OTP BANK PLC.

PAYMENT SERVICES

SUPPLEMENTARY PRIVACY STATEMENT

This Privacy Statement is an addition to Annex 5 of OTP Bank Plc.'s General Business Regulations, which deals with data processing, and specifies the terms and conditions of data processing carried out in the provision of payment services. This Privacy Statement shall be applied together with the data processing-related Annex 5 of OTP Bank Plc.'s General Business Regulations.

1 Data controller and contacts

1.1 Name of the controller: OTP Bank Plc. (hereinafter referred to as: **"Data Controller**")

Registered office: 1051 Budapest, Nádor u. 16

Mailing address: OTP Bank Plc., 1876 Budapest

E-mail address: informacio@otpbank.hu

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

Website: www.otpbank.hu

Information of the data protection officer of the Data Controller:

Mailing address: 1131 Budapest, Babér u. 9

E-mail address: adatvedelem@otpbank.hu

The additional controller involved in joint processing

Name: GIRO Zrt. (hereinafter referred to as: **"Controller2**")

Registered office: 1054 Budapest V, Vadász u. 31

Mailing address: 1054 Budapest V, Vadász u. 31

E-mail address: info@mail.giro.hu

Phone number: +36 1 428 5600

Website: http://www.giro.hu/

Information of the data protection officer of the Controller2:

Mailing address: 1054 Budapest V, Vadász u. 31

E-mail address: dpo@mail.giro.hu

Phone number: +36 1 428-5695

(hereinafter referred to as: "**Controllers")**

2 Processing of the data of the clients

2.1 Scope of Clients

The Controller processes the personal data of the following natural persons (hereinafter referred to as: “Data Subject”) during the provision of payment services and the preparation thereof:

a) account holder,

b) person entitled to dispose,

c) payer party,

d) beneficiary,

e) the natural person entitled to dispose over the account only by means of a secondary account identifier,

f) a natural person representing the Client, Potential Client (statutory representative, parent, guardian, custodian, proxy, name writer),

g) liquidator, bankruptcy administrator, receiver, family administrator,

h) witness.

2.2 Scope of the processed data

Besides the data groups defined under subsection 2.1 of Annex 5 of the General Business Regulations, the Controller processes Data Subjects’ data belonging to the following data groups during the provision and preparation of payment services:

a) data necessary for the identification and execution of payment orders and transactions, including official measures, and related provisions,

b) the documents attached to payment orders,

c) data required for assigning, deleting and conducting the annual review of the validity of a secondary account identifier,

d) data processed within the Complaint handling procedure,

e) data required in connection with the exchange of denominations (for clients not in a contractual relationship with OTP Bank Plc.) for the exchange list, and possibly for the invoicing of fees,

f) mandatory content elements of the report on suspicious banknotes based on Decree No. 19/2019 (V. 13.) of MNB on the processing and distribution of banknotes and on technical tasks relating to the protection of banknotes against counterfeiting.

g) data connected to request to pay.

In connection with this data processing, the Controller does not process personal data described in section 2.1 d) of Annex 5 of the General Business Regulations.

The exact data processed during the provision and preparation of the payment services are included in the provisions of the Business Regulations, the bank account agreement, the payment order and other documents created during the performance of the agreement for the provision of payment services.

2.3 Purposes of the processing

In addition to the purposes specified in Section 3.1 of Annex 5 of the General Business Regulations, the Controller also processes the data defined in Section 2.2 for the following purposes and in accordance with the following additional provisions:

a) Execution of payment orders and transactions, including official measures,

b) Fulfilment of requirements regarding the assignment, deletion, and annual review of the validity of secondary account identifier, ensuring identification of authorized person involved in these operations,

c) Compliance with the obligation to provide the bank account statement and the statement of fees,

d) Administration in relation to additional documents, in addition to the documents to be submitted for opening an account,

e) Processing of the signature sample and the related information sheet (in particular processing the signature sample for checking),

f) The processing of data relating to incorrect or erroneous transfer orders and cash payments, in particular the processing of data of third parties in connection with recall or the transfer of data to them,

g) Processing of data of the payer third party in connection with cash deposits,

h) The data reconciliation according to the sub-chapter “Liability rules” included in the Business Regulations on Payment Services, as data processing,

i) administration in connection with amendment of the data included in authorizations for batch direct debit mandates,

j) Data processing applied in the case of suspected fraud,

k) Data processing for the review of previous payment transactions,

l) Data processing in connection with the procedure for the submission of a claim for repayment,

m) Administration related to initiation of objection handling procedure,

n) Execution of request to pay.

2.4 Legal grounds for data processing

The Controller processes the data of the Data subjects during the provision and preparation of the payment services based on the legal grounds listed in Section 4 of Annex 5 of the General Business Regulations.

The Controller processes the personal data specified in section 2.2 primarily on the legal grounds of preparing the conclusion of the Agreement and the performance of the agreement. For cases not mentioned previously, this Statement indicates the data group(s) processed based on the given legal grounds.

2.4.1 Preparing the conclusion of the agreement and performance of the agreement for the provision of payment services

The Controller processes the personal data provided in the bank account agreement for the purposes of preparing the conclusion of the Agreement and performance of the Agreement, including the enforcement of rights and claims under the Agreement, and filing legal claims.

In addition to the above, the Controller collects personal data in relation to the Data Subject for the purposes of the conclusion or performance of the Agreement from the following sources:

a) documents included in, related or attached to the payment order,
b) official decisions and measures.

