

## **Internal Procedure for Whistleblowing and Follow-up Action at ACTION S.A.**

### **1. Aims and objectives of the Procedure**

1. The internal procedure for reporting violation of the law and taking follow-up action at ACTION S.A. was introduced pursuant to the Law of 14 June 2024 on the Protection of Whistleblowers, implementing Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of whistleblowers under the EU law with a view to limiting damage to the public interest, taking follow-up action and ensuring balanced and effective protection of whistleblowers.
2. The objective indicated in point 1. above and the promotion of the whistleblowing attitude is pursued by the Employer on the basis of the Act of 14 June 2024 on the protection of whistleblowers and the provisions of the Internal procedure for reporting violation of the law and taking follow-up action at ACTION S.A.

### **2. Basic Terms Used in the Procedure**

Whenever the Internal Procedure for Whistleblowing and Follow-up at ACTION S.A. refers to:

- 1) **Secure communication channel** – refers to the mode of written reporting of Violation using electronic forms, including the anonymous reporting, in accordance with paragraph 4, points 10 - 14 of the Procedure.
- 2) **Identity Data** – refers to personal info relating to the identity of the Whistleblower, the Person to whom the report relates and the third party named in the report.
- 3) **Follow-up action** – refers to an action taken by the Employer in order to assess the accuracy of the information contained in an Internal Report and to counteract the Violation of the law which is the subject of the report, in particular by means of an investigation, initiation of control or administrative proceedings, filing of charges, action taken to recover funds or closure of a procedure carried out under the Procedure.
- 4) **Retaliatory Action** – refers to a direct or indirect action or omission in a Work-related Context that is caused by a Submission or Public Disclosure and that violates or is likely to violate the rights of the Whistleblower or causes or is likely to cause unwarranted harm to them, including the unwarranted initiation of proceedings against the Whistleblower, the specific instances of which are indicated in paragraph 8, points 1 - 4 of the Procedure.
- 5) **Violation Report** – refers to the information, including reasonable suspicion, concerning an actual or potential Violation that has occurred or is likely to occur at the Company (as an entity where the Whistleblower has participated in the recruitment process or other pre-contract negotiations, works or has worked) or at another Legal Entity where the Whistleblower maintains or has maintained contact in a work-related context, or concerning an attempt to conceal a Violation.
- 6) **Feedback** – refers to the information given to the Whistleblower on the follow-up actions planned or taken and the reasons for such actions.
- 7) **Work-related Context** – refers to the past, present or future work-related activities based on an employment or other legal relationship underpinning the provision of work or services, or the performance of functions in or for a Legal Entity, or the performance of service in a Legal Entity, in the course of which a Violation Report is obtained and the possibility of experiencing Retaliation exists.
- 8) **Violation** – refers to a Violation of the law, consisting of an unlawful act or omission or intended to circumvent the law, concerning: a) the provisions of generally applicable law, including in particular: 1) corruption; 2) public procurement; 3) financial services, products and markets; 4) anti-money laundering and anti-terrorist financing; 5) product safety and compliance; 6) transport safety; 7) environmental protection; 8) radiological protection and nuclear safety; 9) food and feed safety; 10) animal health and welfare; 11) public health; 12) consumer protection; 13) protection of privacy and personal data; 14) security of ICT networks and systems; 15) financial interests of the State Treasury of the Republic of Poland, a local government unit and the European Union; 16) internal market of the European Union, including competition and state aid rules and taxation of legal persons; 17) constitutional freedoms and rights of a human being and a citizen – occurring in the relations of an individual with public authorities and

not related to the areas indicated in points 1-16; b) provisions of all internal acts in force at the Employer, which were established by the Company on the basis of universally applicable law.

