INTERNAL INFORMATION SYSTEM POLICY

OF FANOX ELECTRONIC, S.L.

INDEX

1.- OBJECTIVE

2.- SCOPE OF APPLICATION

3.- PERSON IN CHARGE OF THE INTERNAL INFORMATION SYSTEM

4.- PROCESSING OF THE INTERNAL INFORMATION SYSTEM

5.- MEASURES FOR THE PROTECTION OF THE INFORMANT

6.- PROTECTION OF PERSONAL DATA

7.- EXTERNAL INFORMATION CHANNEL

- 1 -

OBJECT

This system is implemented under the considerations of Law 2/2023 of 20 February, regulating the protection of persons who report regulatory infringements and the fight against corruption, which transposed into Spanish law the Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019.

According to this regulation, the minimum requirements to be met by the organization of FANOX ELECTRONIC, S.L. are determined in relation to the Internal Information System (hereinafter IIS), in which its internal ethical channel or whistleblowing channel is integrated.

In accordance with the provisions of 5.2 d) of Law 2/2023, the SII integrates all the internal information channels belonging to other sectors that the company should have.

- 2 -

SCOPE OF APPLICATION OF THE SYSTEM

The SII is intended to serve as a means of communication between the company and the informants with respect to infractions related to:

- Facts or conducts that may have criminal transcendence.
- Severe or very serious administrative infractions.
- Infringements of labor law in matters of occupational health and safety (without prejudice to that established in its specific regulations).
- Infringements of European Union Law included in the material scope of application of Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019, on the protection of persons who report infringements of Union Law and the Spanish transposition Law.
- Infringements of the company's Codes of Ethics or Codes of Conduct.

- 3 -

PERSON RESPONSIBLE FOR THE INTERNAL REPORTING SYSTEM AND WHISTLE-BLOWING CHANNEL

Ms. Leire Gómez, a member of the company's Supervisory Body, has been appointed by the Board of Directors as the person responsible for the system.

Two channels are available as preferential means of information:

a) Public Channel, for any informant, through the mail:

canaletico@fanox.com

b) For the members of the organization, through the link:

https://canal.fanox.com/

The management of the information will respect the confidentiality of the informant's identity and other data that deserve such consideration, in accordance with articles 5 and 9 of Law 2/2023, although the reception of information transferred anonymously is admitted.

In the event that it is preferred to transfer information orally by means of a face-to-face meeting or telephone call, this may be done in the person of Ms. Leire Gómez at the offices of FANOX ELECTRONIC, S.L., located at Edificio 604, Parque Tecnológico de Bizkaia, Astondo Bidea, 48160, Derio, or by telephone at 944 711 409, ext. 150. This meeting will take place within a maximum period of 7 days from its request and the informant will be advised that the communication will be documented by recording or transcription in minutes that will be signed by the informant.

Likewise, it is also an accepted means of communication by mail, to the person of Mrs. Leire Gómez at the same address of the company.

- 4 -

PROCESSING OF THE INTERNAL REPORTING SYSTEM

4.1 Content of the report.

The informant has the duty to provide all the information as detailed as possible, as well as to provide all the data and evidence available to him/her in order to facilitate the possible subsequent investigation procedure. Likewise, in order to be able to carry out

such a procedure, the communication is required to have, as a minimum, the following information:

- Description of the facts.

- The evidence on which the informant's suspicion is based.

- If known, the identity of the person/s who has/have carried out the facts, or of those persons who have been able to cover it up.

- If known, the place where the facts occurred.

- Date of when the informant became aware of the facts, or since when the informant has been aware of them.

- How the informant has known the facts (if he/she has witnessed it personally, through third parties, by means of documentary evidence, etc.).