Detailed terms and conditions of the provision of services conforming to the Agreement are set out in the Business Regulations on Payment Services (hereinafter referred to as: "**Business Regulations"**) and the documents referenced therein.

To achieve said goals, Data Controller, in particular:

a) processes the Data subject's contacts for the purposes of communication during the preparation and performance of the agreement,
b) identifies the Data subject based on the personal data.

2.4.2 Mandatory data processing

Besides the legal obligations specified in Section 6 of Annex 5 of the General Business Regulations, the Data Controller processes the Data Subjects' personal data for the purpose of performing the following legal obligations, for the following periods:

a) pursuant to Decree No. 35/2017 (XII.14.) of MNB on Payment Service Activities where payment orders are cleared or settled between payment service providers through a domestic payment system, it is mandatory to forward all numeric and alphanumeric data, as properly indicated in the payment orders, including the contents of the "Comment" field, by itemised data transmission separately for each payment order to the other payment service provider. The retention period is according to Section 6.2 of Annex 5 of the General Business Regulations.
b) notification shall be sent via the payee's account servicing payment service provider within four business days following receipt of any authorisation received from the payer to execute batch direct debit mandates, as well as of the modification or withdrawal thereof.
c) pursuant to Decree No. 19/2019 (V. 13.) of MNB on the processing and distribution of banknotes and on technical tasks relating to the protection of banknotes against counterfeiting, for the purposes of the denomination exchange initiated by clients (the retention period is according to Section 7.4 of Annex 5 of the General Business Regulations) and for the purpose of compliance with the rules applicable to suspicious banknotes (the information on the payer and the account holder must be retained for 8 weeks),
d) in respect of the statement of fees and the data required for preparing the statement of fees, according to Government Decree No. 144/2018 (VIII.13.) on certain issues related to the provision of information on fees for consumer

payment accounts. The retention period is 5 years from the termination of the legal relationship pursuant to the provisions of Act V of 2013 on the Civil Code.

e) in respect of the bank account statement and the data required for preparing the bank account statement, according to Act LXXXV of 2009 on the Pursuit of the Business of Payment Services. The retention period is no less than 8 years pursuant to the provisions of Act C of 2000 on Accounting.

2.4.3 The Controller's legitimate interest

The Controller processes the Data Subjects' personal data specified in this section on the basis of the following legitimate interests, besides those specified in Section 7 of Annex 5 of the General Business Regulations.

a) compliance with official measures ordered under the applicable act on judicial enforcement, public administrative procedures and on penal procedures (currently Act LIII of 1994 on Judicial Enforcement, Act CLIII of 2017 on the Means of Execution to Be Effectuated by the Tax Authority, Act CL of 2016 on General Public Administration Procedures and Act XIX of 1998 on Criminal Proceedings) during the period of blocking. The Controller retains the documents received and generated during the designated measures for 5 years after the measure is lifted, taking into account that both the civil and criminal statute of limitations in these cases is 5 years. Proving the proper implementation of the ordered official measures within the limitation period is the legitimate interest of the Controller.

b) the signature samples and related data forms are processed by the Controller on the basis of its legitimate interest to facilitate the identification of Data subjects and to prevent fraud. The data shall be retained for 5 years from the date of collection.

c) In case of a failed secondary account identifier assignment, data relating to a natural person who is authorized to hold a secondary account identifier but does not have the right of disposal of the payment account are retained for 6 months from the date of the request.

d) Data associated with the deleted secondary account identifier are retained for 13 months after the deletion.

2.4.4 Consent of the Client

The method of providing bank account statements; notifying the beneficiary service provider about the upper limit specified in the authorization for the execution of a direct debit order; data processing required for assigning a secondary account identifier used to identify the account holder's payment account, the transfer of such data to the organization operating the central database for secondary account identifiers (GIRO Zrt., as Data Controller 2), forwarding messages in connection with the recall of erroneous transfers and cash deposits, the data processing which is necessary for enforcing a claim for reimbursement or to initiate the Complaint Handling Procedure is based on the affected Account Holder's consent (a voluntary, specific, and unambiguous expression of will based on adequate information). Consent can be given:

a) in the Agreement, by providing the data on the mode of provision of the bank

account statement,

b) upon completion of the batch direct debit mandate and the submission of the claim for reimbursement,

c) when assigning a secondary account identifier,

d) During administration related to initiation of Complaint handling procedure.

Consent can be given voluntarily, and Data subject is entitled to withdraw their consent at any time without restrictions by a notification sent to the Controller. This notification can be sent by the Data Subject to any of the addresses listed under section 1 of this Statement.

The withdrawal of the consent has no consequences for the Data subject beyond termination of access to the service concerned. The withdrawal of consent, however, does not affect the legitimacy of the data processing—carried out based on the consent—before the withdrawal.

3 Recipients of the personal data

Except for public authorities specified in law or a binding act of the European Union who request personal data from OTP Bank Plc. for investigating individual cases, the Controller forwards Data Subjects' personal data to the following third parties and organisations:

a) the payment service provider of the payer party, or beneficiary – independent controller,

b) in respect of suspicious payment instruments the National Bank of Hungary (in Hungarian: Magyar Nemzeti Bank, MNB) – independent controller,

c) the contents of payment orders and transactions, in respect of the secondary account identifiers GIRO Zrt. – joint controller.

4 The rights and the available legal remedies of the affected Customers

The rights of the affected Data subjects are declared in the 21.1.-27.3. sections of the General Terms and Conditions, and the available legal remedies of the affected Customers are declared in the 28.1.-28.5. sections of the General Terms and Conditions.

Budapest, September 1, 2026