PRIVACY NOTICE

on the data processing by OTP Bank Plc. related to Whistleblowing concerning breaches of ethics/law

The data processing activities are carried out in full compliance with Regulation (EU) 2016/679 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 (hereinafter referred to as the "GDPR" or the "General Data Protection Regulation"), Act CXII of 2011 on the Right to Informational Self-determination and Freedom of Information (hereinafter referred to as the "Information Act"), and Act XXV of 2023 on Complaints, Whistleblowing and the Rules for Reporting Abuse (hereinafter referred to as the "Whistleblowing Act").

In compliance with Act CCXXXVII of 2013 on Credit Institutions and Financial Enterprises (hereinafter referred to as the "Credit Institutions Act") and the Whistleblowing Act, the Bank operates a whistleblowing system for reporting possible violations of the values set out in the Code of Ethics and the violations referred to in the Whistleblowing Act.

OTP Bank Plc. (registered office: 1051 Budapest, Nádor u. 16., hereinafter referred to as the "Bank" or the "Company") ensures the lawfulness and purpose limitation of the processing of personal data processed by it. The purpose of this Privacy Notice is to provide the private individual Whistleblowers and the Reported Party concerned by the whistleblowing (hereinafter collectively referred to as "Data Subjects") with full information about the processing of their personal data in the context of the whistleblowing procedure set out in the Administrative Instruction on the Whistleblowing System for Breaches of Ethics and Breaches of Law.

The Company reserves the right to modify this Notice, and shall provide the relevant notification through the publication of the revised Notice on its website.

1. NAME AND CONTACT DETAILS OF THE CONTROLLER

Controller's name: OTP Bank Plc.

Registered office: H-1051 Budapest, Nádor utca 16.

Postal address: OTP Bank Plc., H-1876 Budapest

E-mail: informacio@otpbank.hu

Phone number: (+36 1/20/30/70) 3 666 666

Website: www.otpbank.hu

2. THE CHARACTERTISTICS OF THE DATA PROCESSING UNDER THIS PRIVACY NOTICE ARE SUMMARISED IN THE TABLE BELOW

The Bank may also collect the Data Subject's personal data—in addition to the data provided by the Data Subject, in particular the Whistleblower—from the following sources:

a) from public registers containing data relating to the Data Subject or—where a right or legitimate interest is demonstrated—from registers accessible to any person;

b) from the registration systems at the Bank's disposal containing the data necessary for the investigation of the relevant Whistleblowing.

No sensitive data[1] are processed in the whistleblowing system for ethics and legal breaches.

[1] Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership, genetic data and biometric data revealing the identity of natural persons, health data and personal data concerning the sex life or sexual orientation of natural persons.

PURPOSE OF PROCESSING	LEGAL BASIS FOR PROCESSING	DATA SUBJECTS AND THE SCOPE OF DATA PROCESSED	STORAGE PERIOD
The Bank processes the Data Subject's personal data for the purpose of operating the Whistleblowing System for Ethics and Legal Breaches, and, in this context, for the purpose of receiving and investigating the Whistleblowing of actual or suspected ethical misconduct and breaches of law and taking the necessary measures.	The legal basis for the processing is the fulfilment of a legal obligation to which the Controller is subject pursuant to Article 6(1)(c) of the GDPR Article 116 of the Credit Institutions Act, and Article 18(1) of the Whistleblowing Act.	The Bank processes the following main categories of personal data of the Whistleblower and the Reported Party: a) the data provided by the Whistleblower in the Whistleblowing, in particular: ▪ the data necessary for identification, ▪ the data necessary for contacting, ▪ other facts and circumstances provided in the Whistleblowing which are relevant to the investigation of the Whistleblowing and which relate to or may relate to the Whistleblower or the Reported Party; b) photos or images; and c) in the case of a verbal report made by the Whistleblower to the phone helpdesk, the audio recording made by the Bank.	The Bank shall keep the data relating to the Whistleblowing and the investigation conducted on the basis of the Whistleblowing, as well as the measures taken, for a period of 5 years from the date of completion of the last investigative act or measure, after which it shall delete them.

