Privacy Notice

Misconduct reporting procedure at UniCredit Banka Slovenija d.d.

(Whistleblowing)

Need to know procedure for reporting misconduct at UniCredit Banka Slovenia d.d.

Whistleblowing procedures provide secured channels for employees or other whistleblowers to report fraud, corruption or other serious misconduct (or dereliction of duty) at UniCredit Banka Slovenija d.d. in accordance with the Global Policy (CRIA-111-2022-PL-COMP). Such procedures require the processing of certain personal data:

- information about the persons suspected misconduct (hereafter also referred to as the accused person) and information about whistleblowers and/or other third parties such as witnesses.

What are the main data protection issues covered by UniCredit Banka Slovenija d.d. in the context of managing whistleblowing?

Confidentiality - Information about the whistleblower and the accused person is treated with the utmost care and confidentiality.

Data quality - When processing personal data, the minimum amount of personal data is processed (no more personal data than necessary, following the principle of minimisation).

Right to information - the persons concerned are informed as soon as possible about how their personal data are being processed. Personal data in a report of unacceptable treatment may relate to whistleblowers, persons under investigation, witnesses or other individuals. However, as it is possible that informing the accused at an early stage could jeopardise the investigation, the sharing of the relevant information with the accused may also be delayed. The decision to withhold information is taken on a case-by-case basis and the reasons for any restriction are always documented.

Right of access - in the event of such a request, an assessment of the interests of the persons involved, including those of the applicant and the accused person(s), shall be carried out.

Retention period - reports that do not lead to an investigation, i.e. if it is established that the report cannot be considered as a report of unacceptable conduct, taking into account the internal rules, and no further procedures are necessary, the personal data obtained in the context of the report will be deleted after 5 years.

After the acknowledgement of the Report of the reported unacceptable practice triggering the start of the retention period, all documents in the closed case are reviewed and separated into those containing personal data and those that do not. Documents without personal data may be retained independently of the statutory time limit, since Article 7 of the Whistleblower Protection Act (Official Gazette of the Republic of Slovenia No 16/23) provides that the records of the complaint and the report referred to in Article 12(5) of this Act may be retained in accordance with the Bank's Global Policy. Documents (applicable to electronic and physical documents) containing personal data shall be kept in accordance with the retention period, i.e. 5 years, after which they shall be deleted or destroyed.

Data security - Given that the information processed is sensitive and that a leak or unauthorised disclosure may have adverse consequences for both the whistleblower and the accused, particular attention is paid to the technical and organisational measures necessary to mitigate the risks and ensure data security.

The records relating to the reports are confidential and are stored securely in accordance with the rules applicable within the Group on the classification and handling of confidential information, which are also summarised in the General Information on the Processing of Personal Data - July 2023 Update (GDPR) and in accordance with the Whistleblower Protection Act (Official Gazette of the Republic of Slovenia, No. 16/23). These records are kept in the Compliance Office and in all functions involved in any investigation, and are accessible only by employees who, by virtue of their role and authority, are required to have access to these records.

In accordance with the Law on the Protection of Applicants and the Internal Rules, whistleblowers, accused persons and witnesses have the right to obtain confirmation if personal data relating to them are being processed and may therefore request the adaptation, inclusion, updating or cancellation of processing if the personal data are no longer necessary for the purposes for which they were collected or otherwise processed, where this is possible in the light of the nature of the case.

UniCredit Banka Slovenija d.d. collects and stores the personal data of the whistleblowers, when provided by them, in order to investigate the factual situation arising from the application. The data so provided shall be kept confidential and secure by UniCredit Banka Slovenija d.d. and shall be processed solely to assist in the handling and processing of the given disclosure of irregularities.

UniCredit Banka Slovenija d.d. processes personal data in the context of the submitted report in order to comply with its legal obligations. In connection with the notification of irregularities, UniCredit Banka Slovenija d.d. handles and investigates disclosures of irregularities that take place or have taken place within UniCredit Banka Slovenija d.d. in relation to such processing of personal data.

The legal basis on which UniCredit Banka Slovenija d.d. relies for the processing of personal data is Article 6(1)(c) of the GDPR, which permits the processing of personal data where necessary for compliance with a legal obligation.

What personal data is collected and who has the access to it:

As set out in the Global Whistleblowing Policy (CRIA-111-2022-PL-COMP), an employee or a third party may submit a report, stating his or her identity, anonymously through the whistleblowing channels established by UniCredit Banka Slovenija d.d. The whistleblowing channels guarantee the confidentiality of the identity of the whistleblower, unless the whistleblower has agreed to disclose his or her identity, in which case personal data such as the following may be processed:

- Name,
- surname,
- any other personal data disclosed that is necessary for the investigation process.

If the whistleblower wishes to report the disclosure anonymously, this is also possible.

Anonymous disclosures are treated just as seriously as those made openly. However, if a disclosure is made anonymously, it may not be possible to investigate the whistleblower's concerns as effectively.

Privacy Notice on whistleblowing and legal basis for processing:

UniCredit Banka Slovenija d.d. is aware that the personal data contained in the report of unacceptable conduct may relate to the whistleblower(s), the accused, witnesses or other persons mentioned. Article 6(2) of the Personal Data Protection Act (Official Gazette of the Republic of Slovenia, No. 163/22) is used as the lawful basis for the processing of this personal data, as this type of processing of personal data is provided for in the Whistleblower Protection Act (Official Gazette of the Republic of Slovenia, No. 16/23), as well as in the Banking Act (Official Gazette of the Republic of Slovenia, No. 16/23). 92/21 and 123/21 - ZBNIP), and the processing of

personal data of the whistleblower, witnesses and persons concerned is also carried out by UniCredit Banka Slovenija d.d. in the context of its detection and remediation efforts as defined in the Global Policy.

Information on the processing of personal data at UniCredit Banka Slovenija d.d. is available here: (https://www.unicreditbank.si/content/dam/cee2020-pws-si/SI-DOK/gdpr/GENERAL%20INFORMATION%20ON%20THE%20PROCESSING%20OF%20PERSONAL%20DATA.pdf).

In order to ensure that UniCredit Banka Slovenija d.d. treats each report equally and fairly, all disclosures, including those sent to other departments, will be forwarded to the Compliance Department for action.

The information will be shared internally with UniCredit Banka Slovenija d.d. staff in the relevant departments who will handle, investigate and respond to the disclosure. Internal access to the information processed in the context of the investigation is granted to a limited number of persons who must have access to the information in order to perform their duties in connection with the resolution of the complaint. UniCredit Banka Slovenija d.d. aims to ensure the confidentiality of the information received to the greatest extent possible and to protect the identity of the whistleblower and all other persons involved, in accordance with the Group's applicable rules on the classification and handling of confidential information and in compliance with applicable local laws and regulations.

In certain cases, the information provided by the whistleblower may need to be shared with third parties, such as government departments, public authorities and the police, if it is deemed necessary. In certain circumstances, there may also be a situation where it is necessary to share information in order to comply with the law or disclosure is necessary to prevent or reduce a serious threat to human health or safety.

Storage of personal data and retention period:

Personal data will be stored securely in UniCredit Banka Slovenija d.d.'s case management, document management and email systems. Access to this data is strictly controlled and traceable.

UniCredit Banka Slovenija d.d. will keep the information about the disclosure of the misconduct, including the personal data of the whistleblower, for five years, as stipulated in Article 6, paragraph 4 of the Whistleblower Protection Act (Official Gazette of the Republic of Slovenia, No. 16/23), the Global Policy - Reporting of Unacceptable Conduct, and in accordance with the Rules on Anonymisation or Deletion of Personal Data in Whistleblowing Cases.

The retention period may be interrupted and the scheduled deletion postponed if:

- any proceedings (in particular administrative, judicial or extrajudicial proceedings) are initiated in relation to the case during the retention period;
- an internal or external investigation/inspection is initiated during the retention period;
- in the meantime, supervision is initiated or a request is made by a regulator or other public authority in relation to the case.

How UniCredit Banka Slovenija d.d. protects your personal data:

UniCredit Banka Slovenija d.d. takes the security of personal data carefully and seriously and has internal policies and controls in place to protect data against loss, accidental destruction, misuse or disclosure. Some of the ways in which UniCredit Banka Slovenija d.d. protects personal data include:

- implementing appropriate technical and organisational measures to protect the confidentiality, integrity and availability of personal data and information;
- periodic review of policies and procedures for the provision and protection of information

- ongoing training and awareness-raising for staff on information security and protection;
- Compliance with codes of conduct, certification schemes and guidelines of the Information Commissioner;
- regular review of security and cyber risks.

Applicant's rights:

UniCredit Banka Slovenija d.d. is a data controller in accordance with data protection legislation and complies with the data protection principles when processing personal data.

In accordance with local legislation or internal rules, whistleblowers, the persons concerned and any witnesses have the right to obtain confirmation if their personal data are being processed and, consequently, the right to request amendments, mergers, updates or cancellation if the personal data are no longer necessary for the purposes for which they were collected or otherwise processed.

Under data protection law, the data subject can always:

- request access to and a copy of your personal data;
- request UniCredit Banka Slovenija d.d. to correct/amend incorrect or incomplete personal data;
- request UniCredit Banka Slovenija d.d. to delete/remove personal data where appropriate and possible (for example, if the data is no longer necessary for the purpose for which it was collected and the legal retention period has expired);
- require UniCredit Banka Slovenija d.d. to restrict the processing of personal data (in certain cases where possible);
- request their personal data in portable form;
- object to the processing of your personal data (if appropriate and possible).

With regards to the restriction of the processing of personal data by UniCredit Banka Slovenija d.d., the whistleblower should also be aware that, unfortunately, it is not always possible to guarantee absolute confidentiality, as it could happen that the identity of the whistleblower would have to be disclosed, if such a course of action is defined by law. However, UniCredit Banka Slovenija d.d. takes the issue of maintaining the confidentiality of whistleblowers seriously and will protect identities as far as possible. The whistleblower should also be aware that he/she may be identified by others due to the nature or circumstances of the reported case.

If you wish to exercise any of the above rights, please contact the Data Protection Officer of UniCredit Banka Slovenija d.d. by e-mail to: dpo@unicreditgroup.si

Final provisions:

- UniCredit Banka Slovenija d.d. reserves all rights to amend or supplement the privacy notice in order to ensure compliance with the personal data protection regulations or regulations on the handling of reports of misconduct (Whistleblowing legislation).
- Privacy Notice: version No. 1 valid as from 30th August 2023. This is an annex to CRIA-111-2022-PL-COMP.