4.2 Principles of action:

(a) Reports shall be treated with absolute confidentiality.

b) The identity of the complainant shall not be given to the person being reported.

c) The identity of the complainant shall only be provided to the competent authority in the cases provided for by law.

d) The system permits the investigation of anonymous complaints.

e) The right to honor and the right to defense of the reported person shall be guaranteed.

f) Communicating or publicly disclosing information knowing it to be false is typified by Law 2/2023 as a very serious offense and may constitute a crime of libel or slander.

g) The whistleblower has the protection rights guaranteed by Law 2/2023, including the right to support measures and protection against retaliation.

4.3 As regards the processing of the information, in accordance with the provisions of Articles 7 and 9 of Law 2/2023, it shall follow the following steps:

a) An acknowledgment of receipt shall be issued to the informant within no more than 7 calendar days.

b) The informant will be informed of his or her rights, including those relating to the protection of personal data.

c) The investigation's resolution shall be carried out within a period not exceeding 3 months, extendable for another three months in cases of extreme complexity.

d) In the event that the information transferred refers to facts constituting a crime, it will be transferred to the competent authority.

- 5 -

MEASURES FOR THE PROTECTION OF THE INFORMANT

One of the purposes pursued by Law 2/2023 is adequate protection against possible retaliation in order to strengthen the culture of information and integrity within organizations as a mechanism to prevent and detect threats to the public interest.

Therefore, Law 2/2023 in Article 36 determines the following:

"Acts constituting retaliation, including threats of retaliation and attempts of retaliation against persons who submit a communication as provided for in this law are expressly prohibited."

In this way, the whistleblower will be protected provided that the communication or information transferred falls within the objective material scope of application of Law 2/2023, set forth in paragraph 2.

In accordance with the provisions of articles 18 and 35 of Law 2/2023, the cases not covered by whistleblower protection are listed:

- The reported facts lack any plausibility or basis.
- The facts do not constitute an infringement of the legal system in accordance with the scope of application of Law 2/2023.
- Interpersonal conflicts.
- Facts that only affect the informant.
- Information is already available to the public.
- Mere rumors.
- Information that does not add anything new or significant to a prior report.
- Information obtained through the commission of a crime. In this case, in addition, the facts constituting a crime must be immediately forwarded to the Public Prosecutor's Office.

- 6 -

PROTECTION OF PERSONAL DATA

The processing of personal data arising from the application of Law 2/2023 shall be governed by the provisions of the RGPD and the Organic Law 3/2018 of 5 December on the Protection of Personal Data and Guarantee of Digital Rights (LOPDPGDD).

The SII must prevent unauthorized access, preserve the identity, and guarantee the confidentiality of the data corresponding to the persons concerned and any third party mentioned in the information provided, especially the identity of the informant, in case he/she has been identified. The identity of the informant may only be communicated to the Judicial Authority, the Public Prosecutor's Office, or the competent administrative authority in the context of a criminal, disciplinary, or sanctioning investigation, and these cases shall be subject to safeguards established in the applicable regulations.

If the information received contains special categories of personal data subject to special protection, it will be immediately deleted unless the processing is necessary for reasons of essential public interest as provided for in Article 9.2. g) of the RGPD, as provided for in Article 30.5 of Law 2/2023.

In any case, personal data whose relevance is not apparent for processing specific information will not be collected or, if collected by accident, will be deleted without undue delay.

Communications that have not been followed up may only be recorded in anonymized form, without the blocking obligation provided for in Article 32 of the LOPDPGDD being applicable.

- 7 -

EXTERNAL INFORMATION CHANNELS AND PUBLIC DISCLOSURES

Law 2/2023 establishes an Independent Authority for the Protection of the Informant, a public body under the Ministry of Justice, to ensure compliance with this standard's requirements.

In addition, this Authority will be provided with an "external channel" to which any informant can address if he/she prefers this means of transferring the information.

Similar channels are also foreseen to be set up at the autonomous community level through the competent authorities or bodies.

Whistleblowers who transfer information through this external channel or make a public disclosure will enjoy the same protection as if they used their organization's private channel.

June 2024