3. CONTACT DETAILS OF THE DATA PROTECTION OFFICER

Data Protection Officer's name: Zoárd Gázmár

Postal address: H-1131 Budapest, Babér u. 9.

E-mail: adatvedelem@otpbank.hu

4. SOURCE OF PERSONAL DATA

The Bank may also collect the Data Subject's personal data—in addition to the data provided by the Data Subject, in particular the Whistleblower—from the following sources:

a) from public registers containing data relating to the Data Subject or—where a right or legitimate interest is demonstrated—from registers accessible to any person;

b) from the registration systems at the Bank's disposal containing the data necessary for the investigation of the relevant Whistleblowing.

No sensitive data[2] are processed in the whistleblowing system for ethics and legal breaches.

[2] Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership, genetic data and biometric data revealing the identity of natural persons, health data and personal data concerning the sex life or sexual orientation of natural persons.

5. RECIPIENTS OF PERSONAL DATA

Recipient shall mean a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not.

Pursuant to the Whistleblowing Act, the Bank may, on a case-by-case basis, transfer personal data necessary for the investigation of Whistleblowing, if a whistleblower protection lawyer is involved in the investigation of the Whistleblowing.

The Bank transmits any Whistleblowing concerning the top managers, senior managers or senior executives of an OTP Group company established in the European Union and in third countries, and the personal data concerning the Data Subject provided in the Whistleblowing, to an OTP Group company established in the European Union and in third countries for the purpose of investigating the Whistleblowing. The legal basis for the transfer of data is the legitimate interest of the Bank or of the given company belonging to the OTP Group in the protection of its ethical business operations and ethical values. A list of these domestic companies belonging to the OTP Group is available at the following link: https://www.otpbank.hu/portal/hu/Rolunk/OTPCsoport.

A transfer to another country may take place if the Bank is required to do so by law or if the Bank has a legitimate interest in doing so as a result of the balancing of interests test. If the recipient of the transfer is a third country, one of the safeguards in Chapter V of the GDPR must be applied. The transfer of data processed under the internal whistleblowing system under the Whistleblowing Act to a third country or an international organisation may only take place if the recipient of the transfer has given a legal undertaking to comply with the rules on whistleblowing set out in this Act and subject to the provisions on the protection of personal data.

6. SECURITY OF PERSONAL DATA

The IT systems and other data storage facilities of our Company are located at its registered seat and on the servers leased by the processor. Our Company selects and operates the IT tools applied for the processing of personal data during the provision of the service in such a way that the data processed are:

- accessible for the authorised persons (availability);
- credible and authenticated (authenticity);
- verifiably unchanged (data integrity);
- protected from unauthorised access (confidentiality).

We take particular care to ensure data security, and take all technical and organisational measures and adopt procedural rules required for enforcing the safeguards specified in the General Data Protection Regulation. We take appropriate measures to protect the data from unauthorised access, alteration, transfer, public disclosure, deletion or destruction, as well as damage and accidental loss, and ensure that the data stored cannot be corrupted or rendered inaccessible due to any changes in or modification to the applied technique.

The information systems of our Company and our partners are both protected from computer-assisted fraud, computer viruses, hacking and distributed denial-of-service attacks. Moreover, the operator ensures security by means of server-level and application-level security procedures. Data are backed up on a daily basis. Our company takes all possible measures to prevent personal data breaches and in the event of a data breach it takes action immediately to minimise the risks and eliminate the damages.

7. RIGHTS OF DATA SUBJECTS IN CONNECTION WITH THE PROCESSING

Pursuant to Articles 12–22 of the General Data Protection Regulation, data subjects may request from the controller access to, rectification or erasure of their personal data as well as the restriction of processing; moreover, they have the right to withdraw their consent or object to the processing.

In the event of a violation of their rights defined in the General Data Protection Regulation, data subjects may lodge a complaint with the Controller at the contact details specified in Clauses 1 and 3.

In accordance with Article 12(3) of the GDPR, the Company shall comply with the data subject's request to exercise his or her rights without undue delay, but not later than one month from the date of receipt of the request. That period may be extended by two further months where necessary, taking into account the complexity and number of the requests. The Company shall inform the data subject of the extension of the deadline within one month of receipt of the request, stating the reasons for the delay.

