Report2Box by datax

Internal Information System Policy
Autor: DATAX
June 2023

TABLE OF CONTENTS

1. Purpose, scope and guiding principles

1.1. PURPOSE AND OBJECTIVE

The purpose of this Policy is to explain to all users of the company's Internal Information System (hereinafter IIS or Whistleblower Channel) how it works, how they can access it and what its functionalities are. That is, its general operating principles as well as those of the whistleblower's defence.

The Whistleblower Channel is the tool through which all members of the company, i.e. members of the governing body, managers and employees, as well as third parties who have or have had an employment or professional relationship with the company can inform the company of possible risks and breaches of its regulations (both legal and internal) of which they are aware (these will be the reporting parties or communicators).
These third parties, i.e. those who should be allowed to make a report, should be at least the shareholders, participants and members of the management body, including non-executive members, self-employed persons, any person working for or under the supervision of contractors, subcontractors and suppliers; former employees, trainees, candidates in selection processes or in pre-contractual negotiation, volunteers and trainees of the company.

The aim is to create a mechanism, among others, to ensure compliance with the law and the effectiveness of the Code of Ethics and the company's internal protocols, thus preventing them from becoming mere declarations of intent.

Furthermore, the use of this Channel can allow the company to adapt its activity to current regulations, guarantee compliance with its internal regulations and reduce the risk of criminal or illicit conduct within the company, thus also protecting its employees.

1.2. SCOPE AND MANDATORY NATURE

Objective scope of application: What can and cannot be reported through the SII?:
Communications made through the Whistleblowing Channel must refer to actions or omissions that occur within the company's scope of action and that constitute an infringement in an employment or professional context of a rule or principle affecting the company. In any case, they must be reported:

Conduct constituting a crime or a serious or very serious administrative offence such as, for example, a fraud offence, the payment of an undue commission or the non-payment of a tax;
a) any act or omission of the law of the European Union provided that:
    - It concerns matters relating to public procurement; financial services, products and markets and the prevention of money laundering and terrorist financing; product safety and conformity; transport safety; environmental protection; radiation protection and nuclear safety; food and feed safety, animal health and animal welfare; public health; consumer protection; protection of privacy and personal data; and security of networks and information systems.

- Affects the financial interests of the European Union; or
- affects the internal market, e.g. infringements of EU competition rules and State aid granted by States.

b) Any breach of the company's internal regulations, principles and values;
c) Any event that may involve an ethical dilemma;
d) Any event that could compromise the reputation of the company.

Incidents that are not included in this section, such as issues closely linked to human resources or personnel policies (e.g. holidays, remuneration, relations between employees, interpersonal conflicts, etc.), recommendations or suggestions not linked to regulatory compliance issues or to the provision of company services, shall not be considered incidents to be reported.

In case of doubt about the nature of the fact in question on the part of the informant, and provided that the informant acts in good faith, the fact can be reported without any problem. The IIS Officer will review its content and analyse its possible admissibility, which will be reported to the whistleblower.

Concerns

In the event of any concerns that the addressees of this Policy may have regarding regulatory compliance or the use of the Whistleblower Channel (e.g. how to interpret a regulation or how to act in a specific case), they may address them to elena.lozano@creaempleo.es

Subjective scope of application: Who is this Policy addressed to?

This Policy is addressed to the company's shareholders, as well as to all those who, in any way, provide services for the company in an employment or professional capacity, i.e. participants or members of the company's governing, management or supervisory bodies including non-executive members, employees and regular external collaborators (as detailed in art. 1.1), as well as to any person who may act on behalf or for the benefit of the company and third parties without any geographical limitation. The Policy shall also apply to (i) all of them whether they have the status of reporting subject, investigated/complainant or witness and (ii) to the body in charge of receiving and/or processing the complaints that may be received through the Complaints Channel, i.e. the Responsible Person of the SII (hereinafter, the Responsible Person).

Obligatory nature:

Its respect constitutes a labour or contractual obligation of all of them (with the exception of third parties), so that its non-observance could be disciplinarily sanctioned in accordance with the provisions of the regulatory labour regulations where the company carries out its function (e.g. Collective Bargaining Agreement of application), as well as in the corresponding regulations or contractual document.
Any of the addressees of this Policy is obliged to report any incidents of which they become aware through the means contemplated in the following chapter.

