and guidelines laid down by relevant bodies which have jurisdiction over it such as MENAC. There are also policies determined by the management of Rauva Technology and the detailed internal rules and procedures which must be adhered.

3.2 The following regulations contain references to the principles in relation to Whistleblowing include:

- Law no. 93/2021 of December 20 - General Regime for the Protection of Whistleblowers
- Law no. 83/2017 of 18 August - Money laundering and terrorist financing prevention Law
- Decree-Law no. 109-E/2021 of 9 December General Regime for the Prevention of Corruption
- Directive (EU) no. 2019/1937 of 23 October – Directive on the protection of persons who report breaches of Union law
- Regulation (EU) no. 2016/679 - General Data Protection Regulation

4. Whistleblowing Cases

4.1 Rauva Technology aims to foster a culture of transparency and accountability by encouraging its employees and stakeholders to report any wrongdoings or potential misconduct whenever reasonable information indicating a suspicion is found so that violations can be detected, and

corrective actions can be implemented in a timely manner. These violations could encompass a wide range of scenarios including but not limited to:

- Bullying & Harassment
- Discrimination
- Ethics & Misconduct
- Fraud & Theft
- Bribery, Corruption & Money Laundering
- Purchasing & Public procurement
- Product and transport safety and compliance
- Protection of the environment
- Radiation protection and nuclear safety
- Food and feed safety, animal health and welfare
- Public health
- Competition & Consumer protection
- Data protection and privacy and cybersecurity
- Other violations

4.2 Any possible irregularities presented, and that are not in-scope of the identified in the preceding paragraph, as well as complaints regarding the quality of the Company's products and services, will not be subject to processing or analysis.

5. Channels for Reporting Violations

5.1. This policy is supported by Rauva Technology Whistleblowing Channel, which allows the reception, processing and treatment of communications of potential irregularities by whistleblowers without the need for approval or permission of any kind.

5.2 All employees and stakeholders are encouraged to voice their concerns through the channels for reporting that are in place at the earliest opportunity. These channels are secure and guarantee confidential reporting and Whistleblower protection. The channels available are:

- Portal available on Rauva Technology website – https://eu.deloitte-halo.com/whistleblower/website/RauvaTechnology
- Whistleblower e-mail – RauvaTechnology_Whistleblowing@deloitte.pt
- Mail – an e-mail should be sent to the e-mail address presented immediately above, to schedule a session.

5.3 The above identified channels are made available and managed by an external and independent entity – Deloitte, which will receive and perform the preliminary screening and analysis of the disclosures received. Access to disclosures is limited to persons with relevant competences to handle and guarantee the confidentiality of the Whistleblowing Channel and all the information, ensuring that only authorized personnel of Rauva Technology will have access to the reports.

5.4 It is to be noted that the above-mentioned channels are strictly to be used for the purpose of reporting any violation or wrongdoing within the organization. Any reports that are based on rumours or personal conflicts or related to complaints about the services provided by Rauva Technology will not be entertained.

6. Procedures to be followed

6.1 Submission of Report

6.1.1 Reports shall be submitted by the whistleblower through any of the channels mentioned in Section 5 "Channels for Reporting Violations" mentioned in this document. The whistleblower must select the confidentiality level he/she wishes to submit the disclosure of the potential irregularity. The disclosure may contain the identification of the whistleblower or be totally anonymous if that is the intention.

6.2 Content of the Report

6.2.1 The report must contain the information necessary for subsequent treatment and analysis, being as detailed as possible, containing sufficient amounts of data, and be supported by documentary evidence, if applicable, as reports that do not include sufficient amount of details are difficult to investigate. The reports must contain a following reasonable amount of information, including but not limited to:

- Author's Name (if that is the whistleblower decision)
- Concerned person / parties involved
- Witnesses, if any
- Description of the facts supporting the alleged irregularity
- Details of the incident, its dates, place(s), and the number of times it has occurred
- Any other information that would assist in the investigation.