- 9) **Public authority** – it should be understood as the chief and central government administration bodies, field government administration bodies, bodies of local government units, other state bodies and other entities performing public administration tasks by virtue of the law, competent to take follow-up actions in the areas constituting the subject of the Violation.
- 10) **Person affected** – refers to an individual, a legal person or an organisational unit without legal personality, to which the Act confers legal capacity, identified in the Report or Public Disclosure as the person who committed the Violation, or as a person with whom the person who committed the Violation is associated.
- 11) **Reporting Helper** – refers to an individual who assists a Whistleblower with Reporting or Public Disclosure in a Work Related Context and whose assistance should not be disclosed;
- 12) **Person related to the Whistleblower** – it should be understood to mean a natural person who may experience Retaliatory Actions, including a co-worker or a person close to the Whistleblower within the meaning of Article 115 § 11 of the Act of 6 June 1997. - Polish Penal Code (Journal of Laws of 2024, item 17).
- 13) **Legal Entity** – is to be understood as a Private Entity or Public Entity;
- 14) **Private entity** – refers to a natural person engaged in economic activity, a legal person or an organisational unit without legal personality which is endowed with legal capacity by law, or an employer, where they are not public entities.
- 15) **Public entity** – refers to the entity indicated in Article 3 of the Act of 11 August 2021 on open data and reuse of public sector information (Journal of Laws of 2023, item 1524).
- 16) **Legal proceedings** – refers to proceedings under generally applicable law, in particular criminal proceedings, civil proceedings, administrative proceedings, disciplinary proceedings or proceedings for violation of public finance discipline, or proceedings under internal regulations issued in order to implement generally applicable law, in particular anti-mobbing proceedings.
- 17) **Procedure** – refers to this Internal procedure for reporting and following up on legal violation at ACTION S.A.
- 18) **Register** – refers to the register of Internal Reports, the rules and scope of which are set out in paragraph 9 of the Procedure.
- 19) **Company** – refers to ACTION S.A.
- 20) **Whistleblower** – refers to an individual who reports or publicly discloses Violation Report obtained in a Work-related Context, including: 1) an employee; 2) a temporary employee; 3) a person performing work on a basis other than employment relationship, including on the basis of a civil law contract; 4) an entrepreneur; 5) a proxy; 6) a shareholder or partner; 7) a member of a body of a legal person or organisational unit without legal personality; 8) a person performing work under supervision and management of a contractor, subcontractor or supplier; 9) an intern; 10) a volunteer; 11) an apprentice; 12) an officer within the meaning of Art. 1 section 1 of the Act of 18 February 1994 on pension provision for officers of the Police, the Internal Security Agency, the Intelligence Agency, the Military Counterintelligence Service, the Military Intelligence Service, the Central Anti-Corruption Bureau, the Border Guard, the Marshal Guard, the State Protection Service, the State Fire Service, the Customs-Security Service and the Penitentiary Service and their families (Journal of Laws of 2023, item 1280, 1429 and 1834); 13) soldier within the meaning of Article 2(39) of the Act of 11 March 2022 on Defence of the Fatherland (Journal of Laws 2024, items 248 and 834). The Act shall also apply to an individual referred to in this paragraph 17(1)-13) of the Procedure in the case of a Report or Public Disclosure of Violation Report obtained in a Work-Related Context prior to the establishment of an employment or other legal relationship forming the basis for the provision of work or services, or the performance of functions in or for a Legal Entity, or the performance of service in a Legal Entity, or already after their termination.
- 21) **Public Disclosure** – refers to the making of the Violation Report to the public.
- 22) **Act** – refers to the Act of 14 June 2024 on the protection of whistleblowers.
- 23) **Internal Report/Violation Information Report** - refers to the communication of an Information of Violation to the Employer.
- 24) **External Report** - is understood to mean the communication of a Violation Report to the Public

Ombudsman or a Public Authority.

25) **Report** - refers to either Internal Report or External Report.