1.3. LEGAL REGIME

The organisation, use and operation of the Whistleblowing Channel shall be governed by this Manual. Likewise, any regulations that may be issued by the authorities or administrations in relation to the whistleblowing channels or other regulations that may regulate aspects relating thereto (e.g. laws regulating the protection of personal data or the prevention of money laundering and the financing of terrorism and, significantly, all those that regulate the protection of fundamental rights) shall also be observed.

1.4. GUIDING PRINCIPLES

The adoption of the Whistleblowing Channel responds to the company's desire to establish a commitment to zero tolerance towards the commission of crimes, administrative infractions, non-compliance with regulations and respect for legality and good practices.
In line with the above, the procedure for managing the communications received through the Whistleblowing Channel will always comply with the following principles:

Confidentiality: all information processed through the Whistleblowing Channel shall be considered confidential and shall be treated as such; the confidentiality of the identity of the informant as well as that of any third party mentioned in the communication and also of the actions carried out in its processing shall be guaranteed; only those authorised to do so shall have access to it;
Indemnity and prohibition of retaliation: bona fide users of the Whistleblowing Channel will be protected by the company, by the authorities where appropriate, and will not receive any retaliation for the proper use of the Channel;
Impartiality: the Controller will always observe and treat the information submitted to it objectively and impartially; and
Trust: the company will generate trust in the use of the Channel among all its members in order to make the Channel as efficient as possible.

2. Incident reporting: How can an incident report be made?

2.1. MEANS OF INCIDENT REPORTING

The recipients of this Policy may make the reports mentioned in point 1.2 above through the Whistleblowing Channel that the company has enabled, i.e. through the ReportBox by Datax platform accessible through this link: https://creaempleo.report2box.com/home

If the whistleblower so requests, he/she may also submit his/her report by means of a face-to-face meeting with the person in charge within a maximum period of 7 days from the date of his/her request.

In order to ensure the confidentiality of the channel, only the persons listed here will have access to the reports submitted, and they will be responsible for their management and processing: Ethics Committee, who will immediately receive all the reports that may be sent through the indicated platform. In the event that the report is appropriate, the Ethics Committee will be notified in order to initiate the corresponding investigations. Likewise, the Report2Box by Datax platform will always be protected by a password that must be modified every 3 months and only known by the subjects mentioned here. These tools and any other that may be used for the processing of complaints shall also include the necessary technical and security measures to guarantee the confidentiality of the Whistleblowing Channel.

The above constitute all the internal means of the company through which the complaint may be sent, and these should be the preferred means of use. However, whistleblowers may also address their complaints to an external body: the Independent Whistleblower Protection Authority (IPA) or any other authority competent to receive complaints.

In the event that any person in the company who is not the IMS Officer receives a report by any means, he/she must immediately forward it to the Officer and keep the information received confidential.

2.2. BASIC INFORMATION

The reports communicated through the Whistleblowing Channel must contain the following minimum information:

- The fact, behaviour or irregularity being reported, as well as the date on which it took place. No legal classification or legal assessment of the fact investigated by the informant shall be required, although the informant must have reasonable grounds to believe that the reported fact is true;
- The reason why the occurrence is considered strange or irregular;
- Identity of the persons responsible for the above if known (reports on unknown but identifiable subjects may be admitted);
- Elements of evidence that may be available to prove that the event or irregularity has been committed (the provision of evidence by the reporting party is not compulsory). In no case shall evidence be obtained in violation of fundamental rights or in an unlawful manner. In cases where this doubt may arise, the informant shall refrain from obtaining the evidence without the advice of the person in charge or the third party he/she deems appropriate;
- Identification of the whistleblower, although anonymous communications may also be accepted. In the event that an anonymous report is received through the whistle-blowing channel, the information received will be treated with the necessary precautions required for this type of communication and without this circumstance preventing the application of this Policy. In this scenario, it is important to bear in mind that the Report2box by Datax platform allows constant communication with the anonymous whistleblower through a tracking code provided by the platform. It is important to note that

in the event that the anonymous whistleblower loses the tracking code, it will not be possible to retrieve it and, therefore, to access the follow-up of his or her report.

