Prisma
Agile. Secure. Reliable.

PRISMA PAYMENTS, E.P., S.A.

INTERERNAL INFORMATION SYSTEM POLICY

INTERNAL COMMUNICATION CHANNEL

27 March 2025

1. Introduction

Law 2/2023, of February 20, regulating the protection of persons who report regulatory violations and the fight against corruption, incorporates Directive (EU) 2019/1937 of the European Parliament and the Council of October 23, 2019, into Spanish law. This directive establishes a homogeneous regulatory framework across the European Union to ensure legal security and protection for those who, in the course of their professional or work activities, detect irregularities or legal breaches and report them through the appropriate channels.

The main objective of this regulation is to protect whistleblowers from possible retaliation due to their reports, ensuring the existence of appropriate mechanisms for handling such information and promoting a culture of transparency and regulatory compliance within organizations. To this end, the law requires the implementation of internal reporting channels that allow the secure communication of alleged violations, guaranteeing whistleblower confidentiality and expressly prohibiting any form of direct or indirect retaliation.

In compliance with these legal obligations, the Board of Directors of Prisma Payments EP, S.A. (hereinafter, "**Prisma**") has approved this Policy on the Internal Reporting System (hereinafter, "**Internal Reporting System**"). This policy is part of the entity's internal regulatory framework, aligning with its commitment to transparency, business ethics, and regulatory compliance.

Through this policy, Prisma regulates its Internal Reporting System, ensuring compliance with the principles and guarantees established by applicable laws. This reinforces Prisma's commitment to preventing, detecting, and managing possible regulatory breaches, fostering an environment where individuals can report irregularities without fear of retaliation, thereby contributing to a corporate culture based on legality, integrity, and corporate responsibility.

For matters not expressly regulated in this policy, the provisions of Law 2/2023, of February 20, on the protection of persons who report regulatory violations and

the fight against corruption, shall apply subsidiarily. In case of any contradiction between the content of this policy and the imperative provisions of the law, the latter shall prevail.

2. Characteristics of the Internal Reporting System

Prisma's Internal Reporting System is characterized by the following:

a) It allows all individuals within its personal scope to report information on violations covered by its material scope (as detailed in Sections 3 and 4).

b) It ensures confidentiality regarding the identity of the whistleblower and any third party mentioned in the report, as well as the actions carried out in handling the report, protecting data and preventing unauthorized access.

c) It incorporates an Internal Communication Channel (hereinafter, "**Internal Communication Channel**") that allows written and/or verbal reporting and meets legal requirements.

e) It guarantees that submitted reports are effectively managed within Prisma.

f) It has a designated responsible person appointed by Prisma's Board of Directors, complying with legal requirements.

h) It includes a procedure for managing reports that complies with legal requirements.

j) It establishes guarantees for the protection of whistleblowers, in accordance with legal provisions.

3. Material Scope

The Internal Communication Channel is the means by which the Internal Reporting System allows the reporting of actions or omissions related to the conduct of organization members or other interested parties linked to Prisma's activities that:

a) May constitute violations of European Union law[1].

b) May be considered criminal or serious administrative offenses, including those causing economic harm to the Public Treasury or Social Security.

c) May constitute breaches of Prisma's Code of Conduct or other corporate policies, including those in the Anti-Money Laundering and Counter-Terrorist Financing Manual and the Criminal Prevention Policy.