6.2.2 Rauva Technology reserves the right to consider only those matters included in Article 4 of this policy, refusing to process disclosures that exceed this scope or that do not:

- Contain a sufficient description of the facts supporting the potential irregularity; or
- Allow a supported investigation

6.2.3 Once the report is submitted, the whistleblower will be notified of the receipt of the disclosure within 7 days from the date it has been received.

6.3 Investigation of the Report

6.3.1 Reports of potential irregularities will be subject to an inquiry and investigation process, unless it is manifestly unfounded, insufficiently informed or excluded from the scope of this policy. All

investigations are initiated by the external and independent entity through a preliminary analysis of the completeness of the information made available in relation to the scope of the disclosure and Whistleblowing Channel.

6.3.2 If the disclosure is within the scope of the Whistleblowing Channel and the information made available enables the investigation, it will be sent to Rauva Technology responsible for its analysis of credibility and veracity.

6.3.3 The investigation will be:

- Confidential;
- Documented in an internal report. Rauva Technology responsibles shall decide whether the communication should be archived or subject to additional investigation.

6.4 In case there is a conflict of interest of one the persons responsible for the investigation of the disclosure, he/she will not be informed of the existence of the disclosure.

7. Violation Report Processing

7.1 In case of receipt of Whistleblowing incidents, and with the exception of disclosures related to Bullying & Harassment or Discrimination, which are directed to the Head of People, the remaining types will be directed to the HoC. The Head of Legal will be a backup in case these responsibles are not available. Whenever these responsibles are involved / mentioned in the disclosures, the report will be escalated / directed to the CRO.

7.2 The responsibles mentioned above will independently investigate the incident and determine the actual outcome. If needed, other responsibles might support the investigation. A report will be published post completion of the investigations and the outcome of the same shall be duly recorded as part of such report. This report will be made available to the Board of Directors in its meetings who should decide about the measures / consequences.

> **Note** – If any of the responsibles mentioned above is accused, then he / she will be immediately excluded from the investigation process.

7.3 Rauva Technology has permanent access to Deloitte Conductwatch system which provides the following information at any point in time:

- The channel for receiving reports
- Total number of reports received
- Total number of reports by subject
- Number of reports processed and reports that are in progress
- Type of processing.

7.4 Rauva Technology will develop working procedures for processing reports, describing detailed steps of each procedure, and specifying the inputs, outputs, models, and automated systems used

for each procedure as well as individuals authorized to do the same. These working procedures shall include but not be limited to the below report processing stages:

- Report reception
- Initial assessment
- Identification of Verification Plan
- Documentation of rationale supporting the processing decision
- Decision taken post investigation
- Follow-up of decision implementation
- Record Keeping.

7.5 The Compliance Department shall record all reports received, actions carried out, corrective actions, etc. in a Whistleblowing Register.

8. Obligations of the Parties Involved

It is important to note that all incidents within the scope of this policy, regardless of their severity, should be reported in order to maintain the integrity and reputation of Rauva Technology. It requires active support from all employees and stakeholders who must report any incidents suspected of involving violations. However, incidents that have a greater impact on the operations of Rauva Technology and the well-being of individuals should be addressed with utmost urgency and care.

8.1 Obligations of Whistleblowers

8.1.1 A Whistleblower shall:

- Highlight any wrongdoings or violations as soon as possible
- Ensure credibility of information being reported by refraining from rumours and baseless allegations
- Avoid reports that are malicious in nature which are aimed at defaming fellow employees and stakeholders, taking reprisal or retaliation against them
- Exercise caution and due diligence while reporting incidents in order to ensure accuracy while providing all necessary information and evidence to substantiate the report as required by the nature of the violation
- Maintain full confidentiality of the reporting done and any supporting evidence in relation to the report
- Take full responsibility for the report made as well as the consequences of reporting malicious allegations that malign the reputation of Rauva Technology or any of its employees and stakeholders
- Perform any other responsibilities as may be defined internally or by regulatory authorities from time to time.