All of the above is requested on the Report2Box home screen, and only the spaces provided for this purpose must be filled in.

Users can also access the instructions on how to use the Channel through the explanatory video that you will find in this link: https://youtu.be/9BFPmYane34

In any case, the reporting party is obliged to make the report truthfully, without misrepresenting the truth, and without prejudice to the fact that the information transmitted is only due to indications of an infringement of those mentioned in section 1.2.

2.3. INCOMPATIBILITY

In the event that the complaint directly or indirectly affects the Responsible, the Report2Box platform allows to assign it to a second manager in order to designate a substitute who must assume the tasks of managing the complaint in place of the incompatible subject.
When this situation of incompatibility with the Responsible occurs, the fact that the latter does not refrain in their functions, will constitute a very serious breach of this Policy with the consequent labour or contractual penalties that may be imposed.

3. Defence and obligations of the whistleblower

3.1. DEFENSE AND OBLIGATIONS OF THE WHISTLEBLOWER

The company, through the person in charge, will ensure the protection of the whistleblower in good faith and who uses the Whistleblowing Channel in accordance with the provisions of this Policy through the following principles of action:

a) It will guarantee and treat as confidential the identity of the whistleblower, the identity of the persons who may be mentioned in the communication made and the facts that are exposed therein. This means that only those persons authorised to do so, and identified above, may access the information relating to the report and may not share it with any other third party.

b) Guarantee anonymity in those cases where the communication is made in this way. That is, when the whistleblower makes the report anonymously, his or her identity will never be known, which is guaranteed by the Report2Box platform, which is managed by a third party outside the company.
c) Provide an interpreter or translated documentation when required by the reporting person to understand the scope of his/her rights and obligations as well as the use of the Whistleblower Channel.
d) Observe an absolute prohibition against retaliation of any kind, including threats of retaliation and attempted retaliation, for information that may be provided to the investigation by the whistleblower. That is, if the whistleblower in good faith receives any form of retaliation for his or her cooperation with the company, he or she will be immediately sanctioned.

At the same time, the whistleblower should consider the following obligations in the use of the Whistleblower Channel:

a) Act in good faith.
b) Not to communicate facts that are false or manifestly contrary to the truth.
c) Provide as much detail as possible about the facts reported and cooperate with the investigation.
d) To follow up on the complaint submitted in order to be informed of its processing and to be able to respond to any clarifications or requests for information that may be formulated.
e) Respect the confidentiality of the information provided and the very existence of the complaint and its subsequent processing procedure.

Likewise, the company shall ensure the rights of the person reported, such as, for example, their right to honour, to the presumption of innocence, to not suffer prospective investigations and to have access to the facts attributed to them and to be heard about them. All of this will be included in the Procedure for the Management of Information Received, which complements the content of this section.

3.2. MAIN PRINCIPLES OF THE INFORMATION MANAGEMENT PROCEDURE

When the IBS Manager receives a complaint through the Whistleblowing Channel and, without prejudice to what is set out in the Procedure for the Management of Information Received, he/she shall initiate the internal investigation phase of the reported facts, the essential guiding principles of which shall be as follows:

a) It shall study the facts contained in the complaint received and shall first carry out an analysis of their plausibility. That is, it will review whether or not the facts reported should be investigated, deciding whether to admit the complaint or to reject it. This will be notified to the whistleblower;
b) In the event that the complaint passes the above plausibility filter, the person in charge will initiate an internal investigation in which he/she will carry out the investigative measures deemed necessary, such

as, for example, an interview with the complainant (if he/she is not anonymous), with witnesses and with the complainant and/or the analysis of any documentation that may be necessary.

c) During the conduct of any investigation it carries out, it shall at all times respect the rights and guarantees set out in this Policy, in the Procedure for the Management of Information Received and in the legal system, such as, for example, proportionality, impartiality, independence and the rights of defence, presumption of innocence, honour and contradiction of the parties affected by the investigation.

d) Finally, with the facts that have been analysed, he/she shall issue a report of conclusions in which the facts observed are assessed and a conclusion is reached. Where appropriate, the Head may also include in his report a proposal for the adoption of measures to improve the company's processes.

e) Based on the conclusions reached by the Head in his report, the company will analyse whether disciplinary or contractual measures should be adopted or whether legal action should be taken.