The following reports are excluded:

i) Reports involving classified information[2].

ii) Those affecting the obligations resulting from the protection of the professional secrecy of the medical and legal professions, the duty of confidentiality of the Security Forces and Corps in the scope of their actions, as well as the secrecy of judicial deliberations.

iii) Those relating to infringements in the processing of procurement procedures containing classified information or which have been declared secret or reserved, or those whose execution must be accompanied by special security measures in accordance with the legislation in force, or where the protection of interests essential to the security of the State requires.

iv) In the event of public information or disclosure of any of the offences referred to in Part II of the Annex to Directive (EU) 2019/1937 of the European

[1] 1ºThese are actions or omissions that: Fall within the scope of the European Union acts listed in the annex of Directive (EU) 2019/1937 of the European Parliament and of the Council of October 23, 2019, on the protection of persons reporting breaches of Union law, regardless of how they are classified under domestic legal systems.; 2.º Affect the financial interests of the European Union, as provided for in Article 325 of the Treaty on the Functioning of the European Union (TFEU); o 3.º Impact the internal market, as referred to in Article 26(2) of the TFEU, including violations of EU competition law and state aid rules, as well as breaches related to the internal market concerning acts that infringe corporate tax rules or practices aimed at obtaining a tax advantage that distorts the object or purpose of the legislation applicable to corporate taxation.

[2] Information related to matters classified as secret or confidential, the disclosure of which may cause harm to the information holder, especially if it pertains to information that could affect national security. For this reason, it is restricted by law or regulated for specific categories of individuals.

Parliament and of the Council of 23 October 2019, the specific rules on reporting of offences in such matters shall apply.

Information involving a complaint of a commercial nature is also excluded and should be referred to the relevant Prisma area or department (customer service).

4. Personal Scope

The Internal Communication Channel is the channel for people to report any actions or omissions within the material scope set out in the previous section:

a) Prisma workers and former workers.

b) Self-employed people who have any kind of economic or professional relationship with Prisma.

c) The shareholders and directors of Prisma.

d) Any person working for or under the supervision and direction of Prisma's contractors, subcontractors and suppliers.

e) Volunteers, trainees, and individuals in training, whether paid or unpaid, as well as those whose employment relationship has not yet begun, in cases where information on infringements was obtained during the recruitment process or pre-contractual negotiation.

Any of the above who submit a report will be referred to as the "**Whistleblower**".

5. Management of the Internal Reporting System

The management of the Internal Information System consists of receiving information.

Management may be carried out by Prisma or outsourced. In the latter case, the external third party shall provide adequate guarantees of respect for independence, confidentiality, data protection and secrecy of communications.

The management of the Internal Information System by a third party shall not undermine the guarantees and requirements laid down by law.

6. Responsible for the Internal Reporting System

The Internal Reporting System will have a designated person responsible for its management, who will be appointed, removed, or dismissed by Prisma's Board of Directors.

The Board of Directors may choose to appoint either an individual or a collegiate body as the responsible entity. In the latter case, the body must delegate one of its members to oversee the management of the Internal Reporting System and handle the processing of investigative cases.

The person responsible for the Internal Reporting System will carry out their duties independently and autonomously from other governing bodies within Prisma and will have all the necessary human and material resources to fulfil their role.

If justified by circumstances, the responsible person may simultaneously hold another position within the company, provided that any potential conflicts of interest are avoided.

The individual in charge of Prisma's Compliance function may also be designated as the person responsible for the Internal Reporting System.

7. Information Management Procedure

Any Whistleblower may report any actions or omissions covered by the material scope of the Internal Reporting System in accordance with the information management procedure set out in Annex I of this Corporate Policy on the Internal Reporting System.

8. Publicity

Information regarding the Internal Reporting System, the Internal Communication Channel, and the management procedure will be provided in a clear and easily accessible manner on Prisma's website[3].

9. Right to Protection

9.1. Protected Persons

The following people are entitled to protection:

a) The Whistleblower, provided they have reasonable grounds to believe that the information reported is true at the time of communication, even if they do not provide conclusive evidence, and as long as the report is made in accordance with the requirements set forth in the Internal Reporting System.

b) Legal representatives of employees in the exercise of their advisory and support functions to the Whistleblower.

c) Individuals within the organization where the Whistleblower provides services and who assist them in the process.

d) Individuals related to the Whistleblower who may suffer retaliation, such as coworkers or family members.

e) Legal entities for which the Whistleblower works, maintains any other work-related relationship, or holds a significant interest.

f) Persons who publicly disclose information about actions or omissions covered by the Internal Reporting System anonymously, but who are later identified and meet the conditions outlined in the system or legally.

