Information on

Internal whistlebowing reporting procedure

KRUK

General provisions

Internal whistleblowing reporting procedure (hereinafter: the Procedure) sets out the principles for reporting, (also anonymously) and managing reports of breaches of the law or aimed at circumventing the law, internal regulations and ethical standards, as well as taking follow-up actions (the whistleblowing process), including the principles for protecting persons who make such reports in good faith ('whistleblowers').

The provisions of the Procedure are based on applicable laws and fulfill the requirements arising in particular from:

1. Article 25(1) and (2) of the Act of June 14, 2024 on the protection of whistleblowers (hereinafter: the Act);
2. Article 97d of the Act of July 29, 2005 on public offerings and the conditions for introducing financial instruments to an organized trading system and on public companies (hereinafter: the Public Offering Act);
3. Article 53 of the Act of March 1, 2018 on counteracting money laundering and financing of terrorism.

The Procedure is a joint internal reporting procedure for the KRUK Group companies, i.e. KRUK S.A. and Kancelaria Prawna RAVEN P. Krupa Sp. k. (hereinafter: the Companies or the Company individually).

The whistleblowing process is an element of the risk management system that supports safe and stable management and serves to ensure that irregularities are detected effectively and that appropriate action is taken to address them and mitigate risk at all organisational levels within the KRUK Group Companies.

Main objectives of the procedure

The purpose of the Procedure is in particular to set out:
- the principles for reporting breaches in good faith (also anonymously);
- the principles for responding to reported breaches;
- the responsibilities of the authorised persons involved in the whistleblowing process and the principles for follow-up;
- principles for the protection of whistleblowers;
- opportunities for external reporting.

Reported breaches are analysed with the utmost care, in an atmosphere free of reprisals and in accordance with the values of the KRUK Group, in order to take adequate measures to eliminate the occurrence of similar breaches in the future, as well as to mitigate risk at all organisational levels within the KRUK Group Companies.

Based on the Procedure, reports of breaches originating from Business Partners and Suppliers cooperating with the Companies are also handled.

What is a breach

A breach is any act or omission which is or may be contrary to the law (or intended to circumvent the law), internal regulations or ethical standards applicable to the Company.

On the basis of the Procedure, a breach may be reported in particular with regard to:

- anti-corruption
- financial services, products and markets
- Anti-Money Laundering and Countering the Financing of Terrorism;

- product safety and compliance
- transport safety
- environmental protection
- consumer protection
- protection of privacy and personal data
- security of networks and information and communication systems;
- the commission of fraud, theft, data falsification or other accounting and financial irregularities;
- the occurrence of conflicts of interest within the Company and during the procurement process, including maintaining impartiality in the selection of the Business Partner/Supplier;
- human rights
- ethical standards;
- diversity policy, including unequal treatment based on gender, age, disability, health, race, nationality, religion, belief, sexual orientation, family status or lifestyle;
- internal procedures for sanction risk management.

Who can report a breach

A reporter can be a natural person who, in a work-related context, has obtained knowledge or information about a breach ('Whistleblower').

A work-related context is to be understood as: past, present or future work-related activities based on an employment relationship or other legal relationship that forms the basis for the provision of work or services in or for the Company, in which knowledge of the breach has been obtained and the possibility of experiencing retaliation exists.

A whistleblower may be, in particular: an employee; a temporary employee; a person providing work on a basis other than employment relationship, including on the basis of a civil law contract; an entrepreneur ('Business Partner'/'Supplier'); a proxy; a shareholder or partner; a member of a body of a legal person or an organisational unit without legal personality; a person providing work under the supervision and management of a contractor, subcontractor or supplier; an intern or trainee; a person applying for a job with the Company ('job candidate') who reports a breach to the Company in the context of employment (during or before its start) or other legal relationship, including on the basis of a civil law contract.

How to report a breach

A whistleblower may report a breach, also anonymously:
1) electronically via the whistleblowing system, which ensures the confidentiality of the information and data provided in the report, available at the following link: https://whistlekruksa.vco.ey.com/,
2) on paper, by addressing it directly (as "confidential") to the President of the KRUK S.A. Management Board / General Partner of Kancelaria Prawna Raven P. Krupa Sp.k. or Group Head of Compliance Area / Head of KRUK S.A. Compliance Unit,
3) by e-mail to authorised members of the KRUK S.A. Supervisory Board at whistleblowing.rn@kruksa.pl - if the infringement concerns a KRUK S.A. Management Board member.

All reports, whether made anonymously or with providing personal data, will be treated as confidential and will be investigated with due diligence in accordance with the Companies' procedures.

What a breach report should contain

The report should contain a clear and complete description of the breach, including at least:
1. the date and place of the breach or the date and place of obtaining information about the breach, 2. a description of the breach or the circumstances creating the possibility of a breach,

3. indication of the person to whom the report relates, who contributed directly or indirectly to the occurrence of the breach,
4. indication of a person, who has been injured by the breach (if applicable),
5. indication of possible witnesses to the breach,
6. an indication of evidence and additional information available to the Whistleblower that may be helpful in the process of handling the report,
7. indication of the preferred method of return contact, if the report has not been sent via the whistleblowing system.

Roles and responsibilities in the whistleblowing process

KRUK S.A. Compliance Unit is an impartial and independent organisational unit responsible for receiving and verifying reports of breaches at the Companies through the whistleblowing system and taking followup actions in the form of assessing the veracity of the information contained in the report, initiating an investigation and coordinating it, as well as conducting communication with the whistleblower.