4. Communication

4.1. COMMUNICATION

A copy of this Policy will be delivered, by telematic means (e.g. via the intranet) or on paper, to all those to whom it is addressed, so that all of them may be aware of their duties, rights and guarantees in relation to the use of the Whistleblowing Channel. In any case, easy and continuous access to this Policy will be ensured to all its recipients through the company's intranet or welcome pack. In the event that the recipients of this Policy do not speak Spanish, a translation into a language they can understand must be provided. Evidence of the delivery of this Policy to all its users will be kept.

This Policy will also be published on the home page of the company's website, in a separate and easily identifiable section for easy access.

4.2. INTERPRETATION

In case of doubt about the interpretation of this Policy, queries will be sent to the Responsible via the e-mail address indicated above so that they can be resolved.

4.3. TRAINING AND AWARENESS RAISING

Likewise, the company shall provide specific training on the use of the Whistleblower Channel to all its members, which shall be supported by this Policy and which shall, in any case, cover the following points:

- The existence of a Whistleblowing Channel in the company for the purposes described herein;
- How to use the Whistleblowing Channel correctly and what its process is
- Rights and duties of the users of the Whistleblowing Channel;

- The obligation of the addressees of this Policy to inform the company of any of the facts described in section 1.2.

The company will also provide specific training on the management of the Whistleblowing Channel to the persons in charge of receiving and processing complaints, in this case the IMS Manager.

The company shall keep evidence of any training or other training or awareness-raising activities that may have been carried out for all users of the Whistleblowing Channel.

4.4. COMMITMENT OF THE ADDRESSEES OF THE POLICY

All members of the company should be aware of the Policy, actively contribute to its observance and report any breaches of it that they become aware of, as well as any deficiencies they may observe in its content or development. The company's governing body will pay particular attention to these duties.

5. HISTORIC, APPROVAL, ENTRY INTO FORCE AND AMENDMENT OF THE HANDBOOK. EVIDENCE

5.1. HISTORIC, ADOPTION AND ENTRY INTO FORCE

Historic:

The following table reflects the different versions of the Manual that have been produced, as well as their date and subsequent modifications that each version of the document may have undergone:

VERSION	DATE	CHANGES
1.0	*June 2023*	Initial version
2.0		

Approval and entry into force:

This Policy shall be approved by the Ethics Committee. The date of approval shall be recorded in the minutes of the Committee. This date shall be the date from which the document shall enter into force in the company.

5.2. MONITORING, CONTINUOUS ADAPTATION AND REFORM OF THE POLICY

Continuous monitoring and adaptation:

Periodic reviews of the content of the Policy will be established to ensure its continuous adaptation to the reality of the company, changes in legislation or jurisprudence, etc. Likewise, its use will be monitored and the performance of the Whistleblowing Channel system may be measured through the use of indicators. All of this in application of the principle of continuous improvement that governs the company's processes.

Reform:

The Ethics Committee may pre-formulate the Policy on its own initiative and/or at the proposal of any addressee of this Policy.

5.3. SAFEKEEPING OF EVIDENCE

The Manager shall ensure the safekeeping of all evidence that accredits the training, control, supervision and correction activities that have been carried out in the company in accordance with the previous sections. This shall be done in coordination with the corresponding personal data protection regulations for each area of activity of the company.

6. PROTECTION OF PERSONAL DATA

In order to ensure compliance with personal data protection legislation and, in general, to prevent the improper use of information, the company will guarantee, in the management and processing processes of the Whistleblowing Channel that may be initiated and with respect to both the informant and the investigated party or third parties, that:

- Only the person in charge of the Internal Whistleblowing System, the persons in charge of the processing designated and the Data Protection Officer will have access to the personal data obtained under this Policy. They must keep them confidential and may not use them for purposes that are not directly related to the management and instruction functions of the Whistleblowing Channel. Personal data shall not be collected if it is not manifestly relevant to the handling of a specific complaint or, if collected by accident, shall be deleted without undue delay. If the information received contains data falling under special categories of data, it shall be deleted immediately.
- Only in the event that precautionary or disciplinary measures are taken against any recipient of this Policy will the HR Manager or competent body be granted access to the personal data. Likewise, in the case of the adoption of disciplinary measures, access shall be granted to the Head of the legal services of the entity or body.