### 3. Legal basis and the scope of the Procedure

4. The procedure has been established on the basis of the provisions of the Act and sets out the internal procedure for reporting Violation and taking follow-up action, including the conditions for whistleblowing, also anonymously, to the internal organisational unit authorised to receive Violation Reports and, in specific cases, to the Supervisory Board, by means of verbal and written internal Notifications, including through a specific, independent and separate channel created to ensure the protection of the Whistleblowers.
5. The Procedure applies to Internal Reports of Violation in accordance with the Procedure and the Act. Where a particular piece of common law or internal Company legislation provides for a stand-alone whistleblowing procedure, the Procedure does not exclude its application.
6. The procedure and provisions of the Act are without prejudice to the provisions of the normative acts established by the institutions of the European Union, as listed in Part II of the Attachment to Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of whistleblowers of Union law ( (OJ EU L 305, 26.11.2019, p. 17, as amended) and the provisions implementing or executing these acts. To the extent not covered by these provisions, the provisions of the Act and the Procedure shall apply to the reporting of Violation information.

### 7. Entities authorised by the Employer to receive Internal Reports, take follow-up action, rules for submitting Internal Reports and establishing a secure communication channel for Internal Reports

1. The internal organisational unit for receiving Internal Reports and taking follow-up action, in particular verifying Internal Reports and carrying out further communication with the Whistleblower, including requesting additional information and providing feedback to the Whistleblower, authorised by the Employer is the **Company's Legal Department** and, in the cases indicated in point 5 below, the **Company's Supervisory Board**.
2. Only persons authorised in writing by the Employer may be allowed to receive and verify Internal Reports, undertake Follow-up Actions and process the personal data of the Whistleblowers, the Persons concerned and third parties indicated in the report. The Authorised Persons are obliged to maintain secrecy with regard to the information and personal data, in particular Identity Data, which they have obtained in the course of accepting and verifying Internal Reports and taking follow-up action. The obligation of secrecy continues even after the termination of the employment relationship or other legal relationship under which the persons performed the work or provided the services.
3. The Employer authorises the following to receive Internal Reports, to undertake Follow-up Actions, in particular to verify Internal Reports, to carry out further communication with the Whistleblower, including requesting additional information and providing feedback to the Whistleblower, and to process the personal data of the Whistleblower, the Persons to whom the submission relates and third parties indicated in the submission: a) the Management Board's Legal Officer; b) the Employees of the Legal Department who have been granted authorisations; c) the Chairman of the Company's Supervisory Board in the cases indicated in point 5 below.
4. The Whistleblower is entitled to submit Internal Reports with Information on Violation directly to the Legal Department.
5. In the event that the Internal Report would concern the Management Board's Legal Officer or the Legal Department's Employees, directly to the Chairman of the Company's Supervisory Board.
6. Violation Reports may be made disclosing the identity of the Whistleblower or anonymously, at the discretion of the Whistleblower. In order to enable the Company to handle the Internal Report and to take follow-up Action, the Whistleblower shall provide in the Internal Report a correspondence address or an e-mail address, hereinafter referred to as the "contact address". If a contact address is not provided, it will not be possible to confirm to the Whistleblower the acceptance of the Report and to provide feedback to the Whistleblower. Where the identity of the Whistleblower is provided, it shall remain available to those

authorised in accordance with point 3 above. The personal data of the Whistleblower allowing his/her identity to be determined shall not be disclosed, except with his/her express consent. The specific conditions for the processing of personal data and the cases of permissible disclosure of such data are set out in paragraph 5 of the Procedure - "Procedure for handling personal data".

