Policy for the Protection of Persons who send signals for breaches in UBB ('Whistleblowing Policy')

Introduction

UBB expects its employees and contractual partners to follow the terms of their contracts in a loyal, co-operative manner and in a good faith. This general duty of care also encompasses the basic moral obligation to send a signal if they've any reasonable suspicion that these subjects might commit a Breach. For this reason, UBB wants to create and foster a corporate culture marked by honesty and openness, where any persons have the opportunity to report potential breaches that may cause financial or reputational loss in the earliest possible stages without fear for any reprisals and they are assured that they will receive fair treatment and their concerns will be investigated properly.

UBB's internal controls and operating procedures are intended to prevent and discourage all Breaches; however, even the best system of controls can't provide absolute safeguards against irregularities. In this way, whistleblowing is one of the effective techniques used for prevention and detection of breaches. It mobilizes the employees and contractual partners to communicate their suspicions and reasonable doubts to the management about malicious activities without fear and prejudice.

This Policy is also based on the requirements expressed in the latest European legislation (*2019/1937 - EU Directive on protection of persons who report breaches of Union law*), international standards and principles of corporate governance.

Objectives

This Policy is aimed to provide a Framework for Whistleblowers to voice their concerns to the Local Ant-Fraud Unit about any suspicious or undesired events / activities, which are against the law, rules of UBB or may have an adverse impact on the business or goodwill of UBB.

The intended objectives of this Policy is that UBB becomes fully compliant with the latest EU legislation in this area and along this:

- To support a culture of openness, accountability and integrity;
- To provide environment to all persons to report, without any fear of retaliation, where they know or suspect a Breach of any current or former employees or contractual partners which may cause financial or reputational risk to UBB;
- To create awareness especially amongst employees, stakeholders and contractual partners regarding the whistleblowing function;
- To enable Management to be informed at an early stage about breaches and take appropriate actions;
- To provide assurance to the whistleblowers about secrecy and protection of their legitimate personal interests upon report of suspicious activities;
- To assure that all reports under this Policy would remain strictly confidential and that UBB is committed to address reports (if any) that alleges acts of retaliation against the whistleblowers.

Definitions

Breach: means act or omission – in work-related context - that violate duties imposed by law, regulations, professional standards, internal policies, rules and procedures of UBB or defeat their object or purpose.

Whistleblowing: is a reporting (either internal or external) to the Local Anti-Fraud Unit of UBB (or as the case may be a Supervisor) by any person to expose and/or inform on a Breach.

Reporting person ('*Whistleblower*'): is any person or legal entity, who reports the breach to the Local Anti-Fraud Unit of UBB. The role of a whistleblower would remain to the extent of reporting only, he

will neither be considered an investigator nor will he determine the appropriate corrective action that may be required under the given situation.

Local Anti-Fraud Unit: is an operationally independent Unit established within the Compliance function for receiving and monitoring concerns raised by the Whistleblower under this Policy.

Good Faith: is the sincere belief of the Whistleblower that the content of the report on a Breach is true and made in the interest of UBB, without consideration of personal benefit and not based on personal grudges. However, it is not necessary that a report made in good faith, proves to be true.

Retaliation: means any act of discrimination, revenge or harassment directly or indirectly taken against a whistleblower, by any person, for reporting the Breach.

Protection: means all reasonable steps taken by UBB to ensure confidentiality of the whistleblower's name as well as measures enforced to protect whistleblowers from retaliation and financial losses.

Work-related context: means current or past work or contractual activities within UBB through which, irrespective of the nature of those activities, persons acquire information on breaches and within which those persons could suffer retaliation if they report such information.

Scope

Personal Scope

This Policy applies to **whistleblowers who acquired information on breaches in a work-related context** including, at least, the following:

- persons having the status of employees or self-employed status;
- shareholders and persons belonging to the administrative, management or supervisory body, including non-executive members, as well as volunteers and paid or unpaid trainees;
- any persons working under the supervision and direction of contractors, subcontractors and suppliers.

This Policy also applies to whistleblowers where information on breaches acquired in a work-based relationship which has ended or persons whose work-based relationship is yet to begin in cases where information acquired during the recruitment process or other pre-contractual negotiations.

