Communications Management Procedure

1. Introduction

Maths for More, S.L. (hereinafter, Wiris) has implemented the following internal communications channel as the first-line means available to all managers, employees, collaborators, and suppliers. It can be used through the following form: whistleblowersoftware.com/secure/wiris or by sending a written communication by mail to C/ de Roger de Flor, 221, Bajos, 08025 Barcelona, Attn: Party Responsible for the Internal Information System, or in a face-to-face meeting, sending the meeting request through any of the above means of communication, in order to report any concern regarding possible non-compliance or violation of the provisions of the Code of Conduct or any other internal Policy of the organization. They can also report a violation or omission they are aware of that may constitute an infringement of European Union law or contravene its financial interests, including criminal and/or administrative breaches of Spanish law, as explained in the Wiris Internal Information System Policy.

This document shapes the Communications Management Procedure, which establishes the provisions necessary for the Internal Information System and the internal communication channel to comply with the requirements established in Law 2/2023, of February 20th, which regulates the protection of persons who report regulatory violations and the fight against corruption.

While the internal communications channel is the preferred medium, any natural person may alternatively inform the national Independent Authority for the Protection of the Whistleblower (hereinafter, "AAI") or the corresponding regional authorities or bodies of any action or omission, whether directly or following communication through the aforementioned internal channel and in accordance with the terms established in Law 2/2023.

2. Stages of the Communications Management Procedure

2.1. Receiving Communications

At Wiris, receiving the communications made through the Internal Information System is managed by the COMPLIANCE COMMITTEE, who as the PARTY RESPONSIBLE FOR THE INTERNAL INFORMATION SYSTEM, guarantees that the independence, confidentiality, data protection, and secrecy of the communications will be preserved at all times.

This communication can be made in writing, anonymously or nominally, being confidential in all cases and including the description of the facts or events, the identification of the people involved and, if possible, providing evidence that substantiates the aforementioned instance

of non-compliance, explaining the circumstances under which access to said information was obtained.

If a communication is exceptionally received via any other means besides the Internal Information System, whether verbally or in writing, this will be sent to the communications channel, with the whistleblower's prior consent, either by recording the conversation or by making a complete and exact transcription of it. After it is sent, it will be processed and managed as per this Procedure.

Moreover, if the communication is received through internal channels other than those established by the organization or is sent to staff members who are not responsible for its processing, the organization still guarantees the preservation of the confidentiality thereof, advising that non-compliance implies a very serious infraction of the Law and that the communication should immediately be sent to the Party Responsible for the System.

Once the communication or information is received, the Party Responsible for the System is the body responsible for initiating the corresponding investigation process, in order to clarify the facts or events mentioned in the communication.

The Party Responsible for the Internal Information System guarantees that the independence, confidentiality, data protection, and secrecy of the communications will be preserved at all times.

An acknowledgment of receipt will be sent to the whistleblower within a timeframe of seven (7) calendar days following its receipt. This acknowledgment of receipt will be incorporated into the file, including in every case clear and accessible information on the external information channels before the competent authorities.

In those cases in which sending an acknowledgment of receipt may jeopardize the confidentiality of the communication, the former will not be sent until a timeframe that is considered prudent has elapsed, in order to ensure said confidentiality.

As mentioned in the previous paragraphs, as an alternative to this first-line internal channel, the national AAI or the corresponding regional authorities or bodies can be informed of any action or omission which may constitute any of the infractions likely to be communicated via the Internal Information System[1], whether directly or having first been sent through this internal channel, as per the provisions of Annex 1 on external information channels.

[1] In this respect, see Section 3, "Content of Communications", in the Internal Information System Policy.

2.2 Acceptance Procedure

After receiving the communication, the IT tool assigns it a RECORD NUMBER that corresponds to its file and a series of codes to anonymize both the whistleblower and the party under investigation, plus any third party that may be affected by the communication.

Being a collective body, the Party Responsible for the System shall delegate, in accordance with the nature or field of the communication, the powers to manage the Internal Information System and handle the procedures for the investigation files to one of the members of the Compliance Committee.

If the Party Responsible for the System advises that the facts or events reported may be classified as constituting crimes, they shall send the information immediately to the governing body, who will decide whether or not to immediately send it to the prosecuting authority.

Additionally, it shall be verified that none of the members of the Compliance Committee are implicated in said communication. If this were to be the case, the administrative body shall be informed and the person implicated shall be removed from the proceedings. If it is necessary to replace the person affected, the Compliance Committee shall be who designates their substitute in order to continue with the investigation in the most appropriate manner for the interests of the parties involved. Said substitution and new appointment will be formalized in writing as part of the documents when the case file is created.