7. Methods of communicating Violation Reports:
  - 1) orally:
    - a) by telephone to the telephone number 22 332 22 22 dedicated to the Whistleblowers Reports,
    - b) at the request of the Whistleblower during a face-to-face meeting organised within 14 days of receipt of the request.
  - 2) in writing:
    - a) by e-mail – sent to the address of the Legal Department (address: [dp@action.pl](mailto:dp@action.pl)), or the Supervisory Board (address: [rn@action.pl](mailto:rn@action.pl)),
    - b) by post to the Company's address, indicating either the Legal Department or the Chairman of the Supervisory Board as addressees, and with the note "Confidential. Please do not open the envelope before handing it to the addressee",
    - c) using the Secure communication channel,
    - d) by any other means deemed appropriate by the Whistleblower.
8. A verbal telephone call is accepted via a recorded telephone line and is documented, with the consent of the Whistleblower, in the form of a searchable recording of the call.
9. If the Whistleblower makes an oral submission during a face-to-face meeting, with the Whistleblower's consent, the submission is documented in the form of: 1) a searchable recording of the conversation, or 2) minutes of the meeting, reproducing the exact course of the meeting, prepared by the Legal Officer of the Management Board or the Chairman of the Supervisory Board of the Company in the cases indicated in point 5 above. The Whistleblower may review, correct and approve the meeting minutes by signing them.
10. The Secure communication channel is made available via an electronic form at the following web address: <https://www.action.pl/pl/zgloszenia-naruszen>
11. The Violation Report form contains 3 fields:
  - 1) content of the Violation Report;
  - 2) check box marked with the letter 'N';
  - 3) check box marked with the letters 'NDP'.
12. The checkbox marked "N" indicates that the Violation relates to the conduct of persons other than Members of the Company's Legal Department and its selection by the Whistleblower will result in a Violation Report in the form of a password-protected pdf file being sent to the email address [dp@action.pl](mailto:dp@action.pl).
13. The checkbox marked with the letters "NDP" indicates that the Violation relates to the conduct of Members of the Company's Legal Department and its selection by the Whistleblower will result in a Violation Report in the form of a password-protected pdf file being sent to the email address [rn@action.pl](mailto:rn@action.pl).
14. Access to e-mail at:
  - a) [dp@action.pl](mailto:dp@action.pl) have authorised members of the Company's Legal Department;
  - b) [rn@action.pl](mailto:rn@action.pl) has the Company's Chairperson of the Supervisory Board.
15. Persons authorised in accordance with paragraph 4(3) of the Procedure shall be able to access reports of Violation Reports sent via the Secure Communication Channel.
16. The internal Report should contain a description of the Violation with information to enable its verification, including the following data considered useful for this purpose:
  - a) the date (period) of its occurrence;
  - b) course of conduct classified as Violation,
  - c) the people who have committed Violations;
  - d) possible witnesses to the Violation;
  - e) any other information or evidence available concerning the Violation.

17. The Whistleblower is not obliged to provide the data indicated above in the Internal Report, including the presentation of evidence of the Violation.
18. In the case of anonymous reports of a Violation Report, these are subject to acceptance and verification including follow-up action, whereby feedback from the Employer to the Whistleblower will be possible if the Whistleblower provides a means of contact address.

## 8. Handling of personal data

1. The personal data of the Whistleblower allowing his/her identity to be determined shall not be disclosed, except with his/her express consent. This principle does not apply if disclosure of the Whistleblower's personal data is a necessary and proportionate legal obligation in connection with investigations carried out by public authorities or pre-trial or judicial proceedings carried out by the courts, including in order to guarantee the reported person's right of defence. However, prior to the disclosure of the Whistleblower's personal data, the competent Public Authority or the competent court shall notify the Whistleblower by sending, in paper or electronic form, an explanation of the reasons for the disclosure of their personal data, unless such report would jeopardise an investigation or pre-trial or judicial proceedings.
2. The employer is the controller of the personal data contained in the Internal Report. The Company, upon receipt of a Report, shall process personal data to the extent necessary to accept an Internal Report or to undertake a Follow-up Action ensuring that the data are adequate, appropriate for these purposes ("data minimisation"). Personal data that are not relevant for the processing of the report are not collected and, if accidentally collected, are deleted immediately. The deletion of this personal data shall take place within 14 days of the determination that it is not relevant to the case.
3. Personal data, including in particular Identity Data, is subject to legal protection in accordance with data protection legislation at all stages of the reporting. The Employer undertakes to exercise due diligence to maintain the utmost confidentiality if the identity of the aforementioned persons is disclosed. The protection of confidentiality applies to information from which the identity of such persons can be directly or indirectly identified.
4. The personal data contained in the Internal Report shall be processed in accordance with the applicable legislation, whereby the Company, as the controller of personal data, when providing the data subject with the information required by law, shall not indicate the source of the personal data and whether it comes from publicly available sources, unless the Whistleblower had no reasonable grounds to believe that the information which is the subject of the Internal Report is true at the time of filing it and that it constitutes Information on a Violation or if the Whistleblower has expressly consented to the disclosure of his or her identity or to such communication.
5. The Employer shall apply technical and organisational solutions to ensure that personal data relating to the identity of the Whistleblower, the Person to whom the report relates and the third party identified in the report are stored separately from the document or other information medium covering the report of the Violation, including, where appropriate, the deletion of all Identity Data from the content of the document or other information medium immediately upon receipt, in particular:
  - a) in the case of reports of a Violation Report made orally, the person making the record of the conversation or meeting shall make it without indicating Identity Data therein. The Identity Data necessary to identify the persons to whom it relates are included in the Register.
  - b) in the case of Violation Reports made in writing:
    - i. by email – the person accepting the Report anonymises the content of the Internal Report by performing the action of copying the content of said Report into a new email and then replacing the Identity Data with "\*\*\*\*" and adding an annotation that reads: *"Report anonymised – personal data of the Whistleblower, the Subject of the report and the third party indicated in the report replaced with \*\*\*\*"*. Once anonymised, the content of the Report is sent to [dp@action.pl](mailto:dp@action.pl) or [m@action.pl](mailto:m@action.pl) (depending on who is undertaking the Follow-up actions). At the same time, the Identity Data necessary to identify the persons to whom it relates are included in the Register. Following the steps described in this section, the