8.2 Obligations of Rauva Technology

8.2.1 **Upon receipt of Whistleblowing reports, Rauva Technology shall:**

- Notify the Whistleblower within 7 days upon receipt of the report
- Treat any report received with caution and exercise scepticism regardless of the impact, nature, language, and adequacy of information in the report
- Refer the report to the responsible department for control and investigation, either inside or outside Rauva Technology
- Conduct a thorough investigation of the facts of the report and document the same along with evidence
- Take all necessary steps to protect the Whistleblower
- Maintain confidentiality throughout the investigation process
- Be fair and keep the best interest of Rauva Technology and its employees in mind
- Ensure that appropriate remedial action is effectively taken in a timely manner
- Ensure violation reports, relevant documents, and any other evidence gathered during the investigation (including recordings) are kept on record and the same shall be kept on record for 10 years
- Notify the Whistleblower regarding the decision taken on the conclusion of the investigation
- Perform any other responsibilities as may be defined internally or by regulatory authorities from time to time.

8.2.2 **Upon receipt of Whistleblowing reports, Rauva Technology shall:**

- Ensure that the Whistleblowers are not victimized during the process of investigation
- Ensure that none of Rauva Technology employees use their administrative positions to prevent others from exercising their rights or comply with their obligations
- Ensure that the information provided by the Whistleblower will be dealt with confidentially and will not be disclosed except to regulatory authorities and as required by law or other authorities that need such information for the purposes of investigation and case settlement. In such instances, Rauva Technology shall inform the Whistleblower before revealing their identity to any regulatory authority
- Not take any action against the Whistleblower in case the disclosure had been made in good faith but has been established as invalid during the investigation
- Where found appropriate, relocate the Whistleblower to a different department
- Ensure awareness and training programs are conducted to make sure that the employees and stakeholders are aware of their safeguards and obligations.

8.2.3 In an event where the Whistleblower believes that they were a victim of retaliation for reporting a violation, he has the right to file a complaint with the People Department for further action.

8.2.4 It is to be noted that a Whistleblower, whose identity has not been revealed or could not have been discovered during the investigation process, may not be able to avail the safeguards as mentioned above.

9. Disciplinary Action

9.1 Any concern made in good faith is welcome by the Whistleblowing Policy. However, any report made with an intent to malign Rauva Technology and its employees or damage the reputation of Rauva Technology will not be tolerated and may be subject to disciplinary action. Violating the commitment to the rules and professional conduct may subject the employees to disciplinary action regardless of their positions in accordance with the investigation stages mentioned above, taking into account whether the violation was committed intentionally or not together with the extent of the violator's good faith upon committing the violation, and whether he / she reported the same or not.

9.2 Disciplinary action can be taken in the below cases including but not limiting to:

- Any employee who permits, directs, agrees on, or participates in the violation of the behavioural principles and controls
- Any employee who fails to report or hides or covers up the violation or intentionally withholds information related to breaching the work principles and professional conduct controls
- Any official who fails to report the violation despite knowing the same when it was reported to him / her by his / her subordinates
- Any report based on false or misleading information
- Bad faith and malicious reports or the Whistleblower's intentional involvement of any employee's name in the report without striving for accuracy or in case of speculation without evidence or the fabrication of evidence.

9.3 On conclusion of the investigation, in case an employee is found to be guilty of committing a violation, any one or a combination of the disciplinary actions will be taken in line with the aspects detailed in the Human Resources Policy.

10. Data Privacy and Protection

10.1 The information processed in the Whistleblowing Channel will be subject to security mechanisms and controls in accordance with applicable data protection and information security legislation. Additionally, the platform is certified according to ISO 27001.

10.2 Rauva Technology is the entity responsible for the processing of the personal data considered in the Whistleblowing Channel. The external and independent entity is a subcontractor of Rauva Technology with regard to the processing of personal data.

10.3 The information communicated in-scope of this policy will be treated in accordance with the lawfulness and purposes defined in Rauva Technology Privacy Policy.