Lastly, after receiving the communication, the Party Responsible for the System will record, among other things, the following:

- The objective information to which the communication refers: facts or events, dates, names, quantities or amounts, places, contacts, etc., provided by the person sending the communication.
- The subjective information: opinions, rumors, ideas, and evaluations that the whistleblower considers necessary as part of the account of the communication.
- Evaluation of whether the communication is associated with a possible or alleged infraction or whether it is just a complaint or suggestion related to improving a business area, work situation, etc.

2.3 Investigational Procedure

In the event that the communication is admitted for proceedings, the investigation is directed and carried out by the Party Responsible for the System.

Firstly, and following agreement with the whistleblower, the preventive precautionary measures deemed appropriate are taken.

If possible, the whistleblower may be asked to provide the additional information necessary for the investigation process which his or her communication has engendered.

At this stage, the PARTY UNDER INVESTIGATION is notified and INTERVIEWED. They are notified of their right to be informed of the actions or omissions they are accused of, and they shall be able to exercise their right to be heard. In no case will the identity of the whistleblower be revealed to them.

The third parties involved (if any) are also contacted and interviewed so they can provide explanations and make the statements they consider pertinent. All of the investigational diligences deemed necessary for the parties will be conducted and everything happening in relation with the file will be documented.

The proceedings that are carried out with regard to third parties or other entities, areas, or departments of the organization must be performed while maintaining the anonymity of the WHISTLEBLOWER and the PARTY UNDER INVESTIGATION, and the reasons for the communication must be kept as secret as possible.

The confidentiality of the information will be guaranteed at all times, as will the presumption of innocence and honor of all persons affected. During this stage, the Party Responsible for the System:

1st.- Investigates the facts or events reported and, specifically:

- The objective and subjective elements provided by the whistleblower, prioritizing the objective elements, supported by documentation that accredits, whether in whole or in part, the facts or events reported.
- The reputation, seriousness and credibility of the whistleblower.
- The allegations and exonerating evidence provided by the party under investigation.
- The evidence presented regarding third parties or other related bodies, areas or departments.

2nd.- Analyzes and evaluates the potential consequences that the facts or events reported may have:

Firstly, the Party Responsible for the System checks whether these events or facts occurred due to a significant lack of internal controls in the organization. If necessary, it will propose urgent remedial and preventive measures to avoid further risks.

Secondly, if the seriousness, specifics or complexity of the facts or events makes it advisable, the Party Responsible for the System may appoint another professional manager or a third specialized party to collaborate in the investigation. Likewise, if a consequence of the reported facts or events could be loss of assets, the Party Responsible for the System will adopt measures that aim to stop or mitigate these losses. If a leak or the destruction of evidence related to the communication may occur, the Party Responsible for the System will secure the evidence before initiating the investigation. The Party Responsible for the System also assesses whether the governing bodies should be informed of this communication.

Finally, they check whether there is a possibility that damages have been caused to third parties, in which case they assess the extent of the damage and determine the need to inform the adversely affected third party.

The timeframe for carrying out the investigation and providing a response to the whistleblower on the actions that have been carried out, as well as the result thereof, depends on the seriousness of the facts reported and their potential consequences, the duration of this stage being at the discretion and risk of the Party Responsible for the System. Nevertheless, in accordance with the provisions of article 9.2.d) of Law 2/2023, of February 20th, which regulates the protection of persons who report regulatory violations and the fight against corruption, this timeframe cannot be longer than three (3) months after receiving the communication or, if the whistleblower was not sent an acknowledgment of receipt, three (3) months from when the timeframe of seven (7) days following the communication elapsed[2]. This applies except in cases of special complexity, whose term may be extended up to a maximum of three (3) additional months.

If the communication contains personal data of third parties other than the party under investigation (for example, witnesses, suppliers, clients, etc.), the Party Responsible for the System will state in writing that all personal information provided that is not necessary for the investigation should be deleted, and the third parties whose data is processed should be informed. The information shall meet the information requirements of the data protection regulations, omitting the identity of the whistleblower, which should remain confidential.

All of these notifications are decided on by the Party Responsible for the System and are recorded in the file.

[2] These timeframes shall be complied with, in any case, without prejudice to the provisions of the labor regulations or collective bargaining agreement applicable to each case, whose timeframes shall prevail in the event of contradiction.