message with the original Report is permanently deleted.

- ii. by correspondence to the Company's address – correspondence meeting the requirements set forth in section 4 item 7. 2) b) above shall be forwarded to the addressee without prior opening of the envelope. This person then anonymises the Identity Data by permanently covering the data (e.g. by circling the data with a black marker and, if necessary, making additional copies on the copier of the Violation Report to prevent the text from "peeking out" from under the anonymised section). At the same time, the Identity Data necessary to identify the persons to whom it relates are included in the Register.
  - iii. using the Secure Communication Channel - the person receiving such a report shall anonymise the content of the Violation Report by editing the pdf file received by replacing the Identity Data with "\*\*\*\*" and adding an annotation that reads: *"Report anonymised – personal data of the Whistleblower, the Subject of the report and the third party indicated in the report replaced with \*\*\*\*"*. At the same time, the Identity Data necessary to identify the persons to whom it relates are included in the Register.
6. Persons authorised to receive Internal Reports and to take follow-up action shall include the personal data contained in the Internal Reports and necessary for the identification of the persons concerned in the Registry, otherwise they shall not be collected.
  7. The personal data processed in connection with the acceptance of an Internal Report or the undertaking of a Follow-up Action and the documents relating to that Report shall be retained by the Controller for a period of 3 years after the end of the calendar year in which the External Report has been transmitted to the public authority competent to undertake the Follow-up Action or the Follow-up Action has been completed, or after the proceedings initiated by those actions have been concluded. After the expiry of the retention period indicated in the preceding sentence, the Controller shall delete the personal data and destroy the documents relating to the Report. Act of 14 July 1983 on the national archival resource and archives (Journal of Laws of 2020, item 164) shall not apply.

## 9. Recognition of whistleblower reports, acknowledgement of their receipt, follow-up measures and provision of feedback

1. Upon receipt of a Whistleblower Report, the entities authorised by the Employer to receive reports shall promptly carry out actions to establish the circumstances of actual or potential Whistleblowers, cover the Whistleblower, remedy the effects of the Whistleblower, and prevent the occurrence of future Whistleblowers.
2. Entities authorised by the Employer to receive Internal Reports are obliged to confirm to the Whistleblower the acceptance of the Internal Report within 7 days of its receipt, unless the Whistleblower has not provided a contact address to which the confirmation should be forwarded.
3. Entities authorised by the Employer to receive Internal Reports shall verify the Violation Report in a duly diligent and impartial manner.
4. Entities authorised by the Employer to receive Internal Reports are obliged to undertake follow-up, in particular, to carry out further communication with the Whistleblower, including requesting additional information and providing feedback to said Whistleblower. The whistleblower is not obliged to complete the Internal Report or to provide any further information. However, the cooperation of the Whistleblower with the authorised persons in receiving and verifying Internal Reports and taking Follow-up Actions may contribute to the detection and rectification of the Violation.
5. The investigation shall be undertaken as soon as possible after receipt of the Violation Report and shall aim to establish:
  - 1) the factual circumstances of the claimed Violation and its nature (actual or potential),
  - 2) consequences of the Violation, including its impact on the Company's operations and reputation, and how to remedy and prevent future Violations,
  - 3) the existence of grounds for notifying the competent authorities of the Violation.
6. The person carrying out the Follow-up actions, including the Investigation within the scope of the Violation Report, has the right to:

- 1) request Members of the Company's Bodies and persons employed by the Employer to provide explanations or documents within the scope of the Violation Report;
  - 2) make photocopies, copies, extracts, compilations or printouts of any documents, information and data and other materials related to the Employer's operations.
7. The investigators and persons participating in the investigations are obliged to keep confidential the facts which they have learned or about which they have given explanations or documents in the course of the investigations.
8. The investigation should be concluded within 21 days of its commencement by issuing a report containing the results of the investigation and the elements indicated in points 5(1) to (3) above.
9. The person carrying out the Follow-up action is obliged to provide the Whistleblower with Feedback within a maximum deadline of 3 months from the acknowledgement of the Internal Report or, if the acknowledgement of the Internal Report has not been made, 3 months from the expiry of 7 days from the date of the Internal Report, unless the Whistleblower has not provided a contact address to which the Feedback should be provided. Feedback shall include, in particular, information on whether or not the Violation has taken place and on the measures, if any, which have been or will be applied in response to the identified Violation.
10. Entities authorised by the Employer to receive Violation Reports, undertake:
- 1) The decision as to how to proceed with the Violation in accordance with the applicable regulations and internal acts of the Employer and, in the event that the Violation is subject to recognition by external bodies, in particular Public Authorities, it shall give the relevant notice to such bodies;
  - 2) actions to indicate ways to remedy the effects of the Violation and to prevent future Violations from occurring.

## **10. Procedure for making External Reports to the Public Ombudsman, Public Bodies and, where appropriate, to European Union institutions, bodies, offices or agencies**

1. A Whistleblower may make an External Report without first making an Internal Report.
2. An External Report is accepted by either the Public Ombudsman or the Public Body.
3. The Public Ombudsman and Public Bodies accept External Reports in accordance with the established procedures for the acceptance of External Reports, which also set out how to deal with anonymous reports.
4. External Report may be made orally or in writing. External Report in a documented way may be made: 1) in paper form - to the correspondence address indicated by the Public Ombudsman or the Public Body receiving the Report; 2) in electronic form - to the electronic mail address or electronic delivery address indicated by the Public Ombudsman or the Public Body receiving the Report, or via a dedicated web form or application indicated by the Public Body as the appropriate application for electronic reporting.
5. If an external Report concerns a Violation Report, the Public Ombudsman shall transmit this Report to the Public Authority with jurisdiction for follow-up as soon as possible and no later than 14 days after the Report.
6. The Public Ombudsman or the public authority shall without undue delay forward the information contained in an external notification to the competent institutions, bodies, offices or agencies of the European Union for the purpose of carrying out follow-up action as provided for by such institutions, bodies, offices or agencies.
7. Either the Public Ombudsman or the Public Authority on their respective websites on the Public Information Bulletin posting in a separate, easily identifiable and accessible section and in a way that is comprehensible to the Whistleblower, inter alia, information on the detailed rules for making External Reports.

