

Procedure on making reports by whistleblowers

Applies to

1. Prudential International Assurance plc Spółka Akcyjna Oddział w Polsce
2. Prudential Poland sp. z o.o.

Introduction

At M&G group, we value a culture of openness, integrity and accountability. We set ourselves the highest possible standards of professional and ethical conduct. We must demonstrate integrity at all times and require ourselves and our associates to do what is right and raise our concerns when we notice breaches of the law or Prudential's internal procedures, or unethical behavior.

This policy encourages about any matter that may adversely affect M&G plc and its affiliates, to raise such concerns via colleagues, line management or the 'Speak Out' service. In addition concerns regarding the behaviour of colleagues that do not align to M&G plc's values and behaviours can also be raised.

We encourage individuals who have concerns or suspicions of actual or suspected wrongdoing in relation to laws, rules, and regulations applicable to M&G plc and its affiliates (a criminal offence has been committed or failing to comply with any other legal obligation) to raise their concerns.

All reports of misconduct are taken seriously and are independently and confidentially investigated, with all investigations being governed by the Speak Out programme.

Individuals who raise concerns via the whistleblowing process are protected from retaliation and mistreatment in response to raising a legitimate concern. This procedure is to ensure that reports are handled without undue delay, independently and accurately by trained specialists, and without adverse consequences for reporting persons.

This Procedure also fulfills legal requirements related to the adoption of the Whistleblower Protection Act of 23 May 2024, as well as the obligation under the Counteracting Money Laundering and Terrorist Financing Act of 1 March 2018 to implement an internal procedure for anonymous reporting by employees or other persons performing activities for the obliged institution of actual or potential breaches of counteracting money laundering and terrorist financing regulations.

Definitions

Follow-up	Action taken by Prudential (M&G) to assess the accuracy of the information contained in the report and to counteract the reported breach of the law, in particular through an investigation
Retaliation	Direct or indirect act or omission which occurs in a work-related context, is prompted by making a whistleblowing reporting or a public disclosure, and which infringes or may infringe the whistleblower's rights or causes or may cause unjustified detriment to the whistleblower, including unwarranted initiation of proceedings against the whistleblower
Information on a breach	Information, including a reasonable suspicion, about an actual or potential breach which occurred or is very likely to occur at Prudential (M&G), in which the whistleblower participated during the recruitment process or other negotiations preceding the conclusion of a contract, where he or she works or has worked, or in another legal entity with which the whistleblower is or was in contact through his or her work, or information about attempts to conceal such a breach
Feedback	Information provided to the whistleblower on actions envisaged or taken as follow-up and on the reasons for such follow-up
Work-related context	Current, past or future work activities under an employment or other legal relationship constituting the basis for performing work, supplying services or holding a position at or for Prudential (M&G)
NAVEX	Third party authorized on behalf of Prudential (M&G) to receive whistleblowing reports under the Speak Out program
EthicsPoint	Telephone, online, and mobile device system for internal reporting at Prudential (M&G) for whistleblowers, operated by a third-party company, NAVEX.
Person concerned	Natural or legal person or unincorporated organizational unit who is granted legal capacity under the Act, referred to in the report as a person who committed the breach or as a person with whom the person who committed the breach is associated
Facilitator	Natural person who assists the whistleblower in the reporting process in a work-related context, and whose assistance should be confidential

Person associated with the whistleblower	Natural person who may suffer retaliation, including an associate or a person closest to the whistleblower (a spouse, ascendant, descendant, siblings, affinity in the same line or degree, person in a relationship of adoption and his or her spouse, and a person in cohabitation)
Prudential	Collectively Prudential International Assurance plc S.A. Oddział w Polsce and Prudential Polska Sp. z o.o., unless specified otherwise
Speak Out	Whistleblowing team based in London, managed by M&G group's Whistleblowing Operations Manager
Whistleblower	Reporting person, as indicated in Chapter 2 of the Procedure
Public disclosure	Making of information on a breach available in the public domain, as described in Chapter 9
Internal report(ing)	Oral or written communication to Prudential (M&G) of information on a breach. Detailed rules and technical issues related to internal reporting are described in Chapter 3 and in other parts of the Procedure
External report(ing)	Oral or written communication to the Ombudsman or a public authority of information on a breach. External reporting is further described in Chapter 9.

Chapter 1 – Objective scope of the Procedure

1. The Procedure covers the reporting by Whistleblowers of breaches of the law specified in the Whistleblowers Act, i.e. acts or omissions that are unlawful or intended to circumvent the law, concerning:
 - 1) corruption;
 - 2) public procurement;
 - 3) financial services, products and markets;
 - 4) counteracting money laundering and terrorist financing;
 - 5) product safety and compliance;
 - 6) transport safety;
 - 7) protection of the environment;
 - 8) radiation 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 network and information systems;
 - 15) financial interests of the State Treasury of the Republic of Poland, local government units and the European Union;
 - 16) internal market of the European Union, including public law rules of competition and state aid, as well as corporate taxation;
 - 17) constitutional freedoms, as well as human and citizen rights – in relations between individuals and public authorities, and not related to the areas specified in items 1-17.
2. Internal reporting may also concern breaches of any internal regulations or ethical standards in force at Prudential, which have been established by Prudential on the basis of, and remain consistent with, generally applicable laws.
3. The object of internal reporting may also include any other irregularities and suspected breaches of applicable laws or Prudential's internal regulations, e.g.:
 - a. an offence or a breach of the law, rules and regulations applicable to M&G plc (a criminal offence has been committed or failing to comply with any other legal obligation);

- b. a breach of M&G plc's policies and procedures;
 - c. a breach of M&G plc's Values and Behaviours;
 - d. bullying or any form of harassment;
 - e. racial, sexual, or disability discrimination concerns;
 - f. health and safety of the public and/or other employees;
 - g. possible human rights violations;
 - h. suspicions of financial crime;
 - i. corporate accounting practices, internal accounting controls, or auditing matters;
 - j. breaches of the protection of privacy and personal data, and security of network and information systems;
 - k. behaviour that harms or is likely to harm the reputation or financial wellbeing of M&G plc;
 - l. neglect, abuse or not acting in the best interest of M&G plc's customers;
 - m. other unethical conduct; or
4. the deliberate concealment of any of the above. Due to the limitations arising from the Whistleblowing Act, the breaches described in Sections 2 and 3 may not be proceeded as external reporting or public disclosures within the meaning of the above Act.

Chapter 2 – Subjective scope of the Procedure

1. Reports with information on a breach obtained in the work-related context may be made by the following natural persons:
 - 1) employee;
 - 2) temporary employee;
 - 3) person performing work on a basis other than an employment relationship, including under a civil law contract;
 - 4) entrepreneur;
 - 5) commercial proxy;
 - 6) shareholder or member;
 - 7) member of an authority of a legal person or an unincorporated organizational unit;

- 8) person performing work under the supervision and direction of Prudential's contractor, subcontractor or supplier;
 - 9) intern;
 - 10) volunteer;
 - 11) trainee
 - 12) or any other individual with concerns about Prudential that were obtained in a work-related capacity.
2. The reports referred to in Section 1 may also be made before an employment or other legal relationship constituting the basis for performing work, supplying services or holding a position at or for Prudential is established or after it has terminated.

Chapter 3 – Reporting method

1. Concerns or suspicions of actual or suspected wrongdoing covered by the Procedure may be reported in one of the following ways:
 - a. Internal reports – the basic method of reporting by whistleblowers who wish to maintain confidentiality or anonymity described in this Procedure;
 - b. External reports – to the Ombudsman or other public authority, further described in Chapter 9;
 - c. Public disclosures – making of information available in the public domain, further described in Chapter 9.
2. Where a person wants to report an actual or suspected breach specified in Chapter 1 within Prudential and wants to benefit from protection granted to a whistleblower or wants to keep his or her report confidential for any reason, he or she should do so through the Speak Out process under internal reporting.
3. Internal reporting at Prudential shall be made through EthicsPoint, which is operated by an independent, third-party company, NAVEX. EthicsPoint is available 24/7 and also operated in Polish (both the hotline and the website). The website can be accessed from any device connected to the Internet.
4. The dedicated EthicsPoint hotline and website allow all reports to be made anonymously. The use of EthicsPoint has no adverse consequences for the reporting person, subject to Section 12. Below are presented the details on how to make an internal report. Additionally, these data are available on Prudential's intranet.
 - a. Free hotline: 800-005-005
 - b. EthicsPoint website where a report can be made electronically/in writing by completing a special form: <https://secure.ethicspoint.eu/domain/media/pl/gui/105606/index.html>

- c. Postal mail to Prudential's address in Poland (ul. 182 Puławska, 02-670 Warszawa) – in this case, please make a visible marking on the envelope that the mail is confidential and concerns Speak Out or a whistleblower's report so that it is not opened by an unauthorized person;
 - d. Physical meeting – the intention of such a meeting can be reported through the EthicsPoint website, hotline or through a request filed with the Head of the Legal and Compliance Department at Prudential.
5. If an oral report is made through the hotline, it shall be documented with the consent of the whistleblower in the form of:
 - a. recording of the conversation in a retrievable form, or
 - b. complete and accurate transcript of the conversation prepared by NAVEX.
6. If, in the case of an oral report, the whistleblower has not consented to recording, the report shall be documented in the form of minutes of the conversation, reproducing its exact course.
7. In the cases referred to in Section 6(b) and Section 7 above, the whistleblower may check, rectify and agree the transcript of the conversation or the minutes of the conversation by signing the same.
8. At the request of the whistleblower, an oral report may be made at a physical meeting held within 14 days of receiving such a request. We emphasize that the meeting will be held in Poland at a location agreed with the whistleblower and will be conducted by an authorized representative of the Compliance Team. In such a case, with the consent of the whistleblower, the report shall be documented in the form of:
 - a. recording of the conversation in a retrievable form, or
 - b. minutes of the meeting, reproducing its exact course, prepared by Prudential (the whistleblower may check, rectify and agree the minutes of the meeting by signing the same).
9. We emphasize that core activities related to whistleblowers' reports made via EthicsPoint or directly to the Speak Out team are handled on behalf of the M&G group based in London, while the involvement of the Compliance Team in this process is limited. If the Compliance Team participates in a given report, only the Head of the Legal and Compliance Department and the Compliance Team Managers are authorized to perform the activities related to whistleblowers' internal reports. These persons have access to data only to the extent necessary to perform their duties under the Whistleblowing Act and to ensure that internal reports are handled properly.
10. While using EthicsPoint the whistleblowers will be required to log into their report via the unique Report Key provided to them and also be creating their own password.
11. All persons involved in the processes provided for in this Procedure are duly authorized in writing and bound by the obligation of secrecy regarding the information and personal data obtained in the context of the receipt and verification of internal reports.
12. Prudential encourages reporting irregularities and breaches immediately upon becoming aware of them. The report should contain the necessary information to allow a confidential investigation to be conducted.

13. The Speak Out program and confidential reporting system must not be used for deliberate rumors or intentional misrepresentation. In an extreme case, such action may also be subject to criminal proceedings (relevant criminal regulations are described in Chapter 10).

Chapter 4 – Prudential’s conduct in the event of a report

1. In accordance with the policy of the M&G plc group, of which Prudential is a member, NAVEX is a third party authorized to supply a confidential reporting system (EthicsPoint) to receive whistleblowing reports under the Speak Out program. Prudential’s Compliance Team in Poland is an internal unit authorized within Prudential to provide M&G’s Speak Out function with necessary support, if required. After receiving a report, NAVEX provides relevant information to the Speak Out team to initiate an investigation.
2. Prudential’s Compliance Team is determined as internal unit authorized to perform follow-up actions within the scope required by Polish law. In accordance with the policy of the M&G plc group, of which Prudential is a member, the Speak Out team based in London is authorized within the entire M&G group to manage whistleblowing reports, conduct confidential investigations and perform follow-up actions, also by verification of a whistleblowing report and further communication with the whistleblower, including requesting additional information and providing feedback to the whistleblower including via EthicsPoint. The Speak Out team liaises with the Compliance Team to the extent that detailed knowledge of local procedures and laws in force at Prudential is necessary to manage the report or such engagement is necessary for other reasons, and provided that there is no conflict of interest, e.g. in connection with the situation where a whistleblowing report concerns the Compliance Team.
3. Prudential ensures that whistleblowing reports of actual or suspected misconduct including breaches and irregularities are confidentially, thoroughly and independently managed.
4. If the Speak Out program is used to make a whistleblowing report through the confidential hotline or the online platform (EthicsPoint), the reporting person shall receive an acknowledgement of receipt of the report, as well as the Report Key and they will need to generate their own password. These are needed to access their report.
5. Prudential must acknowledge the receipt of the whistleblowing report to the whistleblower within seven days of its receipt, unless the whistleblower has not indicated the contact address to which the acknowledgement should be sent and it is impossible to send the same.
6. A review of the report commences with an analysis of the concerns to determine whether the reports qualifies as a whistleblowing. The reporting person may be requested to provide additional information as part of the initial review or on-going confidential investigation. The reporting person will also be provided periodic updates on the status of the confidential investigation and also be provided feedback, including any relevant findings, at the conclusion of the investigation and any the actions taken, where deem appropriate. This information may not contain all details if confidentiality so requires.
7. Prudential shall provide feedback to the whistleblower as soon as possible in the circumstances of the given report, but in any event within a period not exceeding three months from the date of acknowledgement of receipt of the internal report, unless the whistleblower has not provided a contact address to which the feedback should be provided.

8. Where a whistleblowing report is related to the area of counteracting money laundering or terrorism financing, following an investigation, the Speak Out team shall decide on further actions and immediately communicate the relevant information to the Compliance Team. The Head of the Legal and Compliance Department shall assess the legitimacy of notifying the General Inspector of Financial Information or the competent prosecutor referred to in the Counteracting Money Laundering and Terrorist Financing Act of 1 March 2018.

Chapter 5 – Protection and warranties granted to the whistleblower and other persons

1. The communication by the whistleblower, in good faith, of any reports of actual or suspected misconduct including any irregularities or breaches shall not be a reason for any adverse consequences of a repressive or discriminatory nature to the whistleblower or of any actions deteriorating his or her legal or factual situation or involving threats or other manifestations of unfair treatment. In particular, the reporting person shall not be subject to actions that adversely affect the terms of his or her work or employment, as described in detail in Section 4 below.
2. The whistleblower is protected from the moment of making a whistleblowing report (internal or external) or public disclosure, provided that he or she has reasonable grounds to believe that the information which is the object of the whistleblowing report (internal or external) or in the public disclosure is true at the time when such report or disclosure is made and that it constitutes information on a suspected or actual form of misconduct including a breach.
3. Prudential does not tolerate any form of discrimination, harassment, persecution or retaliation in response to making a whistleblowing report. An employee who has suffered retaliation or threats in response to a whistleblowing report should immediately inform the Speak Out team or the Legal and Compliance Department. Every report on retaliation is investigated independently and thoroughly. Persons involved in retaliation against a reporting employee may face disciplinary consequences, including possible dismissal or termination of cooperation.
4. The catalogue of examples of prohibited retaliation against the whistleblower includes, but is not restricted to:
 - a. refusal to enter into an employment relationship;
 - b. termination of employment relationship without notice;
 - c. failure to conclude a fixed-term employment contract or an indefinite-term employment contract after the termination of a probationary contract, failure to conclude another fixed-term employment contract or failure to conclude an indefinite-term employment contract after the termination of a fixed-term contract – where the whistleblower had a legitimate expectation that such a contract would be concluded with him or her;
 - d. reduction of the remuneration for work;
 - e. withholding or omission for promotion;
 - f. disregarding or reducing work-related benefits other than remuneration;
 - g. transfer to a lower job position;

- h. suspension from employee or official duties;
 - i. handing over the whistleblower's existing duties to another employee;
 - j. unfavorable change in the workplace or working time pattern;
 - k. negative performance evaluation or negative job opinion;
 - l. imposition or application of a disciplinary measure, including a financial penalty, or a measure of a similar nature;
 - m. coercion, intimidation or exclusion;
 - n. mobbing;
 - o. discrimination;
 - p. unfavorable or unfair treatment;
 - q. withholding of, or omission from, participation in training courses to improve professional competence;
 - r. unjustified referral to medical examinations, including psychiatric examinations, unless separate regulations provide for referral to such examinations;
 - s. action aimed at making it more difficult to find a job in the future in a given sector or industry on the basis of an informal or formal sectoral or industry agreement;
 - t. causing financial loss, including economic loss, or loss of income;
 - u. causing other non-pecuniary damage, including breach of personal rights, in particular the whistleblower's reputation.
5. An attempt or threat to take the measure referred to in Section 4 shall also be regarded as retaliation for reporting or public disclosure.
 6. If Prudential takes actions against the whistleblower which are included in the catalogue referred to in Section 4, the burden of proving that a given activity is not retaliation shall rest with Prudential.
 7. The ban on retaliation set forth in Section 4 applies accordingly to whistleblowers providing work or services to Prudential on a basis other than employment relationship; in particular the following is banned:
 - a. termination of a contract to which the whistleblower is a party, in particular relating to the sale or supply of goods or services, withdrawal from such a contract or its termination without notice;
 - b. imposition of an obligation or refusal to grant, restriction or withdrawal of an entitlement, in particular a concession, permit or relief.
 8. Making of a whistleblowing report (internal or external) or public disclosure may not give rise to liability, including disciplinary liability or liability for damage for breach of the rights of other persons or obligations set forth in the laws, in particular as regards defamation, infringement of personal rights, copyrights,

protection of personal data and obligation of secrecy, including trade secret, provided that the whistleblower has reasonable grounds to believe that the internal or external report or public disclosure is necessary to disclose the breach of law in accordance with the Act.

9. The rights set forth in this Chapter may not be waived, nor may liability be accepted for damage arising from the making of a whistleblowing report or public disclosure, provided that this shall not apply to acceptance of liability for damage arising from knowingly making a report or public disclosure of false information.
10. The whistleblower who has suffered retaliation is entitled to compensation in the amount not lower than the average monthly salary in the national economy in the previous year, published for pension purposes in the Official Journal of the Republic of Poland, *Monitor Polski*, by the President of the Statistics Poland, or to redress.
11. A person who has suffered damage as a result of the whistleblower's knowingly making a report or public disclosure of false information is entitled to compensation or regress for an infringement of personal rights from the whistleblower who made such a report or public disclosure.
12. The provisions of this Chapter apply accordingly to the facilitator and the person associated with the whistleblower, as well as to a legal person or another organizational unit supporting or associated with the whistleblower, in particular owned by the whistleblower or employing the same.
13. The rules of protection of reporting persons against repression or retaliation set forth in this Chapter also apply to employees or other persons performing activities related to counteracting money laundering and terrorist financing, who, in accordance with the Counteracting Money Laundering and Terrorist Financing Act of 1 March 2018, may notify the General Inspector of Financial Information about:
 - circumstances that may imply the suspected commission of an offence of money laundering or terrorist financing,
 - reasonable suspicion that a specific transaction or specific assets may be involved in money laundering or terrorist financing,
 - conducting a suspicious transaction.

The above also applies to employees and other persons performing activities related to counteracting money laundering and terrorist financing, who, in accordance with the Counteracting Money Laundering and Terrorist Financing Act of 1 March 2018, may notify the competent prosecutor about a reasonable suspicion that the asset which is the object of the transaction originates in or is related to an offence other than an offence of money laundering or terrorist financing or a fiscal offence, or about conducting such a transaction.

Such employees and other persons performing activities related to counteracting money laundering and terrorist financing for Prudential, who are exposed to repressive activities described in this Chapter, are also entitled to report cases of such activities to the General Inspector.

Chapter 6 – Confidentiality and protection of personal data

1. There is an absolute confidentiality obligation in the process of receiving and managing whistleblowing reports. Personal data of the reporting person and other persons indicated in the report are kept confidential by employees or associates authorized to act in accordance with the Procedure, who participate in the processing of the report. These data are only made available to persons who need access to them to process a report and conduct a confidential investigation.
2. The reporting person is granted anonymity throughout the proceedings, unless that person has disclosed his or her identity and subject to situations where disclosure of identity is required by generally applicable laws.
3. The Speak Out program allows anonymity. No action shall be taken in the course of the investigation to identify the reporting person.
4. The joint controllers of the personal data of the reporting and other persons indicated in the whistleblowing report are Prudential International Assurance plc S.A. Oddział w Polsce and Prudential Distribution Limited or Prudential Polska Sp. z o.o. and Prudential Distribution Limited respectively, depending on which Prudential entity in Poland a given report concerns.
5. Personal data of the reporting person and other persons indicated in the whistleblowing report are protected in accordance with the rules set forth in internal regulations related to the protection of personal data in force at Prudential. The data of the reporting person and the persons indicated in the report may be processed only to fulfil the obligations arising from a given report (unless such persons' data are processed by Prudential on the basis of other legal grounds, e.g. under employment relationship).
6. Having received a whistleblowing report, Prudential processes personal data to the extent necessary to handle the report or to take any follow-up. Personal data which are not relevant to the processing of the report are not collected and, in the event of accidental collection, are promptly deleted. Such personal data are deleted within 14 days of the finding that they are not relevant.
7. Prudential deletes personal data contained in the whistleblowing reports after the lapse of the period necessary to fulfil Prudential's legal obligations arising from the content of a report and to assert and defend against claims that may arise as a result of the whistleblowing report – for the period resulting from the running of the limitation periods for the allegations. In accordance with applicable laws, personal data processed in connection with the receiving of a report or the taking of follow-up, as well as documents related to this report, are retained by Prudential (M&G) for three years after the end of the calendar year in which the external report was submitted to the public authority competent for the follow-up or in which the follow-up has been completed, or after the completion of the proceedings initiated by these activities. Detailed rules regarding the retention period of personal data in relation to the indicated purposes of processing such data (e.g. AML, terrorist financing or employment relationship) are set forth by Prudential in its Personal Data Retention Procedure.
8. The rules for confidentiality and protection of personal data transmitted under the Speak Out program are contained in the 'Speak Out Guidance Note. Data Protection & Privacy' available via EthicsPoint: <https://secure.ethicspoint.eu/domain/media/pl/gui/105606/privacy.pdf> and in the 'Data Protection and Privacy Information' made available on EthicsPoint before a whistleblowing report is made. In the case of persons who make a report by mail or during a physical meeting, information on the data confidentiality and protection rules is included on Prudential's intranet and delivered personally during the physical meeting or by mail to the address provided in the report.

Chapter 7 – Prudential’s record of reports

1. Prudential keeps a record of internal reports. The record is owned by the Head of the Legal and Compliance Department.
2. The day-to-day operation of the record, in particular the entry and completion of internal reports, is handled by the Speak Out team, using EthicsPoint.
3. Entries in the record of internal reports are made on the basis of an internal report.
4. The record of internal reports includes:
 - a. report number;
 - b. object of the infringement;
 - c. personal data of the whistleblower and the person concerned, necessary to identify those persons;
 - d. whistleblower’s contact address;
 - e. date of making the report;
 - f. information on the follow-up taken;
 - g. date of completion of the case.
5. Personal data and other information in the record of internal reports are retained for three years after the end of the calendar year in which the follow-up has been completed or after the completion of the proceedings initiated by such follow-up.

Chapter 8 – Other obligations related to whistleblower protection

1. Prudential shall provide information about the internal reporting procedure to a person applying for employment under an employment or other legal relationship constituting the basis for performing work, supplying services or holding a position, at the commencement of recruitment or negotiations preceding the conclusion of a contract.
2. The fulfilment of the obligation referred to in Section 1 is the responsibility of the HR Department, which shall implement for this purpose appropriate arrangements to ensure that its fulfilment can be verified.

Chapter 9 – External reports to the Ombudsman and public disclosures

1. The whistleblower or a person intending to make an internal report concerning Prudential may also (irrespective of the internal report procedure) make a report to the Ombudsman or to a competent public authority, i.e. the supreme and central government administration body, local government administration body, local government unit, other state authority or other entity performing public administration tasks by law, which is competent to take follow-up on the areas of law indicated in Chapter 1, Section 1.
2. The whistleblower may make an external report without a prior internal report.

3. In the case of an external report, after its receipt, the Ombudsman or a public authority shall verify the report by establishing whether the report concerns information on a breach and by identifying the public authority competent for the follow-up.
 4. If it is found that a breach has occurred, the Ombudsman or a public authority shall forward the report to the public authority competent for the follow-up, no later than 14 days after the report has been made.
 5. In the situation described in Section 4, the Ombudsman or a public authority shall inform the whistleblower about the forwarding of the external report, indicating the public authority to which the external report has been forwarded and the date of forwarding.
 6. If it is found that no breach has occurred, the Ombudsman or a public authority shall refrain from forwarding the external report and inform the whistleblower that it has refrained from forwarding the external report and shall provide the findings of the preliminary verification of the report.
 7. By refraining from forwarding an external report, the Ombudsman or a public authority may inform the whistleblower that the information covered by the external report is to be handled in accordance with separate regulations, in particular as an object of a civil action, a notice of suspected offence, a complaint to an administrative court, a complaint, an application or a petition, or may be presented to the competent authorities for other consideration. The informing of the whistleblower shall not affect the admissibility of the subsequent legal action, the running of time limits or the content of the decision or the manner of completion of the proceedings, of which the whistleblower is advised.
 8. Detailed information on external reporting to the Ombudsman or a public authority is available on the website of the Ombudsman or of the competent public authority.
 9. The regulations on external reporting to the Ombudsman or a public authority shall enter into force on 25 December 2024 and reports may be made as described in this Chapter from that date.
 10. The whistleblower making a public disclosure shall be protected if he or she makes:
 - a. an internal report and then an external report and the legal entity and then the public authority, within the time limit for feedback set in the internal procedure and then within the time limit for feedback set in the external procedure of the public authority, do not take any appropriate follow-up and do not provide feedback to the whistleblower; or
 - b. immediately an external report and the public authority, within the time limit for providing feedback set in its external procedure, does not take any appropriate follow-up and does not provide feedback to the whistleblower;
- unless the whistleblower has not indicated the contact address to which this information should be sent.
11. The whistleblower making a public disclosure shall also be protected if he or she has reasonable grounds to believe that:
 - a. the breach may constitute an imminent or manifest danger to the public interest, in particular where there is a risk of irreversible damage; or
 - b. external reporting would expose the whistleblower to retaliation; or

- c. where an external report is made, a breach is unlikely to be effectively addressed due to the specific circumstances of the case, such as the possibility of concealing or destroying evidence, the existence of collusion between the public authority and the perpetrator, or the involvement of the public authority in the breach.
12. In assessing whether follow-up is appropriate, account shall be taken in particular of the activities taken to verify the information on a breach, the correctness of the assessment of the information on a breach and the adequacy of the measures taken following the finding of the breach, including, where appropriate, to prevent further breaches, taking into account the gravity of the breach.
 13. The provisions of Sections 10 to 12 do not apply if the information on a breach is provided directly to the press and the Press Law of 26 January 1984 applies.

Chapter 10 – Final provisions and criminal regulations

1. The Procedure was adopted after consultations with the company's trade union organization operating at Prudential/representatives of persons performing work at Prudential, selected in the vote.
2. The Whistleblowing Act provides, among others, for the following offences:
 - a. Obstructing reports – whoever, in order to prevent another person from making a report, prevents or materially obstructs that person from doing so, is liable to a fine, restriction of liberty or imprisonment of up to one year. If the perpetrator uses violence, unlawful threat or deception against another person, he or she is liable to imprisonment for up to three years.
 - b. Taking retaliation against a whistleblower – whoever takes retaliation against a whistleblower, a person assisting in making a report or a person associated with the whistleblower is liable to a fine, restriction of liberty or imprisonment for up to two years. If the perpetrator acts persistently, he or she is liable to imprisonment for up to three years.
 - c. Disclosure of whistleblower's identity – whoever, contrary to the regulations of the Act, discloses the identity of a whistleblower, a person who assists in making a report or a person associated with the whistleblower, is liable to a fine, restriction of liberty or imprisonment for up to one year.
 - d. False reporting – whoever makes a report or public disclosure knowing that a breach has not occurred is liable to a fine, restriction of liberty or imprisonment for up to two years.
3. The Procedure enters into force after 7 days from the date of its announcement to the persons performing work in Prudential.