

# **RULES OF ARMEEC INSURANCE JSC for submitting internal reports within the meaning of the Act on Protection of Persons, Reporting Information, or Publicly Disclosing Information about Breaches**

<b>Version</b>	<b>Effective date</b>	<b>Adopted by</b>
2.0	08.07.2025 г.	The MB of Armeec Insurance JSC on 08.07.2025

**Headquarters:**

1407 Sofia, 51 James Bourchier Blvd.; tel.: 0700 1 3939; 02/811 91 03; www.armeec.bg  
UIC 121076907, IBAN: BG79 CECB 9790 1061 9050 00, BIC: CECBBGSF at CCB AD

## I. SUBJECT, OBJECTIVES AND SCOPE

1. These rules regulate the terms and conditions for internal submitting of signals in Armeec Insurance JSC, pursuant the requirements of section 1 from chapter II of the Whistleblower Protection Act (WPA or the Law).
2. The purpose of the rules is to provide to company employees an information regarding the terms and conditions for internal submitting of signals under the Bulgarian and European legislations, as well as to inform them of the options available to them when reporting illegal/unethical activity, abuses/unfair practices and any other information about breaches in Armeec Insurance JSC.
3. These rules apply to internal signals or public disclosure of information about:
  - 3.1. Breaches of Bulgarian legislation or the acts of the European Union specified in the annex to the WPA in the field of:
    - a) public procurement;
    - b) financial services, products and markets and the prevention of money laundering and terrorist financing;
    - c) product safety and compliance;
    - d) safety and transport;
    - e) radiation protection and nuclear safety;
    - f) food and feed safety, animal health and humane treatment;
    - g) public health;
    - h) consumer protection;
    - i) the protection of privacy and personal data;
    - j) the security of networks and information systems;
  - 3.2 breaches that affect the financial interests of the European Union within the meaning of Art. 325 of the Treaty on the Functioning of the European Union;
  - 3.3 breaches of the rules of the internal market within the meaning of Art. 26, paragraph 2 from the Treaty on the Functioning of the European Union;
  - 3.4 breaches related to cross-border tax schemes, the purpose of which is to obtain a tax advantage that is contrary to the object or purpose of the applicable law in the field of corporate taxation;
  - 3.5 committed crime of a general nature, for which a person under Art. 5 has learned in connection with the performance of his work or in the performance of his official duties.
  - 3.6. These rules also apply to signals or public disclosure of information about breaches of Bulgarian legislation in the field of:
    - a) the rules for payment of due public state and municipal receivables;
    - b) labour legislation;
    - c) the legislation related to the performance of public service.
  - 3.7 When in the sectoral acts of the European Union, specified in Part II of the Annex to WPA provide for special rules regarding the submission of signals of breaches, the rules specified in these acts or national regulations that introduce the relevant rules shall apply. These rules apply insofar as a matter is not necessarily regulated in the relevant sectoral acts and national regulations.
4. These rules do not apply to breaches signals:
  - 4.1. the procedures for awarding public contracts in the field of defence and national security, when they fall within the scope of Art. 346 of the Treaty on the Functioning of the European Union;
  - 4.2. of the protection of classified information within the meaning of Art. 1, para. 3 of the Law on the Protection of Classified Information;
  - 4.3. (amendment and addition – decision of the MB as of 08.07.2025) information which is protected by the confidentiality of conversations and correspondence between lawyers and their clients;
  - 4.4. of the confidentiality of health information within the meaning of Art. 27 of the Health Act;
  - 4.5. of the secrecy of the judicial conference;
  - 4.6. of the rules of criminal proceedings;
5. Pursuant to WPA protection under these rules is provided to the reporting person from the moment the signal is reported or the information about a breach is made public.
6. Pursuant to the law and these rules, reporting person is an individual who submits a signal or publicly discloses information about a breach committed during or in connection with the implementation of the activities of Armeec Insurance JSC and became known to him in his capacity as:
  - 6.1 worker, employee or other person who performs hired work for Armeec Insurance JSC, regardless of the nature of the work, the method of payment and the source of financing;
  - 6.2 a person, who performs work for Armeec Insurance JSC without an employment relationship and/or exercises a free profession and/or craft activity;
  - 6.3 volunteer or intern;
  - 6.4 partner, shareholder, member of the management or control body of Armeec Insurance JSC, member of the audit committee of Armeec Insurance JSC,
  - 6.5 a person who works for Armeec Insurance JSC, its subcontractors or suppliers;
  - 6.6 a job candidate who participated in a competition or other form of selection for employment at Armeec Insurance JSC and in this capacity received information about a breach;
  - 6.7 a worker or employee of Armeec Insurance JSC, when the information is received within the framework of an employment or service relationship that was terminated at the time of the submission of the signal or of the public announcement.
7. Protection under this rules is also provided to:
  - 7.1 any other reporting person who reports a breach that became known to him in a work context;
  - 7.2 (amendment and addition – decision of the MB as of 08.07.2025) persons who assist the reporting person in the process of submitting the report and whose assistance should be confidential;
  - 7.3 (amendment – decision of the MB as of 08.07.2025) persons connected with the whistleblower who may be subject to retaliation as a result of the reporting;
  - 7.4 legal entities in which the reporting person owns an equity interest, for which or with which he is otherwise connected in a work context.
8. A person submitting a breach signal through an internal or external reporting channel in the sense of WPA has the right to protection provided that:
  - 8.1. had reasonable cause to believe that the information submitted about the breach in the report was correct at the time of its submission and that this information falls within the scope of Art. 3 of these rules;
  - 8.2. has submitted a signal under the conditions and according to the order of these rules and WPA;
9. In the presence of the conditions under Art. 8, the right of protection of the person who submits a breach signal under Art. 3 of these rules to institutions, bodies, offices or agencies of the European Union. Such reporting shall be considered external channelling.
10. A person who publicly discloses an information about a breach has the right of protection when there was a reasonable grounds to believe that the information about the breach was true at the moment of its disclosure and that such information falls within the scope of Art. 3 of these rules and one of the following conditions is met:
  - 10.1 the person reported signal under the conditions and according to the order of these rules and the WPA, but no relevant actions were taken on the signal within the terms provided for in sections I and II of chapter two of the WPA;
  - 10.2 the person has reason to believe that:

