ETHICS CHANNEL OPERATING POLICY

APPROVED BY THE GOVERNING BODY:

July 2022

AMENDMENT CONTROL

VERSION – SECTIONS	REMARKS – DATE
V.0. Initial document	Prepared, supervised and approved by the CB and by the Governing Body on 07/2022

INDEX

1. PURPOSE AND OBJECT

The Governing Body of KLEMARK S.A. (hereinafter KLEMARK or the Organisation), has shown its determination to make decisions for effective implementation of a Compliance System in which its Ethics Channel is configured as one of the main pillars.

The objective of the Ethics Channel is to receive and effectively process notifications regarding behaviour that, essentially, breaches the principles considered in its Code of Ethics and other documents that comprise its Integral Compliance Management System.

To that end, this Operating Policy of the Ethics Channel, records the matters related to management and formalisation of the notifications received, including a flexible, agile model in keeping with the legal regulations in force, standards and best national and international practices, making a distinction between ordinary channels and others called alternative ones through which potential whistle-blowers may explain events that constitute breaches of the Compliance System without fear of reprisal or suffering from harmful conduct.

This Policy, along with its internal investigation and response procedure, is aimed at guaranteeing professional, confidential, impartial management and maximum protection during the whole process, thus generating a climate of confidence for the parties concerned.

2. SCOPE

This Policy is applicable to all the activities and compliance is mandatory for all members of KLEMARK, regardless of the office or post they hold within the organisation, the juridical nature of their relationship and their geographic location.

On the other hand, the Policy shall include third parties, business partners, foreign subsidiaries, non-controlled subsidiaries and, in general, any person who aims to report or provide knowledge of the existence of any infringement related to KLEMARK.

3. OPERATING RULES

3.1. What may be reported?

Information on infringements or non-compliances in an ample sense, that is, reasonable suspicion, real or potential infringements, that may have arisen or that may probably happen.

For illustration, the following is a description of some possible matters to be reported:

- Bribery and corruption;
- Conduct against health and safety in the workplace;
- Conflicts of interest in any action related to personal performance;
- Discrimination, as well as sexual and labour harassment;
- Internal fraud;
- Cases of unfair competition;
- Breaches in matters of defence of competition;
- Undue use of the company's assets;
- Conduct that endangers the health and safety of our users;
- Irregularities in tax or accounting matters, or that compromise the integrity of the business and financial records.
- Disclosure of information when such disclosure may affect the interests of KLEMARK or legitimate rights of third parties;
- Cyberattacks;
- Acts that harm the environment or breach the regulations on town planning and territorial organisation matters;
- Actions against human rights;
- Among others.

3.2. When must it be reported?

It must be reported when the whistle-blower has reasonable cause to believe that the information being provided is true and liable to be considered an infringement or non-compliance. The report must always be submitted in good faith.

3.3. What happens in urgent cases?

Limitation of the reports submitted through the different channels KLEMARK has requires the body in charge of receiving – the Compliance Technical Unit -, to carry out an initial classification, according to the severity and critical nature of the content, in order to be able to prioritise processing.

It is recommendable in urgent cases, as long as the context allows such, to make sure the hierarchical superior and/or Regulatory Compliance Management at KLEMARK is informed as soon as possible, in order to be able to process the matter in the most efficient manner possible pursuant to the organisation's internal investigation and response procedure.

3.4. What channels are available?

KLEMARK has the following channels available to be able to submit the reports this Policy concerns:

- **Ordinary** channels:

- Direct superior or a member of the company management committee.
- Member of the Compliance Committee.
- By post to the attention of:

  Unidad Técnica de Cumplimiento

  Parque Empresarial Vía Norte

  C/ Quintanavides, 19, Edificio 4- Plta. 2ª

  C.P. 28050 – MADRID

a) Alternative channels (*): the "Alternative Channels" are as follows:

- The telematic ones available through the web and mobile application, as well as the 24-hour/7 days a week telephone channel recorded on the web page of the Ethicpoint application of the external provider Navex Global **https://compromiso.ethicspoint.com**

(*) Use of the alternative channels shall be encouraged, as due to matters of security, confidentiality and integrity of the content of the notification, they are more recommendable than using any other means.

3.5. What information must i provide when reporting?

KLEMARK appreciates the information received being the most complete, detailed and true as possible. And due to this it asks that, in the event of reporting, you share all the information known to the whistle-blower, or available in relation to the possible infringements. The text or message must be clear, being able to provide any proof or document to back the report. This allows KLEMARK to be able to carry out case management in the quickest, most effective way possible.

3.6. Do i have to identify myself when reporting?

It is not necessary. The Ethics Channel at KLEMARK allows reports to be submitted anonymously.

Notwithstanding this, in the event of submitting a report in which your identification, post or relationship and contact data are provided, the personnel in charge of processing may contact the whistle-blower for follow-up if necessary. In that sense, KLEMARK does not allow reprisals to be taken when reports are made in good faith. On the other hand, when a (non-anonymous) report is submitted, KLEMARK makes sure that the internal reporting procedure is carried out confidentially, protecting both the identity of the parties involved as well as the related information provided.