[3] Such information must be displayed on the homepage in a separate and easily identifiable section.

c) Those who report violations to the relevant institutions, bodies, or agencies of the European Union, falling within the scope of Directive (EU) 2019/1937 of the European Parliament and the Council of October 23, 2019, on the protection of people who report breaches of EU law.

The following individuals are not entitled to protection:

a) Those whose reports have been inadmissible under the Internal Communication Channel.

b) Those making claims related to interpersonal conflicts or affecting only the Whistleblower and the individuals referred to in the report.

c) Those reporting information already fully available to the public or mere rumours.

d) Those reporting actions or omissions are not covered by the material scope of the Internal Reporting System.

9.2. Prohibition of Retaliation

All acts of retaliation are strictly prohibited, including threats and attempts of retaliation against Whistleblowers and other protected people.

Retaliation is understood as any act or omission prohibited by law or any direct or indirect adverse action that places the affected individuals at a disadvantage in their professional or work environment, solely because of their status as a whistleblower or for having made a public disclosure.

Examples of retaliation include:

a) Suspension of employment, dismissal, or termination of the work relationship, including the non-renewal or early termination of a temporary employment contract after passing the probationary period, or the cancellation of contracts for goods or services. It also includes any disciplinary measures, demotions, denial of promotions, and any other substantial changes in working conditions, as well as the failure to convert a

temporary contract into a permanent one when the worker had legitimate expectations of obtaining permanent employment. These measures are prohibited unless they are justified independently of the whistleblowing and comply with applicable labour laws.

b) Reputational damage, economic losses, coercion, intimidation, harassment, or ostracization.

c) Negative performance evaluations or employment references.

d) Blacklisting or dissemination of information within a professional sector, preventing or hindering future employment or service contracts.

e) Denial or cancellation of a license or permit.

f) Denial of training opportunities.

g) Discrimination, unfair, or unfavourable treatment.

9.3. Protection Measures Against Retaliation

The Whistleblower and other protected individuals may benefit from the following protection measures against retaliation:

a) They will not be considered in violation of any confidentiality restrictions and will not incur any liability in connection with their report, provided they had reasonable grounds to believe that their report was necessary to disclose a violation under the Internal Reporting System or the law. This does not exempt them from potential criminal liabilities if applicable.

This protection also extends to legal representatives of employees, even if they are bound by confidentiality obligations or prohibited from disclosing reserved information. This is without prejudice to specific labour law protections.

b) They will not be held liable for acquiring or accessing the information reported, as long as obtaining or accessing such information was not a criminal offense.

   Any other liabilities unrelated to the communication or unnecessary for disclosing a violation will be handled in accordance with applicable laws.

c) In legal proceedings or before an authority, if the affected person can reasonably demonstrate that they reported or disclosed information in compliance with the Internal Reporting System or the law and subsequently suffered harm, it will be presumed that the harm was a result of retaliation for whistleblowing. In such cases, the burden of proof will shift to the party responsible for the harmful action, requiring them to demonstrate that the measure was based on legitimate and unrelated reasons.

d) In judicial proceedings, including cases of defamation, copyright infringement, confidentiality breaches, data protection violations, trade secret disclosures, or labour claims, whistleblowers will not be held liable for protected communications, they will also have the right to defend themselves in these legal proceedings by citing their status as whistleblowers, provided they had reasonable grounds to believe that their disclosure was necessary to expose a violation.

9.4. Protection Measures for Affected Persons

During the processing of a case, the persons affected by the communication shall have the right to the presumption of innocence, the right of defence and the right of access to the case file under the terms established by law, as well as the same protection established for the informant, preserving their identity and guaranteeing the confidentiality of the facts and data of the procedure.