The measures for the protection of whistleblowers also apply, where relevant, to:

- third persons who are connected with the whistleblower and who could suffer retaliation in a work-related context, such as colleagues or relatives;
    - legal entities that the whistleblower owns, works for or are otherwise connected with in work-related context;

By signing the employment contract with UBB, all newly appointed employees confirm that they are familiar with the contents and regulations of the internal Bank rules and procedures, including the present Rules for protection of whistleblowers in UBB and will strictly comply with all their requirements. A copy of the employment contract, signed by both parties is kept by the Human Resources Management Directorate into the newcomer's personal file.

Material Scope

This Policy lays down common **minimum standards for the protection of whistleblowers** reporting breaches of law or UBB's policies, rules and procedures. Examples of such Breaches include, but are not limited to, fraud, money laundering, bribery and corruption, insider trading and other misconducts, immoral or unethical behavior or malicious practices, negligence of duty (especially matters that jeopardize the credibility and reputation of UBB as a trusted financial services provider).

Out of Scope

This Policy is not designed to question financial or business decisions taken by UBB nor should it be used to reconsider any other matters which have already been addressed under other procedures, rules or regulations of UBB.

Where specific internal Policies, Rules and/or Procedures on the handling of Breaches are provided - those will apply (e.g. Anti-Money Laundering, Fraud).

Principle 1: Protection of Whistleblowers (General Conditions)

Whistleblowers will qualify for protection under this Policy provided that:

- they had reasonable grounds to believe that the information on Breaches reported was true at the time of reporting and that such information fell within the scope of this Policy and
- they reported either internally or externally in accordance with this Policy

This Policy does not affect the duty to accept and follow up on anonymous reports of breaches however anonymous reporting is not preferred and encouraged. Whistleblowers who reported Breaches anonymously, but who are subsequently identified and suffer retaliation, will qualify for the protection provided for under Principle 2, provided that they meet the defined conditions. Persons internally reporting breaches will qualify for protection under the same conditions as persons reporting externally.

Principle 2: Protective Measures

UBB takes the necessary measures to **prohibit any form of retaliation** against whistleblowers (including threats and attempts of retaliation) particularly – but not limited to - in the form of:

- suspension, demotion or withholding of promotion and withholding of training;
- negative performance assessment or employment reference;
- imposition or administering of any disciplinary measure, reprimand or other penalty;
- coercion, intimidation, harassment discrimination or unfair treatment;
- failure to convert a temporary employment contract into a permanent one, where the worker had legitimate expectations that he or she would be offered permanent employment;
- failure to renew, or early termination of, a temporary employment contract;
- harm, including to the person's reputation (particularly in social media) or financial loss, including loss of business and loss of income;
- blacklisting on the basis of a sector or industry-wide informal or formal agreement, which may cause that the person will not find employment in the sector or industry;
- early termination or cancellation of a contract for goods or services.

UBB ensures that whistleblowers have access, as appropriate, to support measures, in particular comprehensive and independent information and advice, which is easily accessible and free of charge, on procedures available, on protection against retaliation, and on the rights of the person concerned.

UBB may also provide to the whistleblowers the financial reward or assistance and other support measures, including psychological support, according to the internal procedures.

If the Whistleblower feels that, at his/her place of posting, he/she might be subjected to victimization or harassment by the alleged officials after „blowing the whistle“, the management may consider transferring him/her to another suitable place on his/her request. However, this assurance is not extended in cases where it is proved that he/she raised the matters to settle personal grudges or grievances or where he/she has been habitually involved in complaining petty issues.

UBB draws appropriate consequences (e.g. disciplinary action, civil or criminal complaint) according to the internal procedures towards any natural or legal persons that:

- hinder or attempt to hinder reporting;
- retaliate against whistleblowers;
- bring vexatious proceedings against whistleblowers;
- breach the duty of maintaining the confidentiality of the identity of whistleblowers.

Employees of UBB must refrain from abusing the reporting procedure and thereby deliberately harming another employee. Where subsequent investigation reveals that it can be proven that the accusations were made with malicious or slanderous intent, appropriate sanctions may apply (these may extend to dismissal for cause, where justified in accordance with the Bank's rules and applicable legislation).

Principle 3: Protection of Persons concerned

UBB guarantees that persons concerned are protected in a way to keep a balance between the interests and rights of the various parties affected (incl. the right of UBB to investigate the breach).

