Whistleblowing Policy

Internal Information System

Last modified 23 - 11 - 2023

Table of Contents

Whistleblowing Policy

Internal Information System

Introduction

In compliance with the provisions of Spanish Law 2/2023, of February 20, regulating the protection of individuals reporting regulatory violations and combating corruption, RavenPack International SLU ("RavenPack") has implemented an Internal Information System hereinafter "IIS".

The IIS serves as a channel for those individuals who, in a work or professional context, have obtained information about actions or omissions that may constitute violations of European Union law or serious or very serious criminal or administrative offenses within the scope of the RavenPack, to report them with all the guarantees of confidentiality and protection.

The law contemplates the existence of two types of information systems that the public can turn to, to report with guarantees of confidentiality and anonymity:

- Internal: This serves as the preferred channel for reporting actions or omissions covered by the law, provided that the infringement can be effectively addressed. It is preferable that information about irregular practices be known by RavenPack itself to correct them or repair damages as soon as possible.

- External: Aimed at providing the public with communication to a specialized public authority, for these purposes, the Autoridad Independiente de Protección del Informante or Independent Authority for the Protection of Whistleblowers ("A.A.I"), or competent regional authorities. This channel may instill more confidence in individuals, dispelling their fear of facing reprisals in their environment. In our case, as a company based in the Andalusian region of Spain the corresponding A.A.I. is the Oficina Andaluza Antifraude, available at https://antifraudeandalucia.sedelectronica.es/

Nevertheless, it will be up to the whistleblower to assess which channel to follow, internal or external, based on the circumstances and the risks of reprisals they consider.

Purpose

The Internal Information System established by RavenPack serves a dual purpose:

- Protecting Individuals: It aims to protect individuals in a work or professional context who detect and report regulatory violations and acts of corruption (“Informants" or “Whistleblowers”). Additionally, it extends protection to individuals who are the subject of the reported facts.

- Strengthening the Culture of Information or Communication: The system is designed to strengthen the culture of information or communication within the organization. This serves as a mechanism to prevent and detect threats to the public interest.

Principles

With the aim of ensuring the effectiveness of the system, RavenPack will ensure that it meets all the requirements established in Law 2/2023, regulating the protection of individuals reporting regulatory violations and combating corruption, particularly:

- Accessibility: The IIS must allow communication, whether in writing, verbally, or both, of information regarding regulatory violations and the fight against corruption to all individuals within its scope of application.

- Independence: The IIS will be managed by a Whistleblowing Officer with complete independence and autonomy from the rest of its organs.

- Confidentiality: The confidentiality of the Informant's identity and of any person mentioned in the communication, as well as the actions carried out in its management and processing, is guaranteed. The internal information channel will even allow the submission and subsequent processing of anonymous communications.

- Protection of Personal Data.

- Secrecy of Communications.

- Security and Protection of Informants and Affected Individuals.

- Presumption of Innocence and Respect for the Honor of Affected Individuals.

What can be reported? - Material scope of application

The IIS must allow the receipt of communications related to events that could constitute, within the scope of the competencies of RavenPack:

- Actions or omissions that may constitute violations of European Union law, provided that:
    - They fall within the scope of application of the acts of the Union listed in the Annex of Directive (EU) 2019/1937, regardless of the classification made by the domestic legal system. The directive establishes common minimum rules for the protection of individuals reporting the following violations of Union law: Violations falling within the scope of the acts of the Union listed in the annex relating to the following areas: i) public procurement, ii) services, products, and financial markets, and prevention of money laundering and terrorist financing, iii) product safety and conformity, iv) transport safety, v) environmental protection, vi) protection against radiation and nuclear safety, vii) food and feed safety, animal health, and animal welfare, viii) public health, ix) consumer protection, x) privacy and personal data protection, and security of networks and information systems.
    - They affect the financial interests of the European Union as contemplated in Article 325 of the Treaty on the Functioning of the European Union (TFEU).
    - They impact the internal market, as contemplated in Article 26, paragraph 2 of the TFEU, including violations of Union rules on competition and state aid, as well as violations related to the internal market regarding acts that infringe on corporate tax rules or practices aimed at obtaining a tax advantage that distorts the purpose or intent of the legislation applicable to corporate tax.