### Headquarters:

1407 Sofia, 51 James Bourchier Blvd.; tel.: 0700 1 3939; 02/811 91 03; www.armeec.bg  
 UIC 121076907, IBAN: BG79 CECB 9790 1061 9050 00, BIC: CECBBSGF at CCB AD

- a) (addition – decision of the MB as of 08.07.2025) the infringement may constitute an immediate or manifest danger to the public interest, or there is an emergency situation or a risk of irreparable harm;
  - b) in case of external signal reporting, there is a risk of retaliatory actions or there is a possibility that the breach will not be effectively dealt with due to the danger of concealment or destruction of evidence, suspicion of collusion between the competent authority and the perpetrator of the breach, or the complicity of the authority in the breach, as well as due to other specific concrete circumstances of the case.
11. (amendment – decision of the MB as of 08.07.2025) No proceedings shall be initiated to examine a report when the report is anonymous.
  12. (amendment and addition – decision of the MB as of 08.07.2025) Individuals who have anonymously reported breaches not in accordance with these rules or the law, or who have publicly but anonymously disclosed information about breaches and subsequently been identified and subjected to retaliation, are entitled to protection where the conditions under Art. 7.1 and Art. 10 of these rules are met.
  13. Considering the possibility of quickly preventing a breach or removing of the consequences deriving from such breach, the signal should be reported as a priority through the internal signal reporting channel described/specified in these rules.
  14. In case there is a reasonable assumption that the reporting person is at risk of retaliation, discriminating against him, and that no effective measures will be taken to verify the signal, the signal may be reported through an external submission channel, namely the signal can be submitted to the Personal Data Protection Commission. Information about the external signal reporting channel, such as address, email address, phone number, etc. can be found on the website of the Commission for the Protection of Personal Data, at the address: www.cdpd.bg.
  15. (amendment and addition – decision of the MB as of 08.07.2025) Persons reporting or publicly disclosing information about violations may choose the method of reporting: through an internal or external reporting channel, or both.

## II. INTERNAL CHANNEL FOR REPORTING SIGNALS

16. Armeec Insurance JSC is creating an internal channel for reporting breaches as the company provides information on the terms and conditions for reporting internal signals on its website, as well as in a prominent place in the company's offices.
17. The channel regulated in these rules for internal reporting of breaches:
  - 17.1 It is managed in a way that guarantees the completeness, integrity and confidentiality of the information and prevents unauthorized persons from accessing that information;
  - 17.2 Enables the storage of information recorded on a durable medium for the needs of the investigation of the signal and for further investigations.
18. Armeec Insurance JSC determines with an internal act the official that will be responsible for considering the signals according to these internal rules and WPA
19. The official mentioned in Art. 18 of these rules may also carry out other duties and functions assigned to him by the company, in the even that their combining them does not lead to a conflict of interests.
20. In order to ensure the absence of a conflict of interest, the continuity of the activity on the examination of the signals and the observance of the terms under the WPA, the company appoints a substitute official, who should meet the conditions and requirements for the official.
21. In the event that the official finds himself in a hypothesis of a conflict of interest for a breach case filed before him/considered by him, he is obliged to submit a reasoned written rebuttal from this case immediately after learning of the conflict, as in these cases the signal is reviewed and processed by the substitute official.

## III. PROCEDURE FOR SUBMITTING AND CONSIDERATION OF INTERNAL REPORTS FOR BREACHES

### Reporting

22. The report shall be submitted to an official responsible for handling reports, in writing, including by personal delivery, regular or electronic mail, or orally.
23. Verbal signalling can be done by phone, through other voice messaging systems, and at the request of the reporting person – through a personal meeting in a suitable time agreed between the parties.
24. To register each submitted report, the company uses a form approved by the national body for external reporting (Personal Data Protection Commission), according to the model representing Annex No. 1 to these rules, which contains at least the following data:
  - 24.1 Full name, address, and telephone number of the submitter, as well as e-mail, if any;
  - 24.2 The names of the person against whom the report is submitted and their place of employment, if the report is submitted against specific persons and they are known;
  - 24.3 Specific details of a breach or of a real danger of such being committed, the place and period of the breach, if it was committed, description of the act or the situation and other circumstances, as far as such are known to the reporting person;
  - 24.4 Date of report's submission;
  - 24.5 Signature, digital signature or other identification of the sender.
25. (amendment and addition – decision of the MB as of 08.07.2025) The written report is submitted by the reporter by filling out the form (Appendix No. 1 to these rules). The verbal report is documented by filling out the form by the official responsible for reviewing reports, who offers the reporter to check, correct, and approve it by signing it. With the explicit consent of the person submitting the report by telephone or other voice messaging system or in a face-to-face meeting, the report may also be documented by means of a recording on a durable medium that allows it to be retrieved.
26. Any kind of sources of information supporting the statements made in it and/or reference to documents can be attached to the report, including indicating data on persons who could confirm the reported data or provide additional information.
27. If the report does not meet the requirements under Art. 22-24 of these rules, the whistleblower is sent a message to eliminate the admitted irregularities within 7 days of receiving the report. If the irregularities are not corrected within this period, the report together with the attachments to it is returned to the reporting person.
28. Each alert is checked for its credibility. Signals that do not fall within the scope of these rules or WPA and the content of which do not give reasons to be considered plausible are not considered. Reports that contain patently false or misleading statements of fact will be returned with instructions to the sender to correct the statements and the sender's responsibility for persuasion.

### Working with signals. Internal inspection

29. The official responsible for the consideration of the signals is obliged to:
  - 29.1 receive reports and confirm their receipt within 7 days after their receipt;
  - 29.2 guarantees that the identity of the reporting person and any other person mentioned in the report will be duly protected and take the necessary measures to limit the access to the report to unauthorized persons;
  - 29.3 maintains contact with the reporting person, requesting additional information from him and third parties if necessary;
  - 29.4 provide a feedback to the reporting person on the actions taken regarding the report no longer than three months after the confirmation of receipt of the report;
  - 29.5 provide the persons wishing to signal for breach a clear and easily accessible information about the procedures for external reporting of signals to the competent national authority and, where appropriate, to the institutions, bodies, offices and agencies of the European Union;

### Headquarters:

1407 Sofia, 51 James Bourchier Blvd.; tel.: 0700 1 3939; 02/811 91 03; www.armeec.bg  
UIC 121076907, IBAN: BG79 CECB 9790 1061 9050 00, BIC: CECBGBSF at CCB AD

- 29.6 documents the verbal signals;
- 29.7 maintains a register of the submitted reports;
- 29.8 listens to the person against whom the report was submitted, or to accept his written explanations and to collect and evaluate the evidence indicated by him;
- 29.9 provides to the concerned person all gathered evidences and gives the opportunity to the person to object them within 7 days, subject to the reporting person's protection;
- 29.10 provides an opportunity to the concerned person to provide and to present new evidences to be collected in the course of the investigation;
- 29.11 in case the facts presented in the report are confirmed:
  - a) organizes the taking of follow-up actions in connection with the report, and for this purpose may require the assistance of other persons or units in the structure of Armeec Insurance JSC;
  - b) offers the company to take specific measures in order to stop or prevent the breach in cases where it has been established or there is a real danger of its imminent commission;
  - c) directs the reporting person to the competent authorities when his rights are affected;
  - d) forwards the signal to the external reporting body (ERB) if it is necessary to take action on his part, and the whistleblower is notified in advance of the forwarding; in case the report is filed against the whistleblower's employer, an official responsible for reviewing the report directs the person to simultaneous reporting to the external reporting body (ERB).

#### Follow-up actions actions of the Company

- 30. Based on the incoming report and the proposals of the official, the company acting through the Board of Directors and/or the persons who are authorized to manage and represent Armeec Insurance JSC:
  - 30.1. undertakes actions within their competency to interrupt the breach or to prevent it, in case it hasn't begun yet;
  - 30.2. prioritizes, according to previously established criteria and rules, the handling in case many reporting signals are submitted regarding more severe breaches;
  - 30.3. terminates the inspection:
    - a) if the breach for which a report has been filed is an insignificant case and does not require the application of additional follow-up actions; the termination shall not affect other obligations or applicable procedures in relation to the breach for which the signal has been submitted, nor it does affect the protection pursuant to this law regarding the internal or external reporting;
    - b) in case there is a repeated report without any new information of a significant importance for a breach, regarding which another inspection has already been completed, unless there are new legal or factual circumstances which provide grounds for undertaking follow-up action;
    - c) when data for a committed crime is collected; the report and the materials thereto are sent immediately to the Public Prosecutor's Office;
    - d) approves the singular report which describes briefly the information from the report, the performed actions, the definite results of the inspection regarding the signal; the results, together with motivation, are reported to the worker or employee who submitted the signal, as well as to the concerned person, fulfilling the obligation of protecting them.
  - 30.4. In case the inspection has been terminated on the grounds of Art. 30.3., letter a) or b), the person who submitted the reporting signal may report to the national body for reporting external signals.

#### IV. REGISTER OF SIGNALS

- 31. Armeec Insurance JSC shall create and maintain a register of the breaches signals (according to the draft approved by the national body for external reporting (the Commission for Personal Data Protection), which is available at Appendix 2 to these rules); the register shall not be public.
- 32. The register shall be administrated by the official and shall contain information about:
  - 32.1. the person who received the signal;
  - 32.2. the date of submitting the signal;
  - 32.3. the concerned person, if such information is available in the signal;
  - 32.4. general data for the claimed breach, such as place and time of performing the breach, a description of the act and other circumstances of its performance;
  - 32.5. the connection between the submitted signal with other signals, after such a connection has been identified upon handling the signal;
  - 32.6. information which has been presented as feedback to the reporting person, and the date of such presentation;
  - 32.7. the undertaken follow-up actions;
  - 32.8. the results of the inspection regarding the signal;
  - 32.9. the period of keeping the signal.
- 33. The information entered into the register shall be kept in a manner that guarantees its privacy and security.
- 34. The procedure for keeping the register shall be determined by an internal act of Armeec Insurance JSC in compliance with the regulation of the national body for external reporting. Before the approval and promulgation of the regulation under the previous sentence, the register shall be kept by the official, and every circumstance to be entered shall appear at the register not later than the end of the day in which the circumstance has been disclosed.
- 35. The official is obliged to submit regularly the mandatory statistics to the national body for external reporting, according to the procedure established by this body, including, if there is a technical possibility, to establish direct connection between the register of Armeec Insurance JSC and the register kept by the Commission for Personal Data Protection.

#### V. ADDITIONAL RULES

- 36. Armeec Insurance JSC shall apply appropriate measures to protect the information related to the reported signals for breaches, as well as to protect the identity of the reporting person, by granting access to the information exclusively to the employees who need the data to perform their work duties, and they shall have the necessary access level to the information.
- 37. Upon transferring data or referring to company's circumstances, the identity of the reporting person cannot be revealed, directly or indirectly, nor can assumptions about their identity be originated.
- 38. Art. 36 and 37 shall be applied to protect the identity of the concerned persons, too.
- 39. The disclosure of the identity or the information under Art. 36 shall be allowed exclusively with the explicit consent in writing of the reporting person.
- 40. The identity of the reporting person or any other information that might reveal, directly or indirectly, their identity, may be disclosed exclusively when it represents a mandatory and proportional obligation imposed by Bulgarian or European legislation, related to investigations by national bodies or legal proceedings, including in respect of protecting the right of the concerned person to defend themselves. In these cases, before disclosing the identity or the information contained in the reported signals, Armeec Insurance JSC shall notify the reporting person for the need to disclose such data. The notification shall be in writing and motivated. The reporting person shall not be notified if such notification might endanger the investigation or the legal proceedings.
- 41. The processing of personal data that is made pursuant to these rules and/or the WPA, including the exchange or transmission of personal data by the competent bodies, shall be performed pursuant to Regulation (EU) 2016/679 and Directive (EU) 2016/680; if institutions, bodies, services or agencies of the European Union take part in the transmission, it shall be performed pursuant to Regulation (EU) 2018/1725, as well as to Personal Data Protection Act.

#### Headquarters:

1407 Sofia, 51 James Bourchier Blvd.; tel.: 0700 1 3939; 02/811 91 03; www.armeec.bg  
 UIC 121076907, IBAN: BG79 CECB 9790 1061 9050 00, BIC: CECBBSGF at CCB AD

42. By carrying out the activities and fulfilling the obligations pursuant to these Terms and Conditions and to WPA, Armeec Insurance JSC shall not collect personal data which is not relevant to handling the particular signal, and if they are collected by accident, they shall be deleted.

## VI. ADDITIONAL PROVISIONS

43. For the purposes of these rules, the following definitions are used
- 43.1. "Breaches" mean actions or omissions which are:
- illegal or related to the Bulgarian legislation or European acts regarding the fields indicated in Art. 3, or
  - contradictory to the subject or the purpose of the dispositions of the acts of the European Union and the fields indicated in Art. 3.
- 43.2. "Employer" means every physical person, legal entity or its department, as well as any other organizational or economically independent entity (enterprise, institution, organization, cooperation, farm, establishment, household, company or other) which enters independently with workers or employees in employment and service relation, by hiring them, including for performing homework or work from home, or send to another company – beneficiary to perform certain tasks.
- 43.3. "Information about a breach" means information, including reasonable suspicions, for existing or potential breaches which have been committed or is highly probable that they might be committed in the organization where the reporting person is employed or has been employed, or in another organization with which such person has been in touch with while working, as well as for attempts to hide breaches.
- 43.4. (amendment – decision of the MB as of 08.07.2025) "Work context" means current or past work activities in the public or private sector through which, regardless of their nature, persons receive information about breaches and within which those persons may be subject to retaliation if they report such information.
- 43.5. "Concerned person" means a physical person or legal entity which is to be indicated upon submitting the signal or upon public disclosure of information as the person to whom the breach is attributed or to which this person is connected.
- 43.6. "Feedback" means providing to the person who reported the signal information about actions which are provided for or undertaken as follow-up actions, as well as about the grounds for this follow-up action.
- 43.7. "Enterprise" means every physical person, legal entity or civil partnership which carries out economic activity, irrespective of its property, legal or organizational form.
- 43.8. (amendment – decision of the MB as of 08.07.2025) "Persons related to the whistleblower" are third parties who may be subject to retaliation in a work context, such as colleagues or relatives without limitation as to degree.
- 43.9. "Retaliation" means every direct or indirect action or omission which takes place in work context, is provoked by internal or external reporting or by public disclosure, and which provokes or might provoke adverse consequences damaging to the reporting person.
- 43.10. "Follow-up actions" mean all actions undertaken by the person who receives the signal or by other competent body with the aim to evaluate the exactness of the allegations presented in the signal and their appropriateness, with the aim of handling the reported breach, including through actions such as internal inquiry, investigation, criminal prosecution, actions to secure funds or terminating the procedure.
- 43.11. "Enough data" means such data which can serve to make a reasonable assumption for a committed breach which falls into the scope of application of this law.
- 43.12. "Internal reporting" means announcing information, verbally or in writing about breaches within certain legal subject of the public or private sector.
- 43.13. "External reporting" means announcing information, verbally or in writing about breaches to the appropriate bodies.
- 43.14. "Privacy of personal life" means every breach of the personal space pursuant to Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (OB, L 201/37 of 31 July 2002).

## VII. FINAL PROVISIONS

44. These rules have been approved by a decision of the Management Board of Armeec Insurance JSC, filed in protocol No 77П/24.04.2023 and they shall enter into force as of the date of their approval. The rules have been amended and supplemented by a decision of the Management Board – Protocol No. 98/08.07.2025, effective as of 08.07.2025.
45. These rules are subject to annual review by the official and the legal department, and amendments of them are to be approved following the same procedure as the approval of the Terms and Conditions. The rules shall be reviewed also in case of changes of the current legislation. Every three years the persons indicated in the first sentence shall perform an analysis of the practice of applying the rules which shall be presented to the Management Board of the company.
46. For matters which concern the application of these Terms and Conditions or the reporting of breaches, you may contact the official  
 – Mr. Ivo Hristov. Contact data of Mr. Ivo Hristov:  
 Address: Sofia, 51 James Bourchier Blvd.  
 Telephone: +359 2 8119 184; email: i.hristov@armeec.bg

Version	Adopted	Effective date	Reasons for the change	Author of the document
1.0	Protocol No. 77П / 24.04.2023	24.04.2023	Initial acceptance of the rules	Compliance Directorate and Legal Directorate
2.0	Protocol No. 98/ 08.07.2025	08.07.2025	Bringing into line with the amendments to the WPA.	Compliance Directorate and Legal Directorate

### Headquarters:

1407 Sofia, 51 James Bourchier Blvd.; tel.: 0700 1 3939; 02/811 91 03; www.armeec.bg  
 UIC 121076907, IBAN: BG79 CECB 9790 1061 9050 00, BIC: CECBBSGF at CCB AD