Whistleblowing reports which are addressed to the President of the KRUK S.A. Management Board or the KRUK S.A. Supervisory Board are handled by the Group Head of Compliance Area or the Head of the Compliance Unit at KRUK S.A., who also performs the role of coordinating the investigation on the basis of the report. The role of Coordinator may be delegated by the Group Head of Compliance Area or the Head of the Compliance Unit to another designated employee of KRUK S.A. Compliance Unit. (hereinafter: Compliance).

The President of the Management Board of KRUK S.A. and authorised members of the Supervisory Board of KRUK S.A. are provided with access to the Whistleblowing System, which can be used to submit Reports addressed directly to them. The President of the Management Board of KRUK S.A. or authorised members of the Supervisory Board of KRUK S.A. may order specific actions, including corrective actions in a given case, if they believe this is necessary.

Handling of a report of a breach

Upon receipt of a report of a breach, a designated and authorised compliance officer (the 'Coordinator') confirms to the whistleblower the acceptance of the report within 7 days of receipt.

Once the Coordinator has accepted the report and made a preliminary assessment of it, they appoint the participants in the proceedings, i.e. the team of people to investigate the case, from among the members of the Violation Report Handling Team operating under the Rules of Procedure (hereinafter: the Team). All persons participating in the examination of a given report have the appropriate written authorization by the Company and they are obliged to maintain confidentiality of information/documents, including protection of the identity of the Whistleblower and the person to whom the report relates, and protection of other personal data received in the course of the investigation.

Following the investigation, a protocol is drawn up, which includes the outcome of the verification of the report (positive/negative), including the required follow-up/corrective actions (e.g. recommendations of specific actions to be taken by a specific deadline). The designated employee of the Compliance Unit (Coordinator) provides feedback to the Whistleblower on the follow-up actions planned or taken and the reasons for such actions within 1 month of the conclusion of the investigation, i.e. within a maximum of 3 months from the date of confirmation to the Whistleblower of the acceptance of the notification or from the expiry of 7 days from the date of receipt of the report.

The person to whom the notification relates, a member of the KRUK S.A. Management Board / designated members of the KRUK S.A. Supervisory Board. (where the report concerns a member of the KRUK S.A.

Management Board) or the Company's Chief Executive Officer/Managing Director will also receive feedback upon completion of the investigation procedure based on the report received.

Whistleblower's and personal data protection

The Companies prohibit retaliation, attempted or threatened retaliation
of such actions against a whistleblower who has made a report, a person assisting in making a report and against a related person.

Pursuant to Section 6 of the Act, a whistleblower is subject to the protection set out in the provisions of Chapter 2 of the Act from the moment of making a report, provided that the whistleblower had reasonable grounds to believe that the information that was the subject of the report was true at the time the report was made or disclosed to the public and that it constituted breach information.

Confidentiality is intended to guarantee the whistleblower's sense of security and to minimise the risk of retaliation. The whistleblower's identity, as well as all information enabling their identification, will not be disclosed to the subjects of the report, to third parties or to other employees and associates of the Company, unless the whistleblower consents to it. The identity of the whistleblower, as well as all information enabling their identification, will not be disclosed to the entities affected by the Report, third parties or other Employees and associates of the Company, unless the whistleblower consents to it. The identity of the whistleblower, as well as other information enabling their identification, may be disclosed only if such disclosure is a necessary and proportionate obligation under generally applicable law in the context of investigations or preparatory proceedings or proceedings conducted by public authorities or courts, respectively. Information about the entities to which the report relates, is subject to confidentiality requirements to the same extent as the identity of the whistleblower.

Unjust accusations, dissemination of false information or formulation of assessments that are not based on facts, may affect the loss of reputation of the Employee to whom the Report relates, and the Company's commercial position, and expose it to financial losses. Thus, it may be the cause of the Employer's loss of trust in the Employee and be the basis for termination of the employment relationship.

It is prohibited to pressure or persuade the whistleblower to reveal their identity if they have made a report anonymously.

Personal data and other information relating to a whistleblower are retained for a period of 3 years after the end of the calendar year in which the follow-up action is completed or the proceedings initiated by the action are completed.

Personal data that are not relevant to the consideration of the Report are not collected, and in the event of accidental collection, they are deleted within 14 days from the date of determining that they are not relevant to the case.

The Whistleblower who reports a Breach familiarises themselves with the information clause available in the Whistleblowing System. In case of Whistleblowers making a Report in paper/e-mail form, the relevant information clause is available on the Company's website at https://pl.kruk.eu/dane-osobowe.

External reports

A Whistleblower may make an External Report without first making a Report to the Company in accordance with the Procedure.

Making an External Report shall not deprive the Signaller of the right to protection against retaliation.

The method of making External Submissions to the Ombudsman is indicated on the Ombudsman's website.

The rules for accepting and processing External Reports are set forth in the provisions of Chapter 4 of the Act.

External Reports regarding potential or actual breaches of anti-money laundering and counter-terrorist financing laws may be submitted by the Whistleblower directly to the General Inspector of Financial Information. The method for making these External Reports to the GIIF is indicated on the GIIF website.

Final provisions

Compliance reviews the Procedure on an annual basis, taking into account changes in the legal status, organizational changes and the validity of the described process. During the review, changes will be made as deemed necessary.

Personal data and other data contained in the report are stored in the Whistleblowing System and in the Register that conducts Compliance on its network resources. This data is confidential and only authorized Compliance Employees have access to it.