UBB ensures that persons concerned fully enjoy their fundamental rights such as fair treatment, rights of defense (incl. the right to be heard and the right to access their file) as well as the presumption of innocence. The Local Anti-Fraud Unit in Compliance Directorate ensures that the identity of such a person is protected for as long as investigations triggered by the report are ongoing. The protection of the identity of whistleblowers also applies to the protection of the identity of the persons concerned.

The persons concerned are entitled to information (the name of the data processing entity, what is the basis of suspicion, who the recipients of this information are) and is also entitled to access, correct and remove information related to himself/herself that is incomplete or incorrect, according to the personal data protection rules.

These rights do not entitle the persons concerned to make copies of documents or other material related to the investigation, the findings and the measures taken.

The exercise of these rights may be postponed to avoid hampering the investigation or restricted in order to safeguard the rights of others involved. The decision on whether or not these rights should be restricted will be made on a case-by-case basis.

Principle 4: Reporting Channels and Procedure

Information on Breaches can be reported through various reporting channels (either internal or external) according to the procedures provided in this Policy. UBB encourages reporting via internal reporting channels before reporting through external reporting channels, where the breach can be addressed effectively internally and where whistleblowers consider that there is no risk of retaliation.

UBB establishes for the purpose of whistleblowing a dedicated email inbox: **concerns@ubb.bg**. This reporting channel and procedure enable persons defined under the scope of this policy to report information on breaches.

Reporting channels are to be operated internally by the Local Anti- Fraud Unit designated for that purpose.

The whistleblowing procedure for reporting breaches and for follow-up includes at least:

- channel for receiving the reports designed, established and operated in a secure manner that ensures that the confidentiality of the whistleblower's identity and any third party mentioned in the report is protected, and prevents access by non-authorized staff members;
- channel for receiving the reports enable the durable storage of information to allow further investigations to be carried out;
- acknowledgment of receipt of the report to the whistleblower within 7 days of that receipt;
- the dedicated impartial Anti-Fraud Unit is competent for following-up on the reports, the same Unit receives the reports and maintains communication with the whistleblower and, if necessary, asks for further information from and provides feedback to the whistleblower;
- diligent follow-up by the Local Anti-Fraud Unit;
- a timeframe to provide feedback, not exceeding 3 months from the acknowledgment of receipt or;

- communicate to the whistleblower the final outcome of investigations triggered by the report;
- transmit in due time the information contained in the report to competent authorities for further investigation according to the relevant legislation.

The reporting channel enabling written or oral reporting (or both) is also designed, established and operated in a secure manner that ensures that the confidentiality of the whistleblower's identity and any third party mentioned in the report is protected, and prevents access by non-authorized staff members. Oral reporting is possible by telephone or through other voice messaging systems, and, upon request by the whistleblower, through a physical meeting with dedicated person within a reasonable timeframe.

Dedicated person, after having duly assessed the matter, can decide that a reported breach is clearly minor and does not require further follow-up, other than closure of the procedure. In such a case, the competent person notifies the whistleblower of the decision and the reasons therefor. The same approach can be followed in case of repetitive reports which do not contain any meaningful new information on breaches compared to a past report in respect of which the relevant procedures were concluded, unless new circumstances justify a different follow-up.

Dedicated person who has received a report but does not have the competence to address the reported breach transmits it to the Local Anti-Fraud Unit in Compliance Directorate, within a reasonable time, in a secure manner, which then should make a decision in regards to taking the necessary follow-up actions .

If a report on breach is received through channels other than the reporting channel or by staff members other than those responsible for handling reports, the staff members who receive it are prohibited from disclosing any information that might identify the whistleblower or the person concerned and they promptly forward the report without modification to Compliance Directorate with this e-mail: concerns@ubb.bg for further decision.

UBB and its local entities designate staff members responsible for handling reports, particularly for:

- receiving and following up on reports on the breach;
- conducting investigation about the breach;
- maintaining contact with the whistleblower for the purpose of providing feedback and requesting further information where necessary.

Such staff members receive specific training for the purposes of handling reports on breaches.

UBB publishes on its website in a separate, easily identifiable and accessible section at least the following information:

- the conditions for qualifying for protection under this Policy;
- the contact details for the external reporting channels, particularly the electronic and postal addresses, the phone numbers for such channels, indicating whether the phone conversations are recorded;
- the procedures applicable to the reporting of Breaches, including the manner in which the competent person may request the whistleblower to clarify the information reported or to provide additional information, the timeframe for providing feedback and the type and content of such feedback;
- the confidentiality regime applicable to reports, especially the information in relation to the processing of personal data;
- the nature of the follow-up to be given to reports;
- the procedures for protection against retaliation and the availability of confidential advice for persons contemplating reporting.

Principle 5: Confidentiality, Personal Data Protection and Records Keeping of the Reports

Confidentiality

The identity of the whistleblower can't be disclosed to anyone beyond the authorized staff members competent to receive or handle the reports, without the explicit consent of that person. This also applies to any other information from which the identity of the whistleblower can be deduced.

The identity of the whistleblower and any other information referred to such a person may be disclosed

only where this is a necessary and proportionate obligation imposed by law in the context of investigations by national authorities, including with a view to safeguarding the rights of the person concerned.

Personal Data Protection

Any processing of personal data carried out pursuant to this Policy, including the exchange or transmission of personal data, will be carried out in accordance with EU and national law and UBB Policies. Personal data which are manifestly not relevant for the handling of a specific report will not be collected or, if accidentally collected, shall be deleted without undue delay.

Records Keeping of the Reports

UBB keeps records of every report received, in compliance with the confidentiality requirements. Reports will be stored for no longer than it is necessary and proportionate in order to comply with the requirements imposed by this Policy.

Where a **recorded telephone line** or another recorded voice messaging system is used for reporting, UBB has the right to document the oral reporting:

- by making a recording of the conversation in a durable and retrievable form; or
- through a complete and accurate transcript of the conversation prepared by the staff members responsible for handling the report. UBB offers the whistleblower the opportunity to check, rectify and agree the transcript of the call by signing it.

Where an **unrecorded telephone line** or another unrecorded voice messaging system is used for reporting, UBB has the right to document the oral reporting in the form of accurate minutes of the conversation written by the staff member responsible for handling the report. UBB offers the whistleblower the opportunity to check, rectify and agree the minutes of the conversation by signing them.

Where a person requests a **meeting** with the competent staff members for reporting purposes, UBB ensures, subject to the consent of the whistleblower, that complete and accurate records of the meeting are kept and have the right to document the meeting:

- by making a recording of the conversation in a durable and retrievable form; or
- through accurate meeting minutes prepared by the staff members responsible for handling the report. UBB offers the whistleblower the opportunity to check, rectify and agree the meeting minutes by signing them.

Principle 6: Designated Units and Persons

Compliance (as a Central Point)

Due to its independency, Compliance Directorate will serve as a central point where all whistleblowing reports and cases will be received, monitored and stored. All other Units/Persons are obliged to transmit all incoming reports on Breaches to the Compliance Directorate without any delay.

Group Compliance – Ethics & Fraud Unit – is responsible for:

- Receiving, monitoring and storing all Whistleblowing cases related to KBC Group level matters;
- Handling all Whistleblowing cases except those where different Unit within/out of Group Compliance is competent (e.g. Anti-Money Laundering);
- Monitoring all Whistleblowing cases related to local entities of KBC Group (local entities are obliged to notify about such cases without any delay).

In case of the breach where Group Compliance – Ethics & Fraud Unit is not competent, then this Unit will send the report on Breach to competent Unit (either on the Group or local level) and will notify the Whistleblower. Competent Unit are then responsible for further steps described in this Policy (communication with whistleblower, taking protective measures, follow up and feedback etc.).

Local Compliance – Ethics & Fraud Unit – is responsible for:

- Receiving, monitoring and storing all whistleblowing cases related to local entity matters;
- Handling all Whistleblowing cases except those where different Unit within/out of Compliance's competence (e.g. Anti-Money Laundering, Consumer Protection, Fraud etc.);
- Notifying all Whistleblowing cases related to local entity to Group Compliance – Ethics & Fraud Unit (via dedicated email box **concerns@ubb.bg**).

In case of the breach where Local Compliance – Ethics & Fraud Unit is not competent, then this Unit will send the report on the Breach to competent Unit (either on the Group or local level) and will notify the whistleblower. The local Anti-Fraud Unit are then responsible for further steps described in this Policy (communication with whistleblower, taking protective measures, follow up and feedback etc.).

Special Investigations Unit in Internal Audit Directorate

Based on local Polices and organizational structure, the investigation of breaches (e.g. AML, fraud) can be handled by the Special Investigations Unit, Internal Audit Directorate. Such Unit is then – inter alia - responsible for:

- Communication with the whistleblower, keeping the whistleblower informed about the progress of the investigation, unless this might harm the whistleblower or hinder the investigation;
    - Conducting investigations in order to determine whether the breach happened. If necessary, any third party mentioned in the report is protected;
- Reporting to management (Local and/or Group Compliance, Executive Committee, Risk and Compliance Committee, Management Board or another Supervisory Body);
- Ensuring that the identity of the whistleblower is kept confidential, unless the whistleblower consents to having his/her identity revealed or it is required by law (e.g. by court in criminal matters). This does not exclude that the whistleblower, like all other people involved, can be interviewed with regard to the breach;
- Take necessary protective measures in relation to whistleblower or other persons affected;
- Reporting facts that must be reported to official bodies. Where appropriate, a complaint can be send to the competent authorities;
- Safeguarding the rights of the persons concerned.

Investigators are subject to strict ethical rules, particularly with regard to observing due discretion and displaying the necessary reserve. Every investigation on the breach is conducted according to UBB's policies and professional standards.

Every employee is required and obliged to co-operate in good faith with the Unit handling the signal on breach.

In exceptional cases, Group Compliance as well as local Compliance can decide that the investigation will be carried out by them.

Principle 7: Monitoring and Reporting

The results of investigations of breaches will be reported in accordance with the standard reporting lines for specific types of breaches. This internal reporting does not affect the duty to report statistics on whistleblowing Cases or status of implementation of legislation in this area to relevant authorities (e.g. European Central Bank).

Group Compliance is responsible for monitoring the functioning of this Policy in all entities of KBC Group. In this regard, the Compliance and Risk Officer of UBB will report on the status of the implementation and functioning of the Policy in periodic and annual reports to Group Compliance and to local Executive Committees and (Audit), Risk & Compliance Committees.

The Group Compliance Officer will submit an annual status report on the implementation of this Policy to Group Executive Committee and Group Risk & Compliance Committee.

Principle 8: Implementation and Communication

The Compliance Directorate in UBB is responsible for transposition, introduction and implementation of this Policy on a local level within 12 months once this Policy is in place and for drawing up reliable, simple and transparent procedures (including contact points and information, also covered in the communication/awareness campaign within every local entity) to guarantee observance of this Policy.

UBB's Compliance Directorate must launch an information campaign for the dissemination of this Policy. The Policy must be published (both internally and externally) and included in training courses.

Amendments

The principles set out in this Policy are minimum standards, applicable to UBB.

Compliancy with this Policy is mandatory and applies with immediate effect to UBB.

UBB will ensure that the rights provided for under this Policy cannot be waived or limited by any agreement, policy, form or condition of employment.

The implementation of this Policy will under no circumstances constitute grounds for a reduction in the level of protection already afforded by UBB in the areas covered by this Policy. Should local law be more protective, it will prevail.

Any questions regarding the Policy and its principles can be directed to the Compliance Ethics & Fraud Unit, UBB (*e-mail*: concerns@ubb.bg).

Transitional and final provisions

This Policy for the Protection of Persons who send signals for breaches in UBB ('Whistleblowing Policy') has been approved with a decision of the Management Board of UBB, pursuant to Minutes № 17 dated 12.04.2021, and shall enter into force at the date of its approval.

Upon its entry into force, the Policy for the Protection of Persons who send signals for breaches in UBB ('Whistleblowing Policy') repeals the current Rules for the Protection of Whistleblowers in UBB, approved by an Executive Director of UBB AD on 07.11.2017 (DZ No. 127682_17/ 07.11.2017), in force as of the date of entry in the Commercial Register of the merger of CIBANK JSC with UBB AD, amended and supplemented by decision of the Management Board of UBB, pursuant to Minutes No 38 dated 22 July 2019.