2.4. Finalizing the Proceedings

After investigating the communication and using the supporting documentation that will serve to clarify the facts or events, a VERDICT or DECISION is made, with the following content:

- Description of the facts or events: record no. of the communication, date of the communication, facts or events reported, parties involved, documentation provided over the course of the investigation by both parties (whistleblower and party under investigation), by other bodies, areas, and departments, and by third parties, interview with the party under investigation and/or with third parties, etc.
- Analysis and evaluation of the evidence obtained.
- If the impropriety reported is found to be true, the Party Responsible for the System shall dedicate a section of the verdict to make the recommendations that they consider necessary to improve the internal controls and protocols that were not sufficient to prevent the issue(s) on this occasion.
- Decision: with the approval of the governing bodies, this decision is substantiated and contains the reasons for the following outcomes: FILE CLOSURE WITHOUT PENALTY or FILE CLOSURE WITH PENALTY.

I. FILE CLOSURE WITHOUT PENALTY: After the investigation, if it is concluded that the infraction reported is clearly minor and does not require further follow-up, the FILE IS CLOSED. File closure also applies in instances of duplicate communications that do not contain new and/or significant information regarding previously reported infractions and whose investigation proceedings have already been concluded, unless new circumstances arise de facto or de jure that warrant a different follow-up. In these cases, the whistleblower must be notified of the resolution and it should be duly justified.

II. FILE CLOSURE WITH PENALTY: the Party Responsible for the System can propose a penalty, but the decision rests with the governing body, in coordination with the human resources department, based on the procedures indicated for applying work-related sanctions or punishments in the organization.

III. NOTIFICATION TO THE AUTHORITIES: If the communication received seems to be related to a crime being committed, the Party Responsible for the System will

immediately notify the appropriate government body so that it can evaluate whether or not to report it to the prosecuting authority.

In this sense, art. 259 of the Spanish Criminal Procedure Law states that whoever witnesses any public crime[3] must immediately make it known to the nearest investigating judge, justice of the peace, district or municipal judge, or prosecuting official, under penalty of a fine of 25 to 250 pesetas[4].

Nevertheless, the duty to report to the competent authorities is even greater for certain crimes, as specified in criminal law. In this respect, art. 450[5] of the Spanish Criminal Code provides for the "omission of duties to prevent crimes or to promote their prosecution", thus punishing any person who does not prevent the perpetration of a crime that affects peoples' life, integrity, health, freedom, or sexual freedom, as long as they could do so through immediate intervention and without putting themselves or others at risk. It also provides for punishing any person who, being able to do so, does not seek out the authorities or their agents in order to stop one such crime they are aware is about to happen or has happened.

Therefore, if the truthfulness of the facts or events is confirmed once the investigation is concluded, all of the measures necessary to put a stop to the fact or event reported shall be taken. If appropriate and if the characteristics of the fact or event so warrant, the appropriate actions shall be taken, from among those included in the disciplinary regime and the current labor laws, in accordance with criminal law.

---

[3] The classification of a crime as public is related to who is in charge of prosecuting it (public prosecutors or prosecutors for the aggrieved party), with public crimes being prosecutable by public prosecutors without requiring a lawsuit brought by the aggrieved party. This also includes crimes that endanger life and liberty. In the catalog of crimes that engender criminal responsibility for the legal person, we find the following non-inclusive list of public crimes: fraud, bribery, influence peddling, money laundering, financing terrorism, crimes against the public treasury and social security, crimes against the environment and natural resources, crimes against land planning, crimes against fundamental rights and public freedoms, contraband, etc.). By contrast, slander and insults between individuals are private crimes (the justice system can only act when the aggrieved party files a lawsuit or grievance) and semi-public crimes are actionable ex officio once the aggrieved party has filed the initial lawsuit (crimes regarding the revelation or disclosure of secrets, crimes against intellectual property, assaults, harassment, sexual abuse, collation, among others).

[4] According to the current literal wording of art. 259 of the Spanish Criminal Procedure Law.

[5] Art. 450 of the Spanish Criminal Code: "1. Any person who, being able to do so through immediate intervention and without putting themselves or others at risk, does not prevent the perpetration of a crime that affects peoples' life, integrity, health, freedom, or sexual freedom, will be punished with a prison sentence of six months to two years if the crime put life in jeopardy and a fine of six to twenty-four months in all other cases, unless the crime not prevented carries a punishment that is the same or less, in which case the punishment imposed for not preventing it shall be less than the punishment for said crime. 2. The same punishments shall apply to whom, being able to do so, does not seek out the authorities or their agents in order to stop one of the aforementioned crimes they are aware is about to happen or has happened.

The measures that may be imposed internally do not limit, at any time, the exercise of the legal actions that the organization may carry out.

In all cases, the DECISION will be NOTIFIED to both the whistleblower and the party under investigation, taking into consideration the maximum timeframe of three (3) months from the communication being received. They will not be notified if they have withdrawn the allegation, there is no contact information, or it is an anonymous whistleblower.

Following this, the Party Responsible for the System will order the FILE CLOSURE, respecting in all cases the current legislation on data protection.

In the case of FILE CLOSURE WITH PENALTY, the notification to the party under investigation will contain the adoption of the contractual, disciplinary, or judicial measures that should be adopted.

As stated in its Internal Information System Policy, Wiris guarantees that no retaliation will occur against anyone who in good faith reports an illicit event, collaborates in the investigation thereof, or helps resolve it. This guarantee does not apply to individuals who act in bad faith in order to spread false information or cause harm to people. The organization shall adopt appropriate legal and/or disciplinary measures in response to these illicit behaviors.

3. Record of Communications

The Party Responsible for the System has a record book for the information received and the internal investigations that have taken place. This enables the storage and/or recovery of key information about each incident, including the date and source of the original communication, the investigation plan, results of the interviews or any other investigational procedure, pending tasks, final decision, as well as the chain of custody of any evidence or key information.

4. Personal Data Protection

As stated in the Wiris Internal Information System Policy, the processing of personal data derived from the application of said Policy and of this Communications Management Procedure is governed by the provisions of Section VI of Law 2/2023, those of Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27th, 2016, those of Organic Law 3/2018 of December 5th, on the Protection of Personal Data and the guarantee of digital rights, and those of Organic Law 7/2021 of May 26th, on the protection of personal data processed for the purposes of the prevention, detection, investigation, and judgment of criminal offenses and the enforcement of criminal penalties.

Considering the data minimization principle of the General Data Protection Regulation for the information covered by Law 2/2023, the organization will only process the personal data necessary for the knowledge and investigation of the actions or omissions subject to investigation through the Internal System. Consequently, insofar as the personal data collected is not deemed necessary, or if it can be proven that the information is untrue, Wiris will proceed to delete the data under the terms established in article 32 of Law 3/2018[6].

In addition, the organization may only process data of a special category[7] when it is necessary for the adoption of the corresponding corrective measures or sanctioning procedures that should eventually take place. Otherwise, it should immediately be deleted as per the terms mentioned above.

Lastly, Wiris should guarantee that the subjects affected by the processing of personal data carried out as a result of the investigation can exercise their rights of access, correction of inaccurate data, deletion, limitation of use, portability, opposition to use and the right to not be subjected to a decision based solely on automatic processing. The following should be borne in mind for the exercise of rights: the right to access may not include information regarding the whistleblower, and regarding the right to opposition, the parties under investigation may decline for legitimate reasons.

5. Approval

This Communications Management Procedure has been approved by the governing body of Maths for More, S.L. and may be modified to improve the confidentiality and effectiveness of the management of the reports received.

In addition, this Procedure is reviewed and/or modified by the Party Responsible for the System, who may outsource the service to specialists:

- Whenever there are important changes in the organization, in the control structure, or in the activity carried out by the entity that make this advisable.

[6] When proceeding to deletion, the data will be blocked, adopting all of the measures necessary to prevent the processing of the blocked information (except it being made available to the judicial authorities, prosecuting authorities, or competent public administrations for the assumption of potential liabilities) during the time necessary to maintain evidence of the operation of the system, which as per the statutes of limitation indicated in Law 2/2023, is set at 3 years.
It is worth mentioning that the obligation to block and conserve does not apply to the personal data contained in communications that are not investigated, which can only be conserved anonymously.

[7] Personal data that reveals the ethnic or racial origin, political opinions, religious or philosophical convictions, or labor union affiliation, and the processing of genetic or biometric data and data related to the health, sex life, or sexual orientation of a person.

- Whenever there are legal changes that make this advisable.
- Whenever important violations of its provisions occur that make this advisable.

This Policy will be reviewed periodically, even when none of the circumstances described above have occurred.

6. Version History

Version	Date	Approved by	Reason for change
Original V.	29/11/2023	Compliance Committee	