- The necessary technical and organisational measures shall be taken to preserve the identity and guarantee the confidentiality of the data corresponding to the persons affected by the information provided, especially that of the person who may have brought the facts to the attention of the company, in the event that 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 disciplinary investigation.
- Personal data will only be collected and stored, where appropriate, in the reporting system to the extent and for as long as it is necessary to decide on the appropriateness of initiating an investigation or investigation into the reported facts and to initiate them.

In any case, after three months have elapsed since the data were entered in the Report2Box platform without any investigation having been initiated, they will be deleted from this complaints system. Those communications that have not been followed up may only be recorded in anonymised form (without the obligation to block them).

- All obliged parties must keep a register of information received and internal investigations, the personal data of which will only be kept for as long as is necessary, and in no case may the data be kept for a period of more than ten years.
- The purpose of collecting this data is to be able to investigate, detect and correct possible breaches or misconduct within the company, especially in the areas of criminal law and regulatory compliance.

- Insofar as the personal data obtained from the instruction will be incorporated into the company's information systems for the purpose of managing the Whistleblower Channel, the data subjects may exercise the rights referred to in articles 15-22 of the General Data Protection Regulation (however, in no case will access to the communication be given to the data subjects). To do so, a letter must be sent to *CREA EMPLEO ETT, SL. C/ MARQUESOS DE BARBERA 138, 08210 BARBERA DEL VALLES (Barcelona)* indicating the specific request and enclosing a photocopy of the requesting party's National Identity Document.

- The stipulations of art. 32 of Law 10/2010 of 28 April on the Prevention of Money Laundering and Terrorist Financing will be respected when the exercise of rights affects a complaint related to the prevention of money laundering and terrorist financing.

- Should you wish to contact the company's Data Protection Officer directly with the intention of formulating any complaint, query or doubt, you may contact us in writing, indicating your details, at the following e-mail address: gestion@creaempleo.es; info@creaempleo.es.

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

ANNEX I

Definitions

a) Whistle-blowing Channel: a tool that the company places at the disposal of all its members and third parties to be able to report, securely, confidentially and/or anonymously, facts that may constitute a crime or a serious or very serious administrative offence. Likewise, they may also report facts that may involve the infringement of an internal rule, a fact that may affect the reputation of the company or that may involve an ethical dilemma.

b) Whistleblower, whistleblower or reporter: a person who, whether identified or anonymously, reports any of the above facts to the company. This person may be a member of the company or a third party. It should be borne in mind that Law 2/2023 of 20 February 23 regulating the protection of persons who report regulatory infringements and the fight against corruption will only protect those who have an employment or professional relationship with the company and who report an event constituting a criminal offence or a serious or very serious administrative offence. This is without prejudice to the protection that may be provided for the whistleblower in other bodies of law.

c) Reported person: person who is presumed to be the author and responsible for the reported facts. This person will also enjoy certain rights that will be developed in the Procedure for the Management of Information Received.

d) Head of the Internal Whistleblowing System: a single-person or collegiate body, appointed by the company's governing body, responsible for the management and/or processing of the Whistleblowing Channel and the subsequent internal investigations that may be carried out.

e) Retaliation: any acts or omissions that are prohibited by law, or that, directly or indirectly, involve unfavourable treatment that places the persons who suffer them at a particular disadvantage with respect to another in the employment or professional context, solely because of their status as whistleblowers, or because they have made a public disclosure. Such as, for example, dismissal, lack of internal promotion, job changes, etc.

ANNEX II

Receipt of the Internal Information System Policy

By signing this document, I certify that I have received, read and understood the Internal Information System Policy. At the same time, I undertake to respect and comply with it.

I also understand that in the event that I fail to comply with its contents, this may lead to disciplinary action by the company.

I also hereby agree to be kept up to date on changes to the Policy and to read future revisions to the Policy.

DATE:

NAME:

SIGNATURE: