



General and Supervisory Board

REGULATION ON WHISTLEBLOWING PROCEDURES

Approved on 24 January 2019

This is an unofficial translation of the Regulations on Whistleblowing Procedures prepared for information purposes only. In the case of any discrepancy between this translation and the Portuguese version of the Regulations, the Portuguese version will prevail.



INDEX

1. Framework	3
2. Scope of application	3
3. Rights and guarantees	3
4. Procedures for receiving whistleblowing	4
5. Initial Confirmation	5
6. Investigation	5
7. Conclusion of the process	6
8. Supervision	6
9. Final provisions	7
10. Publication	7
Annex A	8
ANNEX B	9



1. Framework

The General and Supervisory Board (GSB), while EDP's supervisory board, and the Audit Committee (AUDC), as specialized committee of that body to carry out functions that are legally and statutorily assigned duties, promote monitoring permanently and evaluation of internal procedures relating to accounting and auditing matters, as well as the effectiveness of the risk management system assessment, the internal control system and internal audit system, including the receipt and processing of complaints and queries, arising from employees or not. The mechanisms and procedures covered by these regulations for receiving, storing and handling whistleblowing abide by data protection and security of information standards in force¹.

2. Scope of application

2.1. Matters covered – These regulations establish the rules regarding the mechanisms and procedures for receiving, treatment and resolution of whistleblowing received by the company in matters of (i) accounting, (ii) internal accounting control, (iii) auditing, (iv) complaints, denunciation or other irregularities and (v) fighting against corruption, banking and financial crime, which have been notified by shareholders, employees, ROC/SROC of the company or others.

2.2. Matters excluded – Whistleblowing that exceeds the scope of “matters covered” will not be handled, and shall be forwarded to the competent services.

2.3. Voluntary aspect – These regulations are based on voluntary whistleblowing.

3. Rights and guarantees

3.1. Prohibition of retaliation – The Company may not dismiss, threaten, suspend, repress, harass, withhold or suspend salary and/or benefit payments, demote, transfer or take any other kind of disciplinary or retaliatory action related to the terms and conditions of the employment agreement of an employee, agent or representative of the Company because that person has legally blown the whistle or provided information or assistance in the investigation of allegations.

3.2. Abusive use – Pursuant to the general terms of the law, the abusive use and use in bad

¹ Regulation (EU) 2016/679, European Parliament and Council, of 27 April 2016 regarding personal protection of personal data processing and data freedom of flow and Law no. 67/98, 26 October, modified by Law no. 103/2015, 24 August.



faith of the whistleblowing mechanism may render its author liable to disciplinary sanctions and legal proceedings.

4. Procedures for receiving whistleblowing

4.1. Channels of communication – EDP has set up and maintains a whistleblowing reception mechanism through dedicated communication channels addressed to the AUDC. These are identified in Annex A:

- a) Email address,
- b) Fax line,
- c) Postal address.

4.2. Information on whistleblowing channels – Information on whistleblowing channels is provided on EDP's Intranet and Internet sites.

4.3. Whistleblowing requirements – Whistleblowing on “matters covered” must:

- a) Identify the communication as confidential and, in the case of letters and faxes, use a format that guarantees their confidentiality until they are received by the respective addressee.
- b) Identify the whistleblower, who must expressly state if they wish to keep their identity confidential.
- c) Contain a description of the facts that back up the alleged irregularity.

4.4. Record of whistleblowing – The AC will be responsible for keeping a record of all whistleblowing covered by the regulations' scope of application. The record must include:

- a) A number identifying the communication;
- b) Date of reception;
- c) Method of transmission;
- d) Brief description of the nature of the communication;
- e) Measures taken as a result of the communication;
- f) Current status of the process (pending or closed).

4.5. Reports on whistleblowing – The staff authorized by the GSB /AUDC must follow up instances of whistleblowing. Every communication must be given a number, to be included in the whistleblowing database.

4.6. Anonymity –The communication must identify the whistleblower, and anonymous information will only be accepted and handled in exceptional cases.



4.7. Confidentiality – Under the terms of these regulations, whistleblowing is treated as confidential information, in particular by the GSB/AUDC and support staff tasked with the operational management of the mechanisms and procedures for receiving, storing and handling whistleblowing.

4.8. Security measures - Under the terms of the **data protection and security of information standards**, the AUDC must implement appropriate security measures so as to protect the information and data contained in the communications and respective records.

5. Initial Confirmation

5.1. Confirmation process – The AUDC shall conduct an initial confirmation that there are sufficient grounds for an investigation.

5.2. Prior contact with the whistleblower – Whenever the whistleblower's identity is known, she/he may be contacted in advance in order to obtain relevant information for initial confirmation.

5.3. Initial confirmation report – The initial confirmation shall be based on preliminary information and shall be the subject of a report taking into account the following factors:

- a) The nature of the communication, determining whether it falls under “matters covered”;
- b) The irregular nature of the behavior mentioned in the communication;
- c) The feasibility of an investigation, highlighting potential obstacles or limitations;
- d) People who may be involved or be aware of relevant facts, who should be questioned or confronted with the information.

6. Investigation

6.1. Appraisal by the AUDC – Initial confirmation reports on allegations and their accompanying documentation shall be examined by the AUDC, which shall decide on how to proceed, for example:

- a) Keeping on file because the allegation does not fall under “matters covered”, due to lack of sufficient grounds or characteristics for the purposes of these regulations;
- b) Opening of an investigation process.

6.2. Investigation process – The investigation process is conducted and supervised by the AUDC, assisted by the GSB support office and by other company employees, with possible



recourse to hiring external auditors or other experts to help in the investigation under the terms of the internal rules of the GSB.

6.3. Legality of the process – In conducting the investigation, the GSB shall comply with and enforce current laws and the Company's internal rules.

6.4. Right to defense - Those implicated in any investigation shall be advised of their right to hire legal counsel before speaking to any investigator.

6.5. Urgent measures – Without prejudice to the final decision on the investigation process, in situations of obvious urgency and seriousness the AUDC shall take appropriate measures to protect the Company's interests in view of the irregularities detected.

7. Conclusion of the process

As a result of the investigation and the final appraisal and assessment of its results, the AUDC will propose to the GSB:

- a) Filing
- b) Adopting appropriate measures, such as:
 - i. Alterations to the Company's control processes and methods or policies;
 - ii. Corrections or adjustments to documents;
 - iii. Report to the competent regulatory bodies;
 - iv. Cessation of contractual relations;
 - v. Commencement of disciplinary procedure, or removal of a member of a corporate body;
 - vi. Commencement of legal proceedings, criminal prosecution or similar measure.

8. Supervision and Report

Under the scope of this Regulation, the AUDC will provide the GSB with a six-monthly report on its activities in implementing these regulations, with particular regard to:

- a) The number of communications received over the period and a summary of the allegations;
- b) The cases kept on file, a summary of their content and the grounds for the decision to file them;
- c) The cases under investigation and a summary of the allegations on which they are based;



d) The urgent measures taken by the AUDC pursuant to these regulations.

9. Final provisions

9.1. Assessment – Every year the AUDC must assess the application of these regulations and if necessary propose to the GSB the changes it deems to be necessary in order to best achieve their objectives.

9.2. Maintenance of records – The AUDC undertakes to keep the records and related information confidential and secure, in accordance with the principles set forth in the Annex of this Regulation.

10. Publication

This Regulation is published on the corporate website of the Company.



Annex A

Contact information for whistleblowing

Intended Recipient: Audit Committee of EDP – Energias de Portugal, S.A.

Address: Avenida 24 de Julho, 12 – Torre Nascente, 7th floor

1249-300 Lisboa

E-mail: audit@edp.pt

Fax 21 001 2929



ANNEX B

PROCESSING OF PERSONAL DATA

The reported information under this Regulation involves personal data processing, which shall be carried out in accordance with the following terms:

A. Controller: The data controller is EDP, company with registered office at Avenida 24 de Julho, no. 12, 1249-300 Lisbon, with the following email address «audit@edp.pt».

B. Purpose and lawfulness of processing: The personal data collected are processed for the purposes of the internal communication management of irregular practices in matters related to (i) accountancy, (ii) internal accounting controls, (iii) audit, (iv) complaints, claims of other irregularities and (v) fight against corruption, banking and financial crime. Processing is necessary for compliance with a legal obligation.

C. Recipients: The personal data processing may be carried out by a reliable service provider, contracted by EDP. The referred service provider shall process data exclusively for the purposes set forth by EDP and in accordance with the respective instructions, strictly complying with the legal provisions regarding personal data, confidentiality, information security and any other applicable provisions.

EDP may disclose data to other entities, which qualify themselves as controllers, processing the data for their own purposes, provided that the lawfulness conditions foreseen in the General Data Protection Regulation (GDPR) are met, such as public entities in particular Tax Authorities, Judicial Courts and competent regulatory authorities.

D. International transfers of data: In case the personal data processing implies its disclosure to third parties established outside the European Economic Area (EEA), EDP shall guarantee that these entities have implemented adequate guarantees for the processing of personal data, taking into consideration the risk exposure to the Data Subject.

E. Retention period: The personal data subject to report shall be immediately destroyed in case they found to be inexact or useless; when a disciplinary or a judicial proceeding is not taking place, the data are subject to verification are destroyed within 6 (six) months as from the closing of investigations; in case of disciplinary or judicial proceeding, the data should be



maintain until the conclusion of such proceeding.

F. Exercise of Data Subject Rights

1. Plaintiff: The data subject may, at any time and regarding his or hers own data, exercise the rights of access, rectification, erasure of personal data, restriction of processing concerning the data subject or objection to processing. For such purposes, data subject is required to send a written request through the referred contacts set forth in Item A of this Annex.
2. Complained: the data subject may, at any time, exercise the rights of rectification, erasure of personal data, restriction of processing concerning the data subject or objection to processing. For such purposes, data subject is required to send to send a written request through the referred contacts set forth in Item A of this Annex.

Under the terms of the General Data Protection Regulation, it is hereby clarified the content of the Data Subject Rights:

Right to Access:

Under the law, the data subject has the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information:

- I. the purposes of the processing;
- II. the categories of personal data concerned;
- III. the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;
- IV. the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;
- V. the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;
- VI. where the personal data are not collected from the data subject, any available information as to their source;
- VII. the existence of automated decision-making, including profiling, and, at least in those cases, meaningful information about the logic involved, as well as the significance and



the envisaged consequences of such processing for the data subject.

Right to rectification

The data subject has the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her.

Right to erasure

Under the applicable law, the data subject has the right to obtain from the controller the erasure of personal data concerning him or her on the following situations:

- I. the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
- II. the data subject withdraws consent on which the processing is based and where there is no other legal ground for the processing of data for direct marketing purposes (sending unsolicited communications);
- III. the personal data have been unlawfully processed;
- IV. the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject;
- V. the personal data have been collected in relation to the offer of information society services.

The right to erasure is not applicable when the processing is necessary for the following purposes:

- I. for exercising the right of freedom of expression and information;
- II. for compliance with a legal obligation which requires processing and which is applicable to EDP;
- III. for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in so far as the right to erasure is likely to render impossible or seriously impair the achievement of the objectives of that processing; or
- IV. for the establishment, exercise or defence of legal claims.

Right to restriction of processing



The data subject has the right to obtain from the controller restriction of processing where one of the following applies:

- I. the accuracy of the personal data is contested by the data subject, for a period enabling EDP to verify the accuracy of the personal data;
- II. the processing is unlawful, and the data subject opposes the erasure of the personal data and requests the restriction of their use instead;
- III. If EDP no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims;
- IV. the data subject has objected to processing pending the verification whether the legitimate grounds of EDP override those of the data subject.

Right to object

Pursuant to the applicable law, the data subject has the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her which is based on, including profiling based on the following situations:

- I. The controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims;
- II. Where the data subject objects to processing for direct marketing purposes, the personal data shall no longer be processed for such purposes.
- III. May also object at any time and with cause, the processing of the respective data for direct marketing purposes including to define profiles that are related with such marketing, without compromising the processing lawfulness based on the prior consent given.

Within the scope of this process, should the data subject consider that EDP has breached or may breach his/her rights pursuant to the data protection applicable legislation, the data subject is entitled to lodge a complaint before the National Data Protection Commission.

For any query related to this information, the data subject may also contact the EDP's Data Protection Officer (DPO) which contact details are the following:

- Email address: dpo.pt@edp.com