Where the data subject makes the request by electronic form means, the response shall also be provided by electronic means where possible, unless requested otherwise by the data subject, with the requested form specifically indicated in his or her request.

7.1. RIGHT OF ACCESS

The data subject shall have the right to request from the Company—using the contact details provided in this Notice—information as to whether or not personal data concerning him or her are being processed, and, where that is the case, to be informed as to:

- which personal data are processed on what legal basis, for what processing purposes and for how long;
- to whom, when, pursuant to which legislation and to which personal data it has provided access to or to whom it has transmitted personal data, and from which source the personal data have been obtained;
- whether it applies automated decision-making and if so, the logic involved, including profiling.

The first time, at the data subject’s request, the Company shall provide a copy of the personal data constituting the subject of processing free of charge and subsequently, in accordance with Article 12(5) of the General Data Protection Regulation, where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character, the Company may charge a reasonable fee, taking into account the administrative costs of providing information or it may refuse to act on the request.

In order to comply with data security requirements and to protect the rights of the data subject, the Company is required to confirm the identity of the data subject or the identity of the person wishing to exercise the right of access; consequently, the provision of information or access to the data, or the issue of a copy of the data is subject to the identification of the data subject.

7.2. RIGHT TO RECTIFICATION

Via the contact details provided in this Notice, data subjects may request the Company in writing to modify or rectify their personal data, provided that they can credibly confirm the accuracy of the rectified data. If they send the request to the Company by electronic means, the Company shall also respond electronically. If they wish to receive the response in any other way, they need to indicate that in the request.

7.3. RIGHT TO RESTRICTION (BLOCKING) OF PROCESSING

Via the contact details provided in this Notice, data subjects may request that the Company restrict the processing of their personal data (by clearly marking the processing operation as restricted and by ensuring that all other data are processed separately) if:

- they contest the accuracy of their personal data (in which case the Company shall restrict processing for the duration of verifying the accuracy of the personal data);
- they believe that the processing is unlawful, but the data subject opposes the erasure of the personal data and requests the restriction of their use instead;
- the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims; or

- the data subject objects to the processing (in which case the restriction shall be in place for the period of verifying whether the legitimate grounds of the controller override those of the data subject).

7.4. DATA PORTABILITY

You shall have the right to receive the personal data concerning you and made available by you to the Company in a structured, commonly used and machine-readable format and have the right to transfer those data to another controller without hindrance from the Controller, if:

- the processing is based on consent or a contract; and
- the processing is carried out by automated means.

7.5. RIGHT TO ERASURE ("RIGHT TO BE FORGOTTEN")

Data subjects may request in writing via the contact details provided in this Notice that the Company erase their personal data.

The Company shall be required to erase your personal data without undue delay where any one of the following grounds applies:

- the personal data are no longer necessary for the purposes for which they were collected or otherwise processed
- you withdraw your consent and there is no other legal basis for the processing;
- the legal basis for processing is a legitimate interest, a public interest or the exercise of official authority, and there are no overriding legitimate grounds for the processing;
- if the processing of personal data is carried out for direct marketing purposes, you have the right to object at any time to the processing of personal data concerning you for such purposes;
- the personal data have been unlawfully processed.

8. RIGHT TO JUDICIAL REMEDY

If data subjects believe that the data protection rules in effect have been infringed by the Company as a result of the processing of their personal data, they may lodge a complaint with the National Authority for Data Protection and Freedom of Information (address: H-1055 Budapest, Falk Miksa utca 9–11.; Postal address: H-1363 Budapest, Pf.: 9; Phone: +36 1 391 1400; E-mail: ugyfelszolgalat@naih.hu). The data subject also has the right to lodge a complaint with another supervisory authority, in particular the supervisory authority established in the EU Member State of his or her habitual residence.

A lawsuit may also be brought against the Controller for the violation of the rules applicable to the processing of personal data. The data subject may bring the case before the Budapest Metropolitan Court or the court of his or her place of residence. The contact details of the regional courts in Hungary are available at: http://birosag.hu/torvenyszekek. If the data subject has his or her habitual residence in another EU Member State, the action may be brought before the competent court in the Member State of habitual residence.