## **11. Measures for the protection of Whistleblowers and the means used by the Employer to verify their performance**

1. No retaliatory action or attempt or threat of such action may be taken against the Whistleblower. The Whistleblower shall be subject to the protections set out in the Act and the Procedure from the time that the Report or Public Disclosure is made that the information that is the subject of the Report or Public Disclosure is true at the time that the Report or Public Disclosure is made and that it constitutes a Violation Report.
2. Retaliatory Actions against a Whistleblower who has been, is or is about to be employed on the basis of an employment relationship are considered to be, in particular, the use or attempted or threatened use of actions consisting of: 1) refusal to establish an employment relationship; 2) termination or termination without notice of an employment relationship; 3) failure to conclude a fixed-term employment contract or an indefinite-term employment contract after termination of a probationary employment contract, failure to conclude another fixed-term employment contract or failure to conclude an indefinite-term employment contract after termination of a fixed-term employment contract - if the Whistleblower had a justified expectation that such a contract would be concluded with him/her; 4) reduction in the amount of remuneration for work; 5) withholding of promotion or omission from promotion; 6) omission from the award of work-related benefits other than remuneration or reduction in the amount of such benefits; 7) transfer to a lower position; 8) suspension in the performance of labour or official duties; 9) transfer of the Whistleblower's current duties to another employee; 10) unfavourable change of the place of work or work time schedule; 11) negative evaluation of work performance or negative opinion of work; 12) imposition or application of a disciplinary measure, including a financial penalty, or a measure of a similar nature; 13) coercion, intimidation or exclusion; 14) mobbing; 15) discrimination; 16) unfavourable or unjust treatment; 17) withholding of participation or omission from typing for participation in training to improve professional qualifications; 18) unjustified referral to medical examinations, including psychiatric examinations, unless separate regulations provide for the possibility of referring an employee to such examinations; 19) action aimed at making it difficult to find future employment in a given sector or industry on the basis of an informal or formal sectoral or industry agreement; 20) causing financial loss, including economic loss, or loss of income; 21) causing other intangible damage, including Violation of personal rights, in particular the



Whistleblower's good name.

3. The Employer shall bear the burden of proof that the action taken, as referred to in point 2 above, is not a Retaliatory Action.
4. The provisions of points 2. and 3. above shall also apply, mutatis mutandis, to a Whistleblower who has provided, is providing or is to provide work or services on the basis of a legal relationship other than an employment relationship which constitutes the basis for the provision of work or services or the performance of a function, provided that the nature of the work or services provided or the performance of a function does not preclude the application of such action to the Whistleblower. In addition, with respect to this group of Whistleblowers, the making of a Report or Public Disclosure may not give rise to the application, or attempted or threatened application, of Retaliatory Actions, including, in particular: 1) the termination of a contract to which the Whistleblower is a party, in particular concerning the sale or supply of goods or the provision of services, the withdrawal from such a contract or its termination without notice; 2) the imposition of an obligation or the refusal to grant, limit or withdraw an entitlement, in particular a concession, permit or allowance.
5. A Whistleblower against whom retaliatory action has been committed is entitled to compensation in an amount not lower than the average monthly salary in the national economy or to damages. Retaliation, preventing or materially obstructing a Report, disclosing Identity Data is subject to criminal liability.
6. The making of a Report or Public Disclosure may not give rise to liability on the part of the Whistleblower subject to the limitations set out in the Act and provided that the Whistleblower had reasonable grounds to believe that the Report or Public Disclosure was necessary to disclose the Violation in accordance with the Act. In the event that Legal Proceedings have been instituted in respect of such liability, the Whistleblower may request that such proceedings be discontinued.
7. The rights granted to the Whistleblower cannot be waived. Nor can you accept liability for any damage caused by making a Report or Public Disclosure. This does not apply in the case of a deliberate Report or Public Disclosure of false information.
8. If the Whistleblower makes a deliberate Report or Public Disclosure of false information, the person who has suffered damage as a result is entitled to compensation or damages for violation of personal rights from the Whistleblower. In addition, making a Report or a Public Disclosure despite knowing that a Violation has not occurred is subject to criminal liability.
9. The provisions set out in the Act and the Procedure concerning the prohibition of Retaliation and the measures of protection against it shall apply mutatis mutandis to a Person assisting in making a report, a Person associated with the Whistleblower, a legal person or other organisational entity assisting the Whistleblower or associated with the Whistleblower, in particular owned or employed by the Whistleblower, as well as in the event that the Violation Report has been reported to the relevant institutions, body or organisational unit of the European Union in accordance with the procedure appropriate for making such reports.
10. The Company provides direct access to the entities authorised by the Employer to receive Internal Reports, including those on an anonymous basis.
11. The Whistleblower is also entitled to notify the Legal Department or the Supervisory Board directly of the retaliation or the fear of retaliation, including by using the Secure Communication Channel or by any other means provided for making Internal Reports.
12. The investigator for the reporting of the Internal Reporting involving persons performing internal control functions in accordance with the Internal Control System adopted by the Board of Directors of the Company on 25.11.2019 and approved by the Audit Committee of the Company on 26.11.2019. (as may be amended from time to time by this document) carry out a regular internal audit of the proper functioning of the system of Violation Report and protection of Whistleblowers. Persons participating in the audit who are not authorised persons do not have access to personal data, in particular Identity Data.
13. Internal audit includes the examination and evaluation of, in particular:
  - a) compliance of actions taken, including Follow-up actions, with the provisions of the Act and Procedure,

