INTERNAL INFORMATION SYSTEM POLICY - REPORT2BOX

Whistleblowing Channel

CONTENTS

1. Purpose, Scope of Application and Guiding Principles

1.1. PURPOSE AND AIM

The purpose of this Policy is to explain how the company's Internal Information System (hereinafter, IIS or Whistleblowing Channel) works to all users and how they may access it as well as all the functional features. In other words, the general principles of operation, as well as the principles of informant defense.

The Whistleblowing Channel is a tool through which anyone at the company; in other words, members of the governing body, management and employees, as well as third parties with or who have had an employment or professional relationship with it, may inform the company of possible risks and breaches of its standards (legal and internal) they may become aware of (thus, they are considered informants or whistleblowers).
Said third parties; in other words, those who should be allowed to file a report, should be at least the shareholders, investors and members of the governing body, including non-executive members, the self-employed, any person who works for or under the supervisor of contractors, subcontractors and suppliers as well as former employees, interns, candidates for hire or those engaged in precontractual negotiation processes, volunteers and workers in training at the company.

Among others, the main idea is to create a mechanism to guarantee compliance with the law and the efficacy of the Code of Ethics as well as the company's internal policies to prevent them from being simple declarations of intent.

Moreover, the use of this Channel may allow the company to adjust its activities to the regulations in effect, guarantee compliance with internal policies and reduce risks in-house as well as the commission of crimes or unlawful conducts and, therefore, protect its employees.

1.2. SCOPE OF APPLICATION AND BINDING NATURE

Objective scope of application. What can and cannot be reported through the IIS?
Communications received through the Whistleblowing Channel must refer to actions or omissions that occur within the company's scope of action and which constitute a labour or professional breach of a rule or principle affecting the company. In any case, the following must be reported:

Conducts that constitute serious or very serious crimes or administrative violations; for example, fraud, the improper payment of a commission or non-payment of taxes;

a) Any actions or omissions that may be considered violations of European Union Law whenever:
   - The situation involves public procurement; services, products and financial markets as well as the prevention of money laundering and terrorism financing; product safety and conformity; transport safety; environmental protection; protection from radiation and nuclear safety; the safety of food and

feed, animal health and wellbeing; public health; consumer protection; the protection of privacy and personal data, and network and information system security
- A situation may affect the European Union's financial interests or
- Have an impact on the internal market such as, for example, violations of European Union regulations on trade and aid granted by the States.

b) Any breach of company policy, as well as its principles and values;
c) Any event that may be considered an ethical dilemma;
d) Any event that may compromise the company's reputation.

Incidents that should not be reported include any events not included in this section such as matters closely associated with Human Resources or personnel policies (i.e., holidays, remuneration, employee relations, interpersonal conflicts, etc.), recommendations or suggestions not linked to regulatory compliance matters or the provision of the company's services.

If the informant has any doubts about the nature of the event in question and, as long as they are acting in good faith, the event may be reported without any problem. The IIS Manager will review the content and analyse the acceptability thereof and then inform the informant.

Concerns

If the recipients of this Policy have any questions regarding regulatory compliance or the very use of the Whistleblowing Channel (i.e., how to interpret a standard or respond to a specific event), they may be addressed to **compliance@masats.es**

Subjective scope of application. Who is this Policy aimed at?

This Policy is aimed at company shareholders as well as anyone who, in any manner, provides the company with employment or professional services; in other words, investors or members of the governing bodies, management, supervisors including non-executive members, employees and habitual external collaborators (as detailed in art. 1.1), as well as any person who may act in the name and on behalf of the company and third parties without any geographic limitations. The Policy will also be applicable to (i) all of them whether they are considered the informant or the reported party or a witness, and (ii) the authority responsible for receiving and/or processing reports that may be received via the Whistleblowing Channel; in other words, the IIS Manager (hereinafter, the Manager).

Binding nature:

Respect hereof is an employment or contractual obligation for everyone (except third parties) meaning any failure to respect it may be sanctioned pursuant to the provisions of labour laws in effect in the location where the company operates (i.e., the applicable Collective Bargaining Agreement), as well as the corresponding contractual document or standards.

All recipients of this Policy are required to report any incidents they gain knowledge of through the means set forth in the following chapter.

1.3. LEGAL NATURE

The organization, use and operation of the Whistleblowing Channel shall be governed by this Policy which will be supplemented by the Procedure on Handling Information received. Likewise, all rules and regulations issued by the authorities or government agencies related to whistleblowing channels and other standards that may regulate aspects of such shall be observed (i.e., laws regulating personal data protection and the prevention of money laundering and terrorism financing, and in particular all those regulating the protection of fundamental rights).

1.4. GUIDING PRINCIPLES

The implementation of the Whistleblowing Channel comes in response to the company's will to establish a zero-tolerance commitment to the commission of crimes, administrative violations, breaches of the law and respect for legality and best practices.
In accordance with the foregoing, the procedure for handling communications received through the Whistleblowing Channel shall always respect the following principles:

Confidentiality: all information processed through the Whistleblowing Channel shall be considered confidential and shall be handled as such. The confidentiality of the informant's identity shall be guaranteed, as well as that of any third party mentioned in the communication as well as in any actions taken as part of the processing thereof; only authorized personnel shall have access to it;
Indemnity and ban on retaliation: good faith users of the Whistleblowing Channel shall enjoy protection from the company, the authorities as appropriate and shall never be subject to any type of retaliation for properly using the Channel;
Impartiality: the Manager must always observe and handle the information submitted objectively and impartially; and
Trust: the company shall generate trust in the use of the Channel among all parties concerned so that it can be as effective as possible.

2. Reporting incidents: How can a report be submitted?

2.1. MEANS FOR REPORTING INCIDENTS

The recipients of this Policy may submit the reports mentioned in 1.2 above through the company's Whistleblowing Channel; in other words, through the Report2Box platform by Datax which is accessible via this link: https://masats.report2box.com

If the informant so requests, they may also submit their communication through an in-person meeting with the Manager within a maximum of 7 days from such request.

For the purposes of ensuring the confidentiality of the channel, only the people listed herein shall have access to the reports submitted as they are the ones responsible for the management and processing thereof: the **Best Practices Committee** will receive all reports that may be submitted through the aforementioned platform immediately. If the report is appropriate, the Best Practices Committee will be notified to begin the corresponding investigations. Moreover, the Report2Box platform by Datax will always be password-protected and all passwords must be changed every 3 months and only known to the parties mentioned herein. These tools and any other may be used to process the reports. Moreover, they shall be equipped with the necessary technical and security measures to guarantee the confidentiality of the Whistleblowing Channel.

The foregoing include all of the company's internal resources through which any report may be submitted as they are the preferential means of use. However, informants may also address their reports to an external body: the Independent Informant Protection Authority (AAI, as it is known in Spanish) or any other authority with the power to receive such reports.

If any person at the company other than the IIS Manager receives a report through any means, they must immediately submit it to the Manager and maintain absolute confidentiality with respect to the information received.

2.2. BASIC INFORMATION

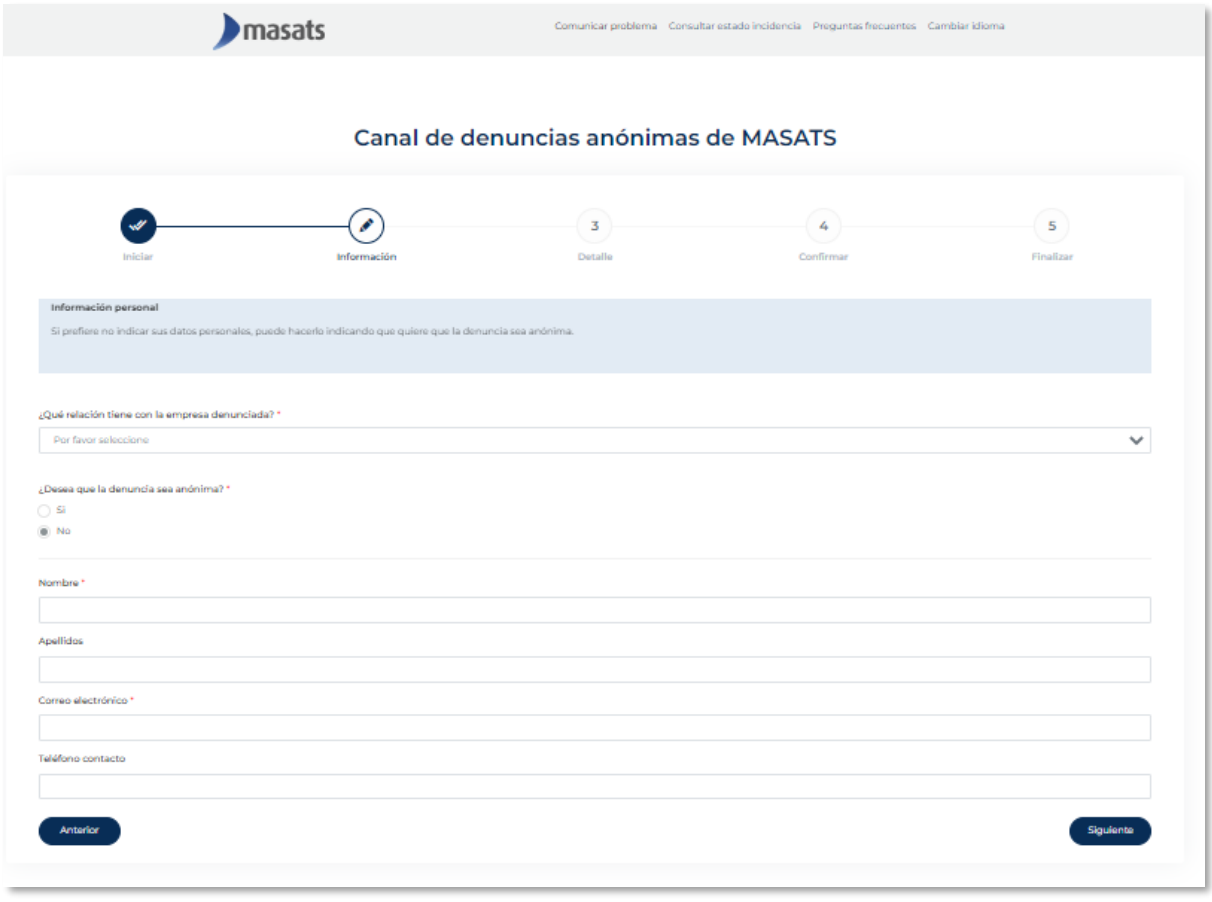
Reports communicated through the Whistleblowing Channel must include the following information at the very least:

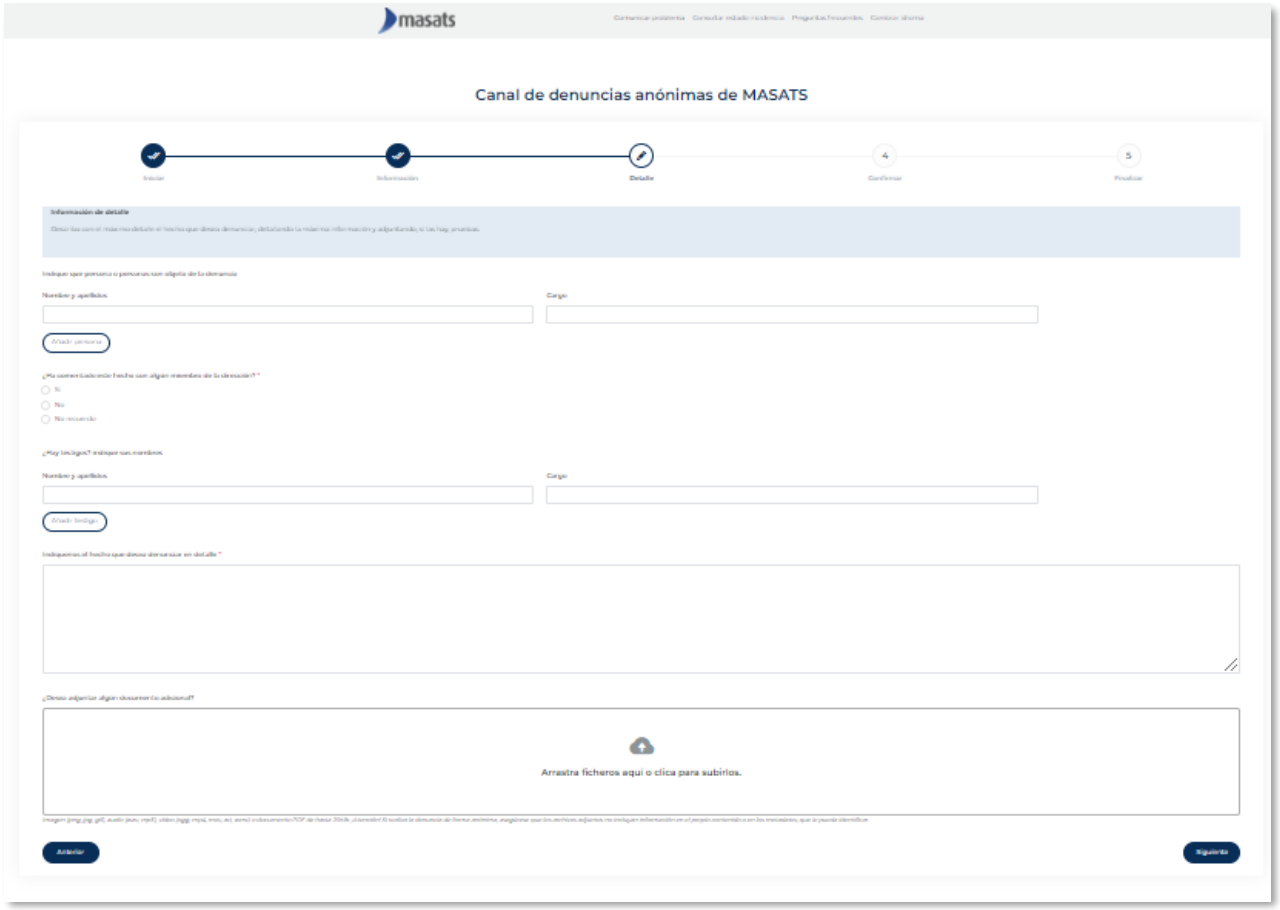
- The event, conduct or irregularity communicated, as well as the date on which it occurred. No legal assessment or classification of the event investigated will be requested from the informant although the latter must have reasonable grounds to believe the event communicated is true;
- The reason why the incident is considered odd or irregular;

- The identity of the people responsible for the foregoing if known (reports may be submitted with regard to unknown subjects if they can be identified);
- All evidence available with regard to the event or irregularity committed (however, the informant is not required to provide proof). Under no circumstance may any evidence violate any fundamental rights or the law. If there are any doubts, the informant shall refrain from obtaining the evidence without the advice of the Manager or a third party deemed appropriate;
- The identification of the informant although anonymous reports are also acceptable. If an anonymous report is received through the whistleblowing channel, the information received will be handled with the necessary caution required for such communications and without such circumstance preventing the application of this Policy. In such a scenario, it is important to remember that this Report2Box platform by Datax enables constant communication with the anonymous whistleblower through a tracking code which will be provided by the platform. It is important to **remember that, if the anonymous whistleblower loses the tracking code, it may not be recovered and, therefore, they will not be able to track their report**.

All of the foregoing is requested on the Report2Box homepage and only the enabled areas should be completed. See, for example:


masats
Comunicar problema
Consultar estado incidencia
Preguntas frecuentes
Cambiar idioma
Canal de denuncias anónimas de MASATS
Iniciar
2
Información
3
Detalle
4
Confirmar
5
Finalizar
Tipificación denuncia
Para facilitar la posterior gestión de su denuncia, ayúdenos a categorizarla lo mejor posible.
¿En qué categoría encaja mejor su denuncia? *
Competencia
Conductas inapropiadas: Soborno, Acoso Sexual, Acoso Laboral, Coacciones, Corrupción
Conflicto de intereses
Contratación pública
Prevención del blanqueo de capitales
Protección del medioambiente
Protección de los consumidores
Protección de los datos personales y la intimidad
Respeto a los derechos humanos
Seguridad de las redes y sistemas de información
Seguridad en el transporte
Seguridad en los productos
Otros
¿Sospecha de alguna de las siguientes personas? *
Director de Compras
Director de RRHH
Director Financiero
Director General
Responsable de Operaciones
No me consta implicación de estas personas
He leído y acepto los Términos de uso. *
Siguiente


masats
Comunicar problema
Consultar estado incidencia
Preguntas frecuentes
Cambiar idioma
Canal de denuncias anónimas de MASATS
Iniciar
Información
3
Detalle
4
Confirmar
5
Finalizar
Información personal
Si prefiere no indicar sus datos personales, puede hacerlo indicando que quiere que la denuncia sea anónima.
¿Qué relación tiene con la empresa denunciada? *
Por favor seleccione
¿Desea que la denuncia sea anónima? *
Sí
No
Nombre *
Apellidos
Correo electrónico *
Teléfono contacto
Anterior
Siguiente


masats
Canal de denuncias anónimas de MASATS
Arrastra ficheros aquí o clica para subirlos.


masats
Comunicar problema
Consultar estado incidencia
Preguntas frecuentes
Cambiar idioma
Canal de denuncias anónimas de MASATS
Iniciar
Información
Detalle
Confirmar
5
Finalizar
Confirmación
Como último paso del proceso debe indicar una clave secreta que solo ud. conocerá. Esta clave, junto al código de identificación que le indicaremos al finalizar serán los únicos medios para poder seguir la evolución de su comunicación
Clave de acceso
Confirmación de clave acceso
Anterior
Siguiente


masats
Comunicar problema
Consultar estado incidencia
Preguntas frecuentes
Cambiar idioma
Canal de denuncias anónimas de MASATS
Iniciar
Información
Detalle
Confirmar
Finalizar
Finalizar
Ya ha introducido toda la información necesaria para iniciar el proceso de gestión de denuncias.
La información está lista para iniciar el proceso de depuración de responsabilidades. Las personas o hechos denunciados serán investigados y las acciones resultantes serán llevadas a cabo.
El denunciante se compromete a la veracidad de los datos aportados en esta denuncia. En caso contrario, la empresa se reserva el derecho de poder iniciar acciones legales en su contra.
Este es el último formulario del proceso, al pulsar Enviar se iniciará la investigación, en un plazo máximo de 3 meses se llevará a cabo la resolución de su denuncia la cual quedará reflejada en la plataforma.
He leído el Aviso sobre protección de datos y consentimiento y acepto el procesamiento de mis datos personales de conformidad con lo dispuesto en dicho aviso. *
Anterior
Enviar


masats
Comunicar problema
Consultar estado incidencia
Preguntas frecuentes
Cambiar idioma
Canal de denuncias anónimas de MASATS
Información enviada
Gracias por utilizar la plataforma de denuncias. Su denuncia ha sido comunicada y en breve recibirá información.
Anote el código de denuncia para poder consultar la evolución de la misma:
Código Denuncia: 24ee44ff-2eba-4687-b4d1-447183172a10
Con la clave que ha generado en el paso anterior y este código, se puede conectar en cualquier momento al portal de denuncias en Consulta estado de denuncia. y consultar el estado de la misma.
Para garantizar la privacidad de la información, desde la plataforma no se le informará de nada, debe de ser ud. el que se conecte y compruebe la información.
Finalizar
Imprimir

To check the status of a report, you must access the Check the status of an incident section and enter the report code and user-generated password.

Employees may also access the instructions of use for the Channel through the explanatory video you can find at this link: https://youtu.be/3zh5g7kG15g

In any case, the informant is required to submit an accurate and truthful report without prejudice to the fact the information submitted may only include suspicions of a violation mentioned in section 1.2. The use of the Whistleblowing Channel in poor faith such as, for example, submitting false or baseless reports is prohibited and will be sanctioned by the company.

2.3. INCOMPATIBILITIES

If the report directly or indirectly affects the Manager, the Report2Box platform allows submitting it to a second manager in order to designate a substitute to handle the management of the report for the person in a situation of incompatibility.

When such a situation of incompatibility occurs with the Manager, any failure by said person to refrain from their duties will be considered a very serious violation of this Policy with the resulting employment or contractual sanctions that may be applied.

3. Informant defense and obligations

3.1. INFORMATION DEFENSE AND OBLIGATIONS

Through the Manager, the company will ensure protection for any good faith informant who uses the Whistleblowing Channel as set forth in this Policy through the following principles of action:

a) It shall guarantee and process their identity confidentially as well as the identity of any persons mentioned in the report filed and those involved with the events described. This means only the persons authorized and identified above may access the information relating to the report and they may not share it with any other third party.
b) It shall guarantee anonymity in cases where the report is submitted anonymously. In other words, when the whistleblower submits a report anonymously, their identity shall never be disclosed as guaranteed through the Report2Box platform which is managed by a third party not associated with the company.
c) It shall provide an interpreter or translated documentation when needed by the informant in order to understand the scope of their rights and obligations, as well as the use of the Whistleblowing Channel.
d) It shall absolutely prohibit any type of retaliation, including threats of retaliation and attempted retaliation due to the information that may be submitted by the informant for investigation. In other words, if a good faith informant is subject of any type of retaliation due to cooperation with the company, the subject in question will be immediately sanctioned.

At the same time, the informant must remember the following obligations when using the Whistleblowing Channel:

a) Honest reporting.
b) Not reporting false events or those manifestly contrary to the truth.
c) Providing as much detail as possible concerning the events reported and collaborating with the investigation.
d) Tracking the report submitted in order to remain informed of the process and provide clarifications or respond to demands for information as appropriate.
e) Respecting the confidentiality of the information provided and the very existence of the report and the later processing procedure.

Likewise, the company shall ensure the rights of the person reported such as, for example, their right to honour, presumed innocence, their right not to be subject of prospective investigations and to have access to the accusations against them as well as to be heard. All of this shall be set forth in the Procedure on Handling Information received which supplements the content of this section.

3.2. ESSENTIAL PRINCIPLES OF THE PROCEDURE ON HANDLING INFORMATION

When the IIS Manager receives a report through the Whistleblowing Channel and, without prejudice to the content of the Procedure on Handling Information received, they must begin the internal investigation of the reported events under the following essential guiding principles:

a) They will study the events included in the report received and first conduct an analysis of the truthfulness. In other words, they will check whether the reported events must be investigated or not and thus decide whether the report shall be admitted for processing or rejected. They shall notify the informant of such decision.
b) If the report passes the truthfulness filter mentioned, the Manager shall begin an internal investigation using the investigation procedures deemed necessary such as, for example, interviews with the whistleblower (if not anonymous), witnesses and the reported party and/or analysing any documentation that may be necessary.
c) Throughout all investigations carried out, the rights and guarantees set forth in this Policy, in the Procedure for Handling Information received and in the law such as, for example, proportionality, impartiality, independence and rights of defense, the presumption of innocence, honour and contradiction of the parties affected by the investigation must be respected at all times.
d) Finally, they shall issue a report on the events analysed with conclusions assessing the facts observed and a final conclusion. As appropriate, the Manager may also include proposed measures for improvement with regard to company processes in the report.
e) Based on the conclusions reached by the Manager as established in the report, the company shall analyse whether disciplinary or contractual measures shall be taken or even legal action.

4. Communication

4.1. COMMUNICATION

A copy of this Policy shall be delivered electronically (i.e., via the intranet) or on paper to all recipients so they may all be aware of their obligations, rights and guarantees in relation to the use of the Whistleblowing Channel. In any case, easy and continuous access to this Policy for all recipients shall be guaranteed via the company intranet or welcome pack. If the recipients of this Policy do not speak Spanish, a translation thereof must be provided in a language they understand. Proof of delivery of this Policy to all users shall be saved.

Moreover, this Policy shall be published on the company's main website in a separate and easily identifiable section for easy access.

4.2. INTERPRETATION

If there are any doubts about the interpretation of this Policy, queries shall be sent to the Manager via the email address indicated herein so they may be resolved.

4.3. TRAINING AND AWARENESS

Furthermore, the company must provide specific training supported by this Policy on the use of the Whistleblowing Channel to all personnel. All such training shall include in any case the following items:

- The existence of a Whistleblowing Channel at the company for the purposes described herein;
- How to properly use the Whistleblowing Channel and the process for such use;
- The rights and obligations of Whistleblowing Channel users;
- The obligation for the recipients of this Policy to report to the company any of the events described in section 1.2.

The company shall also ensure specific training on the management of the Whistleblowing Channel to those responsible for receiving reports and processing them, in this case, the IIS Manager.

The company will save all evidence of courses and other training or awareness activities that may be taken by all Whistleblowing Channel users.

4.4. COMMITMENT BY THE RECIPIENTS OF THE POLICY

All company personnel must know the Policy, actively contribute to respecting it and report any breaches they become aware of as well as any failures they may observe in the content or implementation hereof. The company's governing body shall particularly ensure these obligations.

5. APPROVAL, ENTRY INTO FORCE AND CHANGES IN THE POLICY. PROOF

5.1. APPROVAL AND ENTRY INTO FORCE

Approval and entry into force:

This Policy shall be approved by the Best Practices Committee. The date of approval shall be recorded in the same document. That shall be the date after which the document will enter into force at the company.

5.2. MONITORING, ONGOING ADAPTATION AND UPDATES TO THE POLICY

Monitoring and ongoing adaptation:

Periodic revisions of the content of the Policy shall be established to guarantee constant adaptation to the company's reality, legislative and case law changes, etc. Moreover, the use hereof shall be monitored and the performance of the Whistleblowing Channel may be measured by means of indicators. All of the foregoing is in application of the principle of ongoing improvement which governs the company's processes.

Changes:

The Best Practices Committee may modify the Policy at its own initiative and/or upon a suggestion by any recipient thereof.

5.3. CUSTODY OF EVIDENCE

The Manager shall ensure proper custody of all evidence providing the training activities, oversight, supervision and corrections by the company pursuant to the foregoing. This shall be done in coordination with the personal data protection regulations applicable to each area of the company.

6. PERSONAL DATA PROTECTION

To ensure compliance with personal data protection laws and, in general, to prevent the improper use of the information, the company shall guarantee the following throughout any Whistleblowing Channel management and procedural processes that may be initiated and with respect to the informant as well as the party investigated or any third parties:

- The personal data obtained under this Policy shall only be accessible to the **Internal Reporting System Manager**, the data processors designated and the Data Protection Officer. They must keep all such data confidential and may not under any circumstance use them for purposes not directly associated with their

duties of managing and implementing the Whistleblowing Channel. No personal data will be compiled when not pertinent to a specific report and any data accidently compiled will be deleted without undue delay. If the information received includes data which fall under special data categories, they shall be immediately deleted.

- Only if cautionary or disciplinary measures are taken against any recipient of this Policy will access to the personal data be granted to the HR Manager or competent authority. Likewise, if disciplinary measures are taken, access will be granted to the entity's or organization's Legal Affairs Manager.

- The necessary technical and organizational measures shall be taken to preserve the identity and guarantee the confidentiality of the data corresponding to people affected by the information supplied, especially of the person who reported the events to the company, if they are identified.

- The informant's identity may only be communicated to the Court Authorities, Public Prosecutor's Office or the competent administrative authority as part of a criminal, disciplinary or sanctions investigation.

- Personal data shall only be collected and saved, as applicable, in the reporting system to the extent and for the time necessary to decide upon the admissibility of a procedure or investigation into the reported events and to implement them.

  In any case, data may be anonymized (without being subject to a blockage obligation) three months after they are entered in the Report2Box platform if no investigation is initiated; in other words, when the reports are not accepted for processing.

- All data controllers must have a record of all information received and the internal investigations conducted. Personal data may only be saved for the period necessary and under no circumstance longer than ten years.

- The purpose of collecting such data is to be able to investigate, detect and correct possible breaches or inappropriate conducts within the company, particularly as relates to criminal and regulatory compliance.

- To the extent the personal data are obtained from any procedure, they shall be included in the company's information systems to manage the Whistleblowing Channel. Data subjects may exercise the rights mentioned in articles 15-22 of the General Data Protection Regulation (however, affected individuals will not be given access to the communication under any circumstance). For such access, they must write to *MASATS, S.A. assigned tax identification number: A08207904, and with a registered address of C/ Mestre Alapont, (P.I. Salelles) 08253 Sant Salvador de Guardiola (Barcelona),* indicating the specific request and attaching a photocopy of the requesting party's national identity document.

- The provisions of article 32 of Spanish Law 10/2010, of 28 April, on the prevention of money laundering and terrorism financing will be respected when the exercise of rights affect a report relating to the prevention of money laundering or terrorism financing.

- If a data subject wishes to directly contact the company's Data Protection Officer in order to file any type of complaint, query or question, they may do so in writing, indicating their personal data, at the email address masats@masats.es.

- For more information on our Privacy Policy, please access the following link: https://www.masats.es/politica-privacidad/

CHANGE LOG

The following table reflects the various versions of the Manual that have been created as well as the date and later changes each of the document versions may include:

Version	Prepared by	Reviewed by	Description	Date
1.0	Datax	Mar Alapont	Initial version	June 2023

ANNEX I

Definitions

a) **Whistleblowing Channel:** the tool the company makes available to all personnel and third parties so they may securely, confidentially and/or anonymously report events that may constitute a crime or a serious or very serious administrative violation. Moreover, they may also report events that may be considered a breach of internal policy, an event that may affect the company's reputation or that may involve an ethical dilemma.

b) **Informant, whistleblower or reporting party**: the person who, after identifying themselves or anonymously, communicates any of the foregoing events to the company. This person may be company personnel or a third party. It must be taken into account that Spanish Law 2/2023, of 20 February, regulating the protection of people reporting regulatory violations and corruption matters only protects those with an employment or professional relationship with the company who report an event constituting a criminal or serious or very serious administrative offense. This is without prejudice to any protection that may be provided to the informant through other regulations.

c) **Reported person:** the person who allegedly engaged in the reported events. This person also has certain rights as set forth in the Procedure on Handling Information received.

d) **Internal Reporting System Manager:** the person or persons designated by the company's governing body who is/are responsible for managing and/or processing the Whistleblowing Channel and any subsequent internal investigations that may be carried out.

e) **Retaliation:** any acts or omissions prohibited by law or that directly or indirectly involve unfavourable treatment putting the persons suffering from them at a particular disadvantage in comparison to another person at work or professionally, simply due to their status as an informant or for having made some type of public disclosure. This includes, for example, dismissal, non-promotion, changes in one's job post, etc.

ANNEX II

Receipt of the Internal Information System Policy

By signing this document, I certify I have received, read and understood the Internal Information System Policy. I further agree to respect it and comply with it.

Likewise, I understand that any breach of the content may lead to a disciplinary sanction by the company.

I hereby also agree to remain up-to-date on all changes in the Policy as well as read future modifications that may be made.

DATE:

NAME:

SIGNATURE: