

Whistleblowing Procedure at mBank S.A.

Article 1 **Introduction**

1. At mBank we do not tolerate breaches of law, regulatory requirements, internal regulations and principles or any criminal activity. This is why mBank supports and protects reporting persons (“whistleblowers”) in accordance with the rules set out in this procedure.
2. The purpose of this procedure is to prevent wrongdoing and encourage whistleblowers to report breaches of law, ethical standards and internal regulations adopted at mBank S.A.

Article 2 **Definitions**

1. **Bank** – mBank S.A. with its registered office in Warsaw, ul. Prosta 18, 00-850 Warszawa, registered with the District Court for the Capital City of Warsaw, 13th Commercial Division of the National Court Register, under KRS no. 0000025237, holder of tax identification number NIP 526-021-50-88.
2. **DC** – the Compliance Department.
3. **Follow-up** – an action taken at the bank to assess the accuracy of the allegations made in the report and to address the breach reported, in particular an investigation launched in accordance with this procedure.
4. **Retaliation** – any direct or indirect act or omission which occurs in a work-related context, is prompted by reporting, affects or may affect the rights of the whistleblower or causes or may cause unjustified detriment to the whistleblower, including unfounded initiation of proceedings against the whistleblower.
5. **Feedback** – information on the action envisaged or taken as follow-up and on the grounds for such follow-up provided to the whistleblower.
6. **Work-related context** – past, current or future work activities performed under an employment relationship or any other legal relationship forming the basis for the provision of work or services, where information of a breach of law has been obtained and retaliation may be suffered.
7. **mSignal** – a web-based app enabling its users to report breaches online, either by name or anonymously, accessible 24 hours a day and seven days a week.
8. **Breach** – an act or omission contrary to law, internal regulations and ethical standards of the bank or that aims to circumvent them.
9. **Breach of law** – an act or omission that is contrary to law or aims to circumvent it.

10. **Public authority** – supreme 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 law.
11. **Close person** – wife/husband; ascendant/descendant; other person related by blood or by marriage; cohabitating partner; person related by adoption, custody or guardianship; person who lives in the same household.
12. **Person concerned** – a person who is referred to in the report as a person to whom the breach is attributed or with whom that person is associated.
13. **Facilitator** – a natural person who assists the whistleblower in the reporting process in a work-related context and whose assistance should be confidential.
14. **Associated person** – a natural person who can suffer retaliation, including a colleague or an immediate family member of the whistleblower within the meaning of Article 115 (11) of the Penal Code Act of 6 June 1997 (Journal of Laws of 2024, item 17).
15. **GDPR** – Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).
16. **Whistleblower** – a natural person who reports information on breaches acquired in the context of their work-related activities.
17. **Act** – Act of 14 June 2024 on the Protection of Whistleblowers.
18. **Anonymous report** – the provision of information on breaches of law by a person who did not reveal their identity or provide their contact details.
19. **Internal report** – the provision of information on breaches to the bank.
20. **External report** – the provision of information on breaches of law to the Commissioner for Human Rights or a public authority.

Article 3

General information

1. This procedure outlines steps to be taken to report breaches at mBank S.A. as well as rules for verifying reports, taking remedial actions and protecting whistleblowers.
2. This procedure applies to reported breaches of law in the scope defined in the act and in internal regulations and ethical standards applicable at the bank.
3. This procedure does not change the rules for operation of other channels used to report other issues, e.g. claims and complaints from clients. This procedure does not apply to cases of wrongdoing identified as a result of internal control, to solving complaints from clients and to reported standard cases of external fraud, e.g. card fraud, credit scams or phishing, which can be reported by clients and other people using other channels made available at the bank.
4. The adopted solutions ensure that any reported case is investigated by an independent unit and that the whistleblower is protected. An employee who reports suspected wrongdoing must be protected against any forms of retaliation, discrimination or unfair treatment, even if their information is not confirmed during an investigation. Any retaliation towards whistleblowers is prohibited (**principle of protection of whistleblowers**).
5. The channels dedicated to making internal reports made available by the bank guarantee the protection of the identity of the whistleblower and third parties named in their report and, where necessary, they guarantee anonymity. Any information furnished in a report and

collected during an investigation is subject to data protection regulations and should be treated as confidential (**principle of confidentiality**).

6. The whistleblower should not furnish information which they knew to be false at the time of reporting (**principle of protection against defamation**).

Article 4

Methods for reporting breaches

1. Whistleblowers can report breaches using the following communication channels:
 - **electronically** – via the mSygnał app available on the bank’s website ([mSygnał](#)).
 - **by mail** (in writing) – to the following address: mBank, ul. Prosta 18, 00-850 Warsaw, Compliance Department, WZN with an annotation “breach report, mBank – confidential”.
2. Reports can be made by name or anonymously. Where the identity of the reporting person is revealed based on the contents of their report or actions taken, it is subject to protection provided for in this procedure.
3. Reports of violations considered under this procedure include all reports, whether named or anonymous, made by individuals, who:
 - a) may be members of the bank’s governing bodies, employees, persons whose employment has not yet commenced, as well as those whose employment has already ended, job candidates, contractors (including self-employed individuals), subcontractors, suppliers, temporary workers, as well as interns and volunteers, and
 - b) containing information, including reasonable suspicion of an actual or potential violation, where the reporting person has grounds to believe that the information was true at the time of reporting and that it falls within the scope of the reportable categories defined below:
 - corruption,
 - money laundering / terrorism financing / embargoes and sanctions,
 - fraud, including tax offences,
 - balance sheet manipulation,
 - theft,
 - market abuse / insider trading,
 - embezzlement / breach of trust,
 - environmental risk and violation,
 - breach of regulatory requirements and laws (in particular the ones referred to in the act) and internal regulations of the bank,
 - wrongdoing in employee relations,
 - breach of ethical principles, including human rights.
 - c) submitted via the designated channels specified in the procedure,
 - d) concerning information acquired in a work-related context.

4. We recommend including the following information in the report, to the best knowledge of the whistleblower:
 - a) where the breach happened;
 - b) who was involved;
 - c) when the breach happened / how long it lasts;
 - d) detailed description of the breach reported;
 - e) relation between the whistleblower and the bank;
 - f) estimated amount of potential losses;
 - g) any evidence and information that can prove useful in investigating the breach.
5. We recommend providing contact details. The provision of a contact address for paper correspondence does not apply to anonymous reports. When making a report via mSignal, the whistleblower can set up a contact mailbox.

Article 5

Procedure for dealing with internal reports

1. Direct access to all registered reports of breaches is given to the designated member of the management board, the director of the Compliance Department (DC) and to authorised DC employees holding written authorization to handle and analyze reported violations.
2. DC is the unit authorised to accept and verify internal reports, take actions as follow-up and communicate with whistleblowers.
3. Depending on the scope of responsibility and the required expert knowledge, reports can be dealt with by authorised employees of the bank's units other than DC, who deal with reports by categories and in accordance with their competences and internal regulations of the bank, in keeping with the rules and time limits laid down in this procedure.
4. At any stage of the process a report cannot be dealt with by the employee concerned or the employee whose impartiality or independence raises reasonable doubts, especially where they are a person close to the whistleblower or the person concerned.
5. DC is responsible for coordinating and monitoring whether other organisational units deal with reports in a timely manner.
6. The authorised employee who deals with a report analyses whether the report involves a breach within the meaning of this procedure and whether it contains sufficient information enabling a further investigation. If the outcome of this analysis is positive, an investigation is launched to verify the concern reported. If the outcome of this analysis is negative, the report is closed as unconfirmed.
7. Within seven days from receiving a report, the authorised employee acknowledges receipt of the report to the whistleblower and notifies them that an investigation has been launched or that their report was closed (stating a reason) or classified as a complaint; the authorised employee may also request the whistleblower to provide additional information. The employee contacts the whistleblower in the manner indicated in their report.
8. When launching investigations and taking actions as follow-up, authorised employees exercise due diligence in order to determine the factual circumstances and clarify all doubts about the concern raised in the report. They collect evidence enabling them to deal with reports in an objective, diligent, and unbiased manner.

9. The authorised employee notifies the whistleblower that an investigation has been completed not later than within three months from acknowledging receipt of an internal report.
10. The provisions of Article 5 (7) and (9) do not apply if the whistleblower did not set up a mailbox in mSygnał or provide a contact address to which feedback should be given.