10. Processing of Personal Data

10.1. Personal Data Processing Regime

The processing of personal data deriving from the application of the Internal Information System shall be governed by the provisions of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, Organic Law 3/2018 of 5 December on the Protection of Personal Data and Guarantee of Digital Rights, Organic Law 7/2021 of 26 May on the protection of personal data processed for the purposes of the prevention, detection, investigation and prosecution of criminal offences and the execution of criminal penalties, and this Title, and in particular:

a) The processing of personal data in cases of communication shall be deemed lawful under the provisions of Articles 6.1.c) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, 8 of Organic Law 3/2018 of 5 December and 11 of Organic Law 7/2021 of 26 May.

b) The data subjects may exercise the rights referred to in Articles 15 to 22 of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016.

c) Annex II of this Corporate Policy on the Internal Information System of this document provides the information referred to in Articles 13 of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 and 11 of Organic Law 3/2018 of 5 December when personal data are obtained from a data subject,

No personal data shall be collected unless it is clearly relevant for processing a specific report. If personal data is inadvertently collected, it shall be deleted without undue delay.

Personal data processing necessary for the Internal Reporting System shall be considered lawful.

If the person implicated in the reported facts exercises their right to object, it shall be presumed that, unless proven otherwise, there are overriding legitimate grounds that justify the processing of their personal data.

10.2. Processing of Personal Data in the Internal Reporting System

Access to personal data contained in the Internal Reporting System shall be restricted, within their respective roles and functions, exclusively to the following individuals:

a) The person responsible for the Internal Reporting System and those directly managing it.

b) The head of Human Resources or the competent authority, only when disciplinary measures against an employee may be applicable. In the case of public employees, the competent authority for handling the matter.

c) The head of the entity's legal services, if legal actions need to be taken regarding the reported facts.

d) The data processors that may be appointed from time to time.

e) The data protection officer.

Data processing by other individuals or even communication to third parties shall be lawful when necessary to implement corrective measures within the entity or to conduct administrative or criminal sanction procedures.

Under no circumstances shall personal data be processed if it is not necessary for understanding and investigating actions or omissions covered by the Internal Reporting System. Any such unnecessary data shall be immediately deleted. Likewise, any personal data communicated that refers to conduct not within the scope of the Internal Reporting System or the law shall also be deleted.

If the information received includes special categories of personal data, it shall be immediately deleted and shall not be registered or processed.

Personal data subject to processing shall only be retained within the Internal Reporting System for the minimum necessary period to determine whether an investigation should be initiated.

If it is determined that the information provided, or part of it, is false, it shall be immediately deleted upon verification, unless the false information constitutes a criminal offense, in which case it shall be retained for the duration of the judicial process.

In any case, if three months have passed since the receipt of a report without an investigation being initiated, the data shall be deleted, unless its retention is required to document the proper functioning of the Internal Reporting System. Reports that have not been acted upon shall be stored only in anonymized form.

10.3. Preservation of the Whistleblower's Identity and Affected Individuals

The Whistleblower has the right to remain anonymous and their identity shall not be disclosed to third parties.

The identity of the Whistleblower shall always be kept confidential and shall not be disclosed to the individuals implicated in the report or to any third parties.

The person affected by the report shall not, under any circumstances, be informed of the identity of the Whistleblower.

The Internal Reporting System shall not collect data that could identify the Whistleblower and must implement technical and organizational measures to preserve anonymity and ensure confidentiality of the Whistleblower's identity, affected individuals, and any third parties mentioned in the report.

The identity of the Whistleblower may only be disclosed to judicial authorities, the Public Prosecutor, or the competent administrative authority within the framework of a criminal, disciplinary, or sanctioning investigation.

Disclosures under the previous paragraph shall be subject to safeguards established by applicable law. Specifically, the Whistleblower shall be informed

before their identity is revealed, unless such disclosure could compromise the investigation or judicial proceedings.

Prisma
Agile. Secure. Reliable.

Annex I

Information Management Procedure

I. Reception of Information

1. The Whistleblower may submit information anonymously. In such cases, anonymity shall be ensured through appropriate mechanisms. All actions derived from communications shall remain confidential, regardless of whether they were submitted anonymously or not.

2. Reports may be submitted in writing through any of the following methods:

   a) The Internal Communication Channel, accessible via Prisma's web platform at the following URL: https://whistleblowersoftware.com/secure/Canal-etico-PrismaPayments

   b) Postal mail, addressed to:

   Prisma Payments EP, S.A.
   Compliance Department Manager
   Leganitos Street, 47 - 9th Floor
   28013 Madrid

3. Reports may also be submitted verbally, via telephone or a voice messaging system. Upon the Whistleblower's request, an in-person meeting may be arranged within a maximum period of 7 days. In the case of verbal communications, the Whistleblower shall be informed that the conversation will be recorded, and they shall be notified about the processing of their data in accordance with:

4. When submitting a report through internal channels, the Whistleblower shall provide the following information to facilitate processing:

   a) Whistleblower identification, unless they choose to remain anonymous.

b) Identification of the individual involved, if applicable.

c) A description of the reported facts, including dates (if possible) and reasons for the report.

d) A secure contact method (email, postal address, or another safe location) for receiving notifications from Prisma regarding the report. Alternatively, the Whistleblower may explicitly waive the right to receive any notifications.

5. In the case of verbal communications, including those submitted via in-person meetings, telephone, or voice messaging systems, Prisma shall document the report using one of the following methods: a) A secure, durable, and accessible audio recording of the conversation, b) A full and accurate transcription, prepared by the responsible personnel handling the report.

6. The Whistleblower shall be informed of their right to review, correct, and sign the transcript of the report.

7. Prisma may enable the reception of other communications outside the material scope of the Internal Reporting System. Such communications shall not be covered by the protections of this system or the law.

8. The Whistleblower may also submit reports through external reporting channels, such as those provided by the Independent Authority for Whistleblower Protection or other relevant institutions, including:

- Bank of Spain:

  https://www.bde.es/bde/es/secciones/sobreelbanco/Transparencia/Informacion_inst/registro-de-acti/Canal_de_denuncias.html

- SEPBLAC (Spanish Financial Intelligence Unit):

  https://www.sepblac.es/es/sujetos-obligados/tramites/comunicacion-por-indicio/

9. Once a report has been submitted, it shall be registered in an information management system, assigned a unique identification code, and stored in a secure database with restricted access. The following details shall be recorded:

   a) Date of receipt.

   b) Identification code.

   c) Actions taken.

   d) Measures adopted.

   e) Date of closure.

10. A confirmation of receipt shall be issued within 7 calendar days from the date of submission, unless the Whistleblower expressly waives their right to receive notifications or Prisma determines that acknowledging receipt could compromise the confidentiality of the communication.

11 Prisma may maintain ongoing communication with the Whistleblower and, if necessary, request additional information.

12. The Compliance Officer shall be responsible for receiving and managing reports, ensuring their independence and autonomy from Prisma's governing bodies, departments, and other functions. However, this responsibility may be compatible with other duties performed by the Compliance Officer.

13. The Compliance Officer may request assistance or collaboration from other departments, functions, or external advisors, depending on the nature and complexity of the report.

14. If the Whistleblower or the Compliance Officer detects a potential conflict of interest, the case shall be managed by Prisma's CEO or a delegated individual.

15. If a report is received by someone other than the Compliance Officer, that individual must maintain absolute confidentiality and immediately forward the report to the responsible person.

II. Admission Process

1. Once the report has been registered, Prisma shall verify whether the reported facts or conduct fall within the material scope of the Internal Reporting System.

2. After conducting this preliminary assessment, Prisma shall decide, within a period not exceeding 10 business days from the date of entry into the information registry, whether to:

   a) Dismiss the report in any of the following cases:

      1.º When the reported facts are deemed entirely implausible

      2.º When the reported facts do not constitute a legal violation falling within the material scope of the Internal Reporting System.