- Actions or omissions that may constitute serious or very serious criminal or administrative offenses. In any case, this includes all serious or very serious criminal or administrative offenses that involve economic loss to the Spanish Tax Authority and Social Security

Who can report? - Personal scope of application

The IIS allows the reporting of potential violations to individuals working in both the private and public sectors, who have obtained information about infractions in a work or professional context. This encompasses the following:

- All individuals who hold the status of public employees of RavenPack.

- All self-employed professionals, suppliers, contractors, subcontractors, or any other third party with whom RavenPack has or has previously had any commercial or professional relationship. This includes all individuals working for them or under the supervision or direction of contractors, subcontractors, and suppliers of RavenPack.

- Any person who has had a terminated employment or statutory relationship with RavenPack, volunteers, interns, trainees, regardless of whether they receive remuneration or not, and even individuals participating in personnel selection processes, provided that the information about the infraction was obtained during the selection process or pre-contractual negotiation.

The whistleblower protection measures outlined will also apply, if applicable, specifically to the legal representatives of workers in the exercise of their advisory and support functions for the whistleblower.

The person providing information must hold a reasonable belief in the accuracy of the information being communicated and should not make communications with bad faith or abuse of right. In the latter case, they may incur civil, criminal, and administrative liability.

Content of communications

The communication submitted must include the maximum number of known details necessary for the identification of individuals to whom the information refers, as well as the behaviors contrary to legal provisions attributed to them. In particular, the following information should be provided:

- Full name, ID number (if known), workplace, functional area, job position, location where they perform their duties, and any other available data that allows for clear and unequivocal identification of the person about whom information is being reported.

- Detailed description of the actions and behaviors performed that may constitute any type of violation and about which information is intended to be reported. Documentation available to substantiate these facts should be provided.

- If applicable, an indication of the employment or professional relationship that links the informant with RavenPack, for the purpose of applying the protection measures.

- Any other facts that may be considered appropriate or relevant.

When making the communication, the informant may specify an address, email, or secure location for receiving notifications. The informant may also expressly waive receiving any communication regarding actions taken as a result of the provided information.

Whistleblowing Officer

The CEO of RavenPack is responsible for implementing the IIS and for the processing of personal data. Additionally, they have the authority to appoint, dismiss, or replace the person responsible for the IIS. The person appointed as the Whistleblowing Officer by RavenPack's management is RavenPack's Legal Counsel.

The Whistleblowing Officer is tasked with the diligent management of the IIS and the proper handling of received communications.

The Whistleblowing Officer "*must perform their functions independently and autonomously from the rest of the entity's organs or bodies, may not receive any type of instructions in their exercise, and must have all the personal and material resources to carry them out*".

Protection of Informants and Affected People

Individuals reporting infractions shall have the right to protection.

Preservation of the Whistleblower's and Affected Individuals' identity:
Preserve their identity, except for communications that may be made to the judicial authority, the Public Prosecutor's Office, or the competent administrative authority within the framework of a criminal, disciplinary, or sanctioning investigation.

Conditions for Protection:
Individuals reporting or disclosing infractions within the material scope of application have the right to protection provided that the following circumstances exist:

- They have reasonable grounds to believe that the information is true at the time of communication or disclosure, even if conclusive evidence is not provided, and that the information falls within the scope of the law.
- The communication or disclosure has been made in accordance with the requirements stipulated by law.

The protection outlined in this law is explicitly excluded for individuals reporting or disclosing:

- Information contained in communications that have been rejected by any internal information channel or by the A.A.I.
- Information related to claims about interpersonal conflicts or that only affect the whistleblower and the persons referred to in the communication or disclosure.
- Information already fully available to the public or that constitutes mere rumors.
- Information related to actions or omissions not covered by Article 2 of Law 2/2023.

Individuals who have anonymously reported or disclosed information about actions or omissions publicly but have later been identified and meet the conditions specified to be entitled to the protection.