Article 6

External reports

1. Whistleblowers have the right to make external reports to the Commissioner for Human Rights, public authorities, and where appropriate, to institutions, bodies or organisational units of the European Union, in accordance with the relevant laws. Detailed information on external reports can be found on the website of the Commissioner for Human Rights: <https://bip.brpo.gov.pl/pl/content/zlozenie-wniosku-do-rzecznika-praw-obywatelskich>.
2. Whistleblowers can make an external report without first making an internal report. However, the bank encourages the reporting of breaches through internal channels in accordance with this procedure so as to be able to effectively respond to cases of wrongdoing and prevent them in the future.
3. The making of an external report is without prejudice to the whistleblower's right to protection against retaliation.
4. Detailed rules for making and dealing with external reports and for protecting whistleblowers are laid down in the act.

Article 7

Protection of whistleblowers

1. The bank enables whistleblowers to report breaches in a manner protecting them against retaliation. Any retaliation or attempts or threats of retaliation against whistleblowers are prohibited.
2. The protection against retaliation covers whistleblowers, facilitators and persons associated with whistleblowers. The prohibition of retaliation and measures of protection also apply to legal persons and other organisational units that help whistleblowers or are associated with them, in particular where such a legal person or organisational unit is owned by or employs the whistleblower.
3. Whistleblowers are subject to protection from the time of making a report on condition that they had reasonable grounds to believe that the information on a breach of law or ethical standards / internal regulations of the bank reported by them was true at the time of reporting.
4. The prohibition of retaliation also applies where an investigation shows that a breach reported in good faith has not been confirmed in the end.
5. A whistleblower who suffered retaliation should immediately notify a bank employee about it through communication channels dedicated to internal reports. The notification is dealt with in accordance with the procedure for internal reports.
6. A whistleblower who suffered retaliation has the right to compensation not lower than the average monthly salary in the national economy in the previous year announced for pension

purposes in the Official Journal of the Republic of Poland “Polish Monitor” by the President of Statistics Poland, or the right to reparation.

7. A person who suffered a detriment as a result of false information knowingly reported by a whistleblower has the right to compensation or reparation for infringement of personal rights from the whistleblower.
8. Persons who report information on breaches do not incur liability of any kind, including disciplinary liability or liability for damages for infringement of the rights of others or of obligations laid down by law, provided that they had reasonable grounds to believe that the reporting of such information was necessary for revealing a breach of law.

Article 8

Confidentiality

1. The bank ensures that the adopted procedure for dealing with internal reports and the personal data processing related to it prevent access to the reported information by unauthorised persons and guarantee that the identity of whistleblowers, persons concerned and third parties named in the reports is protected. The protection of confidentiality also applies to information from which the identity of such persons may be directly or indirectly deduced.
2. Any information collected in relation to internal reports is subject to protection and can be accessed only by persons authorised to accept and analyse internal reports, take actions as follow-up and process the personal data of whistleblowers, persons concerned and third parties named in reports of breaches. The above does not apply in cases where such information must be disclosed under generally applicable laws.
3. The authorised persons who deal with internal reports are obliged to keep confidential the information and personal data obtained in the process of accepting, analysing and following up on reports also after the termination of the employment relationship or any other legal relationship forming the basis for performing these tasks.
4. Where a report is made anonymously, any actions taken to reveal the identity of the whistleblower are prohibited.

Article 9

Personal data processing

1. Any personal data obtained in connection with internal reports of breaches in accordance with this procedure is processed in line with the GDPR and other generally applicable laws and internal regulations of the bank.
2. Upon receiving a report, the bank processes personal data in the scope necessary to accept the report or take actions as follow-up if necessary. Personal data not relevant for the handling of a report is not collected or, if accidentally collected, is deleted without undue delay. Such personal data is deleted within 14 days from the moment it is found to be not relevant for a given case.
3. The personal data of a whistleblower making it possible to reveal their identity is not disclosed to unauthorised persons, unless upon the explicit consent of the whistleblower. The above does not apply where such a disclosure is a necessary and proportionate obligation under law in the context of investigations by public authorities or pre-trial and judicial proceedings by courts.

4. Personal data processed in connection with internal reports or follow-up and documents connected with such internal reports are stored for three years after the end of the calendar year in which the actions taken as follow-up were completed or after the end of judicial proceedings initiated by such follow-up.
5. Personal data and other information are stored in the register of internal reports for three years after the end of the calendar year in which the actions taken as follow-up were completed or after the end of proceedings initiated by those activities, unless the applicable laws set out different time limits for storing and deleting information.

Article 10

Final provisions

1. The bank regularly reviews the rules set out in this procedure (at least once every 12 months) and updates them if needed.
2. The procedure is published on the bank's website.