- b) the effectiveness and efficiency of the actions taken, including Follow-up actions, particularly with regard to the actual operation of the protection measures granted to Whistleblowers under the Act and Procedure;
  - c) the impact of actions taken, including Follow-up of reported Violation, on improving the functioning of the affected elements.
14. Following the internal audit, an audit report shall be drawn up taking into account the matters indicated in points 5(1) - (3) of the audit, which shall be presented to the Audit Committee at least once a year, in time for it to be referred to in the Audit Committee's annual report.
  15. If the prohibited behaviour referred to in point 2 above does not occur and no reports are received in relation to it, an Audit is not required.

## 12. Register of Internal Reports

1. The employer keeps a register of Internal Reports.
2. The Register of Internal Reports shall be kept by authorised persons in accordance with paragraph 4(3) of the Procedure. Access to the Register and the data contained therein is restricted to Persons authorised to receive Internal Reports and to take follow-up actions. The register shall be protected from access by persons other than those authorised in accordance with paragraph 4(3) of the Procedure
3. The register referred to in point 1 shall contain, in particular, information on:
  - a) Internal Report number;
  - b) subject of the Violation;
  - c) the personal data of the Whistleblower and the Subject of the Report necessary to identify them;
  - d) Whistleblower's contact address;
  - e) the date of the Internal Report;
  - f) information on actions taken, including Follow-up actions;
  - g) the date of closure of the case
4. The Register of Internal Reports is maintained according to the model in Attachment 1 to the Procedure.
5. The employer is the controller of the data collected in the Internal Report Register.
6. The employer shall keep the documents and information obtained and produced as a result of the Internal Reports for a period of 3 years, after the end of the calendar year in which the Follow-up Actions were completed, or after the proceedings initiated by the Follow-up Actions are completed.

## 13. Final Provisions

1. This Procedure has been established after consultation with the Employee Representatives (elected in accordance with the Regulations for the Election of Employee Representatives of Action S.A.), completed on 18.09.2024.
2. The employer shall make information available about the possibility of reporting Violation, in particular through training and by making the Procedure available. A person applying for a job based on an employment or other legal relationship providing a basis for the provision of work or services or functions shall be informed of the Procedure by the Company at the commencement of recruitment or pre-contractual negotiations.
3. The resolution shall be effective as of 25 September 2024.
4. Employees of the Company and persons providing work or services on any other basis are required to familiarise themselves with the contents of the Procedure before they are allowed to work or provide services.
5. The Procedure is subject to posting on the Employer's website.
6. All amendments hereto must be made in writing or otherwise remain null and void.

**Attachment 1 - Model record of the Violation Report**

<b>Report number</b>	<b>Subject of the Violation</b>	<b>Data necessary for identification</b>	<b>Contact address</b>	<b>Date of Internal Report</b>	<b>Date of receipt of Internal Report</b>	<b>Information on Follow-up actions taken</b>	<b>Date of feedback</b>	<b>Date of case closure</b>