Regarding false communications, Law 2/2023 establishes that knowingly communicating or publicly revealing false information constitutes a very serious offense.

Prohibition of Retaliation and Protection Measures Against Them:
The system establishes the principle of Whistleblower protection, expressly prohibiting any act of retaliation, threat of retaliation, or attempted retaliation against the Whistleblower.
Retaliation is understood to include any acts or omissions prohibited by law, or that, directly or indirectly, result in unfavorable treatment placing those who suffer them at a particular disadvantage compared to others in the work or professional context, solely because of their status as Whistleblowers or for making a public disclosure.
As specified in Article 36.3 of Law 2/2023,"for illustrative purposes," retaliation includes acts such as:

- Suspension of the employment contract, dismissal, or termination of the employment or statutory relationship, including non-renewal or early termination of a temporary employment contract once the probationary period has been exceeded, or early termination or annulment of contracts for goods or services, imposition of any disciplinary measure, degradation, or denial of promotions and any other substantial modification of working conditions and the non-conversion of a temporary employment contract into a permanent one, in case the worker had legitimate expectations that they would be offered permanent employment; unless these measures are carried out within the regular exercise of the power of direction under labor or civil service law, due to circumstances, facts, or proven infractions, and unrelated to the submission of the communication.
- Harms, including reputational, or economic losses, coercion, intimidation, harassment, or ostracism.
- Negative assessments or references regarding work or professional performance.
- Inclusion in blacklists or dissemination of information in a specific sector that hinders or prevents access to employment or the contracting of works or services.
- Denial or annulment of a license or permit.
- Denial of training.
- Discrimination, or unfavorable or unjust treatment.

Measures for the Protection of Affected Individuals:
Individuals affected by the communication, during the processing of the case, shall have the right:

- To the presumption of innocence.
- To defense.
- To access the case file on the terms regulated in Law 2/2023.
- To the same protection established for Whistleblowers, preserving their identity and ensuring the confidentiality of the facts and data of the procedure. An exception is made for communications that may be made to the judicial authority, the Public Prosecutor's

Office, or the competent administrative authority within the framework of a criminal, disciplinary, or sanctioning investigation.

- To exemption or mitigation the sanction that may correspond to them if the requirements are met:
    - Having ceased the commission of the offense at the time of filing the communication or disclosure and having identified, if applicable, the rest of the people who have participated or favored it.
    - Having cooperated fully, continuously, and diligently throughout the entire investigative process.
    - Having provided truthful and relevant information, evidence, or significant data to substantiate the investigated facts, without having proceeded to their destruction or concealment, nor having revealed their content to third parties, directly or indirectly.
    - Having proceeded to repair the damage caused for which they are responsible.

Measure for the Protection of Personal Data

The processing of personal data resulting from the application of Law 2/2023, will be governed by the provisions of Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016, Organic Law 3/2018, on the Protection of Personal Data and the guarantee of digital rights, and Organic Law 7/2021, on the protection of personal data processed for the purposes of preventing, detecting, investigating, and prosecuting criminal offenses and enforcing criminal sanctions.

The SII must prevent unauthorized access, preserve the identity, and ensure the confidentiality of data related to affected individuals and any third party mentioned in the provided information, especially the identity of the Whistleblower if identified.

The identity of the whistleblower can only be disclosed to the judicial authority, the Public Prosecutor's Office, or the competent administrative authority within the framework of a criminal, disciplinary, or sanctioning investigation. In such cases, they will be subject to safeguards established in applicable regulations.

If the received information contains personal data subject to special protection, immediate deletion will be carried out unless processing is necessary for reasons of essential public interest. In any case, personal data that is not evidently relevant for processing specific information will not be collected, or if collected accidentally, will be promptly deleted.

Communications that have not been processed will only be retained in an anonymized form, and the obligation to block will not apply.

Procedure

To learn more about the SII procedure please check out our Whistleblower Procedure

Questions

If you should have any questions or queries regarding the policy, please reach whistle@ravenpack.com

Last modified 23 - 11 - 2023