3.7. What happens when reporting through the alternative channels?

KLEMARK uses a *secure management server for Ethics Channel cases*, to support administration of the alternative channels, in line with the terms required by the applicable regulations. Reports through such *alternative channels* are saved directly on the server, which is extremely secure.

The server allows the whistle-blower:

- To specify the place, date, company affected, as well as the persons related to the report.
- To opt for anonymous communication.
- To be able to attach supporting documentation to the report or

notification to justify its content.

To submit the report through the *alternative channels*, the server shall provide the whistle-blower a case number, as well as their exclusive use password. The case number and password allow the whistle-blower to be able to initiate a session on the whistleblowing web site to be able to obtain comments and/or updates on their report. The system will allow the whistle-blower to provide additional information to amend or complement their report.

KLEMARK shall acknowledge receipt within a term of seven days.

Once acknowledgement of receipt has taken place, and in the event of the whistle-blower having identified themself, KLEMARK may contact the whistle-blower directly through a person appointed internally to provide them comments and updates.

Processing the report shall be settled within a reasonable period, not exceeding three months from acknowledgement of receipt, a term that may be extended to six months in cases of special relevance or complexity.

It is important to emphasise that the server only transfers the reports to specific persons within KLEMARK who are authorised to manage them. Likewise, the internal team that handles the documents produced receives training on how to manage the documents and reports effectively, as well as the way to assure their confidentiality.

The principle of action is that, when there are signs of a possible breach of the Compliance System at KLEMARK, an investigation shall be commenced pursuant to an internal procedure established for the purpose.

KLEMARK shall provide the whistle-blower information on the report and, as far as possible, the result of evaluation of the matter. One must bear in mind that, in some cases, for security reasons or the integrity of the investigation, there may be limitations regarding updates on the report that may be provided, according to the progress of its internal procedure.

3.8. What happens when reporting through the ordinary channels?

KLEMARK shall acknowledge receipt within a seven-day term, from the record of effective receipt of the notification.

Once acknowledgement of receipt has taken place, and if the whistle-blower has identified themself, KLEMARK may contact the action whistle-blower directly through an internally appointed person to provide comments and updates.

Processing the report shall be settled within a reasonable term, not exceeding three months from acknowledgement of receipt, a term that may be extended to six months in cases of special relevance or complexity.

The principle of action is that, when there are signs of a possible breach of the Compliance System at KLEMARK, an investigation shall be commenced according to the internal procedure established for that purpose.

KLEMARK shall provide the whistle-blower information on the report and, as far as possible, the result of evaluation of the matter. One must bear in mind that, in some cases, for security reasons or the integrity of the investigation, there may be limitations regarding updates on the report that may be provided, according to the progress of its internal procedure.

3.9. What is the prohibition on reprisals?

KLEMARK does not tolerate any kind of reprisal. This includes threats, or any other means to make the person reporting events this Policy involves in good faith afraid.

Protection against reprisals also includes persons who, in good faith, report possible infringements externally to the competent authorities. The prohibition on reprisal in this Policy covers the following persons:

1. Any third party related to the whistle-blower (such as colleagues and relatives) who may suffer reprisals in the labour context.
2. Any person who has helped the whistle-blower in the reporting process.
3. Any legal entity that the whistle-blower is the owner of, where they may work, or that is in any other way related in a labour or professional context.

The prohibition of reprisals covers any act or omission, direct or indirect, that may harm a whistle-blower due to reporting possible infringements in good faith. For example, KLEMARK shall not take any of the following measures against whistle-blowers due to presenting a report in good faith:

1. Suspension, dismissal, demotion or equivalent measures.
2. A negative performance evaluation.
3. Refusal of promotion.
4. Unjustified changes of place of work, salary reduction, change in working hours.
5. Coercion, threats, harassment or ostracism.
6. Discrimination, disadvantaged or unfair treatment.
7. Not renewing, or early termination of a temporary labour contract.
8. Damage, even to the person's reputation, in particular in the social media, or financial losses, including loss of business or loss of income.
9. Early termination of a goods or service contract.
10. Cancellation of a permit.
11. Among other measures that may be considered reprisals.

In the event of any person at KLEMARK directly or indirectly taking reprisals against this Policy, KLEMARK itself shall take the necessary measures to ensure the reprisals cease as soon as possible and, when appropriate, shall take disciplinary measures against those responsible for these.

3.10. What must we understand as good faith by the company and the person reporting?

From the point of view of the whistle-blower, good faith requires the report to be made with at least reasonable causes to believe the information provided on possible infringements was true at the moment of reporting.

From the point of view of the company, this involves not adopting any reprisal due to the fact of a report being presented, as well as it protecting the confidentiality and personal identity of the whistle-blower in all cases and with the sole exception of the Law, in its different modes, requiring this to be notified to a judicial or administrative authority.

3.11. Is my personal data protected?

Yes, they are protected.

KLEMARK undertakes to maintain strict protection of privacy, security and data conservation, as detailed in our policy created for the purpose and published on our web.

These rules are also applied with regard to all the personal data related to reports made pursuant to this Policy.

3.12. Who are the receivers of my personal data if i submit a report?

The personal data recorded in the context of a report made, including the alternative reporting channels, may be processed or communicated to the following parties when necessary:

- Navex Global, Inc., the independent third party that manages the alternative reporting channels, as processing manager.
- Members of the Compliance Technical Unit, as well as the Compliance Committee at KLEMARK.
- Authorised representatives of KLEMARK who intervene in the investigation, if the nature or scope of the facts reported requires their participation.
- Investigator, advisor or external consultant hired to support KLEMARK in evaluation of the notification, the investigation of the matter, or to advise KLEMARK regarding the matter.
- The police and/or other regulatory bodies, or in application of the Law.

3.13. What is the legal basis for processing my personal data?

Processing personal data within the setting of the communications channel is based on the existence of a public interest under the terms set forth in Article 6.1.e) of the General Data Protection Regulations, to detect and prevent complaints and thus to prevent damage and risks for which KLEMARK is liable, and defined in Article 24 of Organic Act 3/2018, of 5th December on Data protection and guarantee of digital rights, consisting of creating and maintaining an information system for internal reports and investigating possible irregularities or acts contrary to ethics, legality or corporate regulations.

Moreover, KLEMARK must fulfil the legal obligation to settle the queries submitted, applicable by virtue of the terms set forth in Organic Act 10/1995, of 23rd November, of the Criminal Code, so fulfilment of the legal obligations of Article 6.1.c) of the General Data Protection Regulations may also be the legal basis for processing.

Thus, processing the whistle-blower's personal data is strictly necessary to manage the report and to comply with the aforementioned legal aims and obligations. Under no case shall KLEMARK perform automated decisions based on the data submitted.

3.14. What data is collected, how is it kept and for what purpose is it processed?

Purpose for which KLEMARK processes the personal data

At all times, only the strictly necessary personal data shall be processed in order to manage, process and investigate reports on commission of irregularities or acts contrary to ethics, legality or the corporate regulations of KLEMARK and to carry out the necessary actions to investigate the facts reported, including, where appropriate, adoption of the relevant disciplinary or legal measures. The personal data shall not be used for a purpose other than that stated.

Personal data collected by KLEMARK

In processing the reports made pursuant to this Policy, KLEMARK collects the following personal data and information provided when submitting a report and throughout its investigation:

- Name and contact data (unless reported anonymously) and if a KLEMARK employee.
- Name and other personal data of the persons mentioned in the report, if that information is provided (that is, description of the functions and contact data).
- Any data or information included in the report that may identify a specific person.

Conservation of personal data

KLEMARK shall keep a register of all the reports received. These records ad the personal data they contain shall be kept confidentially.

The records shall be kept for all the time necessary to fulfil any applicable legal requisite from time to time.

In particular, KLEMARK shall conserve the personal data of the whistle-blower for the essential time to decide on whether it is appropriate to commence an investigation of the facts or conduct reported and, once this is decided, it shall be deleted from the Ethics Channel, and may be processed outside the system to investigate the events for the necessary time until conclusion thereof. Once the investigation of the notification is completed and, if appropriate, the necessary actions are taken, the data from reports that have been processed shall be kept blocked to comply with the appropriate legal obligations in each case.

In all cases, the personal data shall be deleted from the Ethics Channel within the maximum term of three (3) months from being input, except if conserved for an additional term due to being necessary to fulfil the legal and corporate obligations, and may not continue to be processed outside the Ethics Channel in the case of not having concluded investigation of the report, for the necessary time until its conclusion.

If it is decided not to proceed with a report submitted, the information may be kept in anonymised format.

3.15. What are the rights of the person reporting in data protection matters?

As whistle-blower, the person reporting may exercise access to their personal data attorney time and under the terms set forth in the applicable regulations.

Should that person believe the data is not correct or is incomplete, they may request correction thereof pursuant to the applicable legislation. They may apply for deletion of data that is no longer necessary, except in the event of there being a legal obligation to conserve such.

Moreover, they may request that processing of their personal data be limited, oppose such, or request portability of their data and they shall be entitled to withdraw their consent.

To that end, they must submit a written application to **rgpd-klemark@klemark.com** attaching a copy of their National Identity Card or other document that proves their identity, and clearly stating the right they wish to

exercise.

In the event of not having achieved satisfactory exercise of their rights, they may submit a complaint to the Spanish Data Protection Agency.

4. ENFORCEMENT, TERM NOTIFICATION AND REVIEW

This Policy shall come into force right on the date of approval, amendment or update of this document.

It shall be published and distributed for adequate knowledge, being made available for consultation through the corporate web.

In ordinary circumstances, KLEMARK shall review its content with the frequency established in its documented information system and, under extraordinary noes, when significant circumstances of a legal, organisational nature arise, or any other that may require its immediate adaptation and/or updating.