      3.º When the report clearly lacks any basis or if, in Prisma's judgment, there are rational indications that the information was obtained through the commission of a criminal offense. In this last case, in addition to the dismissal, a detailed report of the facts deemed to constitute a crime shall be forwarded to the Public Prosecutor's Office.

      4.º When the report does not contain any new and significant information regarding violations compared to a previous report for which the relevant procedures have already been concluded, unless new factual or legal circumstances justify a different follow-up. In such cases, Prisma shall notify the Whistleblower of the decision with a reasoned explanation.

   The decision to dismiss the report shall be communicated to the Whistleblower within 5 business days, unless the report was

anonymous, or the Whistleblower waived the right to receive communications.

b) Admit the report for processing:

The admission of the report shall be communicated to the Whistleblower within 5 business days, unless the report was anonymous, or the Whistleblower waived the right to receive communications.

c) Immediately forward the report to the Public Prosecutor's Office if the reported facts appear to constitute a criminal offense, or to the European Public Prosecutor's Office if the case affects the financial interests of the European Union.

d) Refer the report to the relevant authority, entity, or body deemed competent for its processing.

III. Investigation Process

1. The investigation process shall include all actions aimed at verifying the credibility of the reported facts.

2. The person concerned by the information shall have the right to be informed of the information received, of the facts as succinctly stated and of the right to make written submissions, at such time and in such manner as is considered appropriate to ensure the proper conduct of the investigation.

3. In no case will the identity of the informant be communicated to the subjects concerned, nor will access to the communication be given. During the investigation, notice of the communication with a brief account of the facts shall be given to the person under investigation. This information may be provided during the hearing if it is considered that its prior provision could facilitate the concealment, destruction or alteration of evidence.

3. Without prejudice to the right to make written allegations, the investigation shall, whenever possible, include an interview with the person concerned in which, always with full respect for the presumption of innocence, he/she

shall be invited to explain his/her version of the facts and to provide such evidence as he/she considers appropriate and relevant.

In order to guarantee the rights of defence of the person concerned, he/she shall have access to the file without disclosing information that could identify the Informant, and may be heard at any time, and shall be advised of the possibility of appearing with a lawyer.

4. Prisma's staff or external advisors participating in the proceedings must maintain secrecy regarding the information they learn in the course of the proceedings.

IV. Conclusion of Proceedings

1. Once all proceedings have been completed, Prisma will issue a report that will include at least:

   a) A statement of the reported facts along with the identification code of the communication and the date of registration.

   b) The classification of the communication to determine its priority in processing.

   c) The actions taken to verify the credibility of the reported facts.

   d) The conclusions reached in the investigation regarding whether or not a violation of the law, internal regulations, or any other applicable rules has occurred.

2. Upon issuance of the report, Prisma will adopt one of the following decisions:

   a) If no violation is deemed to have been substantiated, the proceedings will be considered concluded without the need for further action, and the case will be archived. The Informant and, if applicable, the affected parties will be notified.

   b) If a violation is deemed substantiated, the case will be forwarded to:

- The relevant internal department to take appropriate action, including the implementation of disciplinary measures or the adoption of corrective or preventive organizational measures, in compliance with the applicable collective agreement or regulations.

- The Public Prosecutor's Office if the facts could constitute a criminal offense, or to the European Public Prosecutor's Office if the offense affects the financial interests of the European Union.

- If the facts could constitute administrative offences, the information shall be forwarded to the competent authority or body.

3. The deadline for concluding the proceedings and providing a response to the Informant, if applicable, shall not exceed three months from the receipt of the information or, if no acknowledgment of receipt was sent to the Informant, three months from the expiration of the seven-day period following the communication. In cases of particular complexity requiring an extension, the deadline may be extended by an additional maximum period of three months. Regardless of the decision, the Informant will be notified unless they have waived this right, or the communication was made anonymously.

4. The conclusion of the proceedings will not prevent the initiation of new actions if additional information is received that justifies it.

Prisma
Agile. Secure. Reliable.

Annex II

Information on Data Protection

1. Data Controller

The data controller for the personal data collected in the Internal Reporting System is Prisma Payments EP, S.A. ("**Prisma**"), with its registered office at Leganitos Street 47, 9th Floor, 28013 Madrid. For any inquiries regarding the protection of your personal data, you may contact Prisma at the following email address: dpo@prismapay.com.

2. Purpose of Processing

The personal data provided through the Internal Reporting System will be processed for the purpose of managing and handling communications regarding actions or omissions that may constitute legal violations, in accordance with Article 2 of Law 2/2023, of February 20, regulating the protection of individuals who report regulatory violations and corruption. The processing will always ensure the confidentiality and integrity of the information, as well as compliance with the principles of necessity, proportionality, and minimization.

The use of the Internal Reporting Channel is voluntary. However, if the whistleblower chooses to include their personal data in the communication, it will be processed in accordance with this clause and in compliance with Law 2/2023. If the report is submitted anonymously, no personal data of the whistleblower will be collected, and they will still be granted the protection and guarantees established by applicable regulations.

3. Legal Basis for Processing

The processing of personal data is based on compliance with a legal obligation, in accordance with Article 6.1(c) of Regulation (EU) 2016/679 ("**GDPR**"), when the report concerns violations of European Union law, criminal offenses, or serious or very serious administrative violations. Additionally, it is based on Prismas

legitimate interest, under Article 6.1(f) of the GDPR, to ensure legal certainty and prevent legal and reputational risks.

4. Confidentiality and Data Recipients

Personal data will be processed with strict confidentiality. It will not be disclosed to third parties, except when necessary for compliance with a legal obligation or for the proper management and processing of the received information. In this regard, it may be disclosed to competent administrative or judicial authorities when required by applicable legislation. Additionally, data may be shared with legal advisors, external auditors, experts, or any other professional necessary for the investigation of the report.

In all cases, Prisma will ensure that any third party with access to personal data within the Internal Reporting System signs agreements that guarantee the confidentiality of the information and compliance with data protection regulations. Under no circumstances will the identity of the whistleblower be disclosed to the reported person, except when expressly required by a judicial or administrative authority as part of a formal investigation.

5. Data Retention and Deletion

Personal data collected in the Internal Reporting System will be retained only for the time strictly necessary to determine whether an investigation should be initiated. If the report is not admitted for processing, the data will be blocked as described below.

If an investigation is initiated, the data will be retained for as long as necessary for the processing of the case and for an additional period of two years after its conclusion. Once this two-year period has elapsed, or if the report is not admitted for processing, the personal data will be blocked, remaining available only for compliance with possible legal obligations or requests from competent authorities. Finally, after ten years from the receipt of the report, the personal data will be permanently deleted.

6. International Data Transfers

Personal data collected in the Internal Reporting System will be stored on servers located within the European Economic Area (EEA). If, for operational reasons, it is necessary to transfer data to third countries outside the EEA, Prisma will ensure GDPR compliance by applying Standard Contractual Clauses (SCCs) approved by the European Commission or other appropriate safeguards that provide an equivalent level of security as required by European regulations.

7. Data Subject Rights

The data subject may exercise their rights of access, rectification, erasure, restriction of processing, and objection under Articles 15 to 22 of the GDPR. However, under Law 2/2023, the exercise of certain rights may be restricted regarding the whistleblower's identity to ensure confidentiality.

To exercise these rights, the data subject may contact Prisma in writing at the postal or email address indicated above. Additionally, for any inquiries related to data protection, they may contact the Data Protection Officer (DPO) at the following email address: dpo@prismapay.com.

If the data subject believes that their rights have not been properly addressed, they may file a complaint with the Spanish Data Protection Agency (www.aepd.es).

Prisma
Agile. Secure. Reliable.

Versions history

Description	Approval	Date
First version	Board of Directors	27.03.2025