PRIVACY NOTICE

The purpose of this privacy notice is to ensure the consistent processing at OTP Bank Nyrt. (hereinafter: Bank) and at OTP Bank Group of the Due Diligence (DD) inquiries, i.e. in connection with the correspondent bank due diligence, to prevent money laundering and terrorist financing and to check their Compliance, to **increase the efficiency through coordination and shared data storage, as well as to ensure uniform processes and procedures.**

The processing is carried out in compliance with the legal regulations specified under Section 3.1 and pursuant to the provisions of the Regulation of the European Parliament and of the Council (EU) 2016/679 (General Data Protection Regulation) 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, and the provisions of Act CXII of 2011 on Informational Self-Determination and Freedom of Information (hereinafter: 'Infotv.').

1. Data of the Controller

1. **OTP Bank Nyrt.** (1051 Budapest, Nádor utca 16, company reg. no: Cg. 01-10-041585)
Due Diligence Unit (hereinafter referred to as: DDU) of the Compliance Directorate
Postal address: 1131 Budapest, Babér utca 7.
e-mail: ddc@otpbank.hu
Phone number: +36 (1) 2983822

Data Protection Officer of OTP Bank Nyrt.: Zoárd Gázmár
Contact information: H-1131 Budapest, Babér u. 9
E-mail: adatvedelem@otpbank.hu

Additional data controller(s) involved in joint data processing, which are subsidiaries of the Bank when the purpose of data processing what is defined under Section 3.2:

2	**OTP Alapkezelő Zrt., as controller for data, where the direct source of data is the Bank and/or OTP Alapkezelő Zrt.**	
	Registered office:	1026 Budapest, 1-3. Riadó Street, Hungary
	Postal address:	1026 Budapest, 1-3. Riadó Street, Hungary
	E-mail address:	compliance@otpalapkezelo.hu
	Website:	www.otpalap.hu
3	**JSC OTP Bank (Ukraine), as controller for data, where the direct source of data is the Bank and/or JSC OTP Bank (Ukraine)**	
	Registered office:	01033, Kyiv, 43, Zhylyanska Str., Ukraine
	Postal address:	01033, Kyiv, 43, Zhylyanska Str., Ukraine
	E-mail address:	Nemchenko Oleksii, compliance@otpbank.com.ua
	Website:	www.otpbank.com.ua
4	**DSK Bank EAD, as controller for data, where the direct source of data is the Bank and/or DSK Bank EAD**	
	Registered office:	1000 Sofia, Oborishte District, 19, Moskovska Str., Bulgaria
	Postal address:	1000 Sofia, Oborishte District, 19, Moskovska Str., Bulgaria
	E-mail address:	DPO@dskbank.bg
	Website:	www.dskbank.bg
5	**OTP banka Srbija A.D., as controller as controller for data, where the direct source of data is the Bank and/or OTP banka Srbija A.D.**	
	Registered office:	21000 Novi Sad, Trg slobode 5, Serbia
	Postal address:	21000 Novi Sad, Trg slobode 5, Serbia
	E-mail address:	fin.in@otpbanka.rs
	Website:	www.otpbanka.rs

6	**Crnogorska komercijalna banka a.d., as controller Bank (Ukraine), as controller for data, where the direct source of data is the Bank and/or Crnogorska komercijalna banka a.d.**	
	Registered office:	81000 Moskovska bb, Podgorica, Montenegro
	Postal address:	81000 Moskovska bb, Podgorica, Montenegro
	E-mail address:	info@ckb.me
	Website:	https://www.ckb.me
7	**OTP banka Hrvatska d.d., as controller for data, where the direct source of data is the Bank and/or OTP banka Hrvatska d.d.**	
	Registered office:	21000 Split, Domovinskog rata 61, Croatia
	Postal address:	21000 Split, Domovinskog rata 61, Croatia
	E-mail address:	info@otpbanka.hr
	Website:	www.otpbanka.hr
8	**OTP Bank Albania, as controller for data, where the direct source of data is the Bank and/or OTP Bank Albania**	
	Registered office:	Blv. Deshmoret e Kombit, Twin Towers, 1st Tower, 9th Floor, Tirana Albania
	Postal address:	Blv. Deshmoret e Kombit, Twin Towers, 1st Tower, 9th Floor, Tirana Albania
	E-mail address:	info@otpbank.al
	Website:	www.otpbank.al
9	**Mobiasbanca – OTP Group S.A., as controller for data, where the direct source of data is the Bank and/or Mobiasbanca - OTP Group S.A.**	
	Registered office:	MD-2012, Chisinau A, Stefan cel Mare si Sfint av., mun. 81, Moldova
	Postal address:	MD-2012, Chisinau A, Stefan cel Mare si Sfint av., mun. 81, Moldova
	E-mail address:	alerteconf@mobiasbanca.md
	Website:	www.mobiasbanca.md

2. Scope of the processed data and data subjects

Scope of the processed data and data subjects:

a/ Information on changes in the ownership structure of the bank concerned
   a. Name (surname and first name), name at birth, place and date of birth, citizenship, address, ownership share of the **Executive Officer**

b/ Data of the **Beneficial Owners**

a. Name (surname and first name), name at birth, citizenship, place and date of birth, address, and size and type of the ownership share of the Beneficial Owner

c/ Data of the **Executive Officers**
   a. Name (surname and first name), name at birth, title of executive position, citizenship, place and date of birth, address of the Executive officer

d/ The names and positions of the **beneficial owners**, **board members**, and **their relatives**, who
   a. may have an impact on public procurement procedures, or
   b. are members of higher level sports associations, or
   c. may influence government decisions or the government person who makes such decisions, or
   d. hold any senior position that may affect profits.

e/ For **politically exposed persons (PEP)** and lists of sanctions
   a. the name, place and date of birth and citizenship of the **person indicated on the list of sanctions**, and the name of the list of sanctions, which includes
   b. the names, place and date of birth, citizenship and list of sanctions of the **Beneficial Owners**, **Executive Officers** and **Shareholders** who are located or operate in Iran, Syria, North Korea, Cuba, Myanmar or Sudan
   c. the names and positions of the **beneficial owners** and **executive officers**, who are considered politically exposed persons (PEP).

f/ Data of the **contact person** and the **compliance AML manager**
   a. surname and first name, position, e-mail address, phone number
   b. data required for the examination of good business reputation and integrity: reference check, verification of publicly available data

3. Purpose of the processing

3.1 The purpose of data processing for the Bank is to conduct an in-depth analysis for assessing and evaluating the foreign-registered financial service provider's anti-money laundering and anti-terrorist financing controls and in that regard to carry out the required due diligence measures.

3.2 The purpose of the joint data processing by the Bank and its subsidiaries listed under Section 1 (from point 2 to 9) is to ensure that, by effectively avoiding the duplication of work, DD documents have the same data content within the OTP Group, to coordinate responses to inquiries from correspondent bank contacts, and for the Bank to be able to coordinate the outgoing DD requests to correspondent banks at the group level in accordance with the relevant legal regulations. In addition, a further purpose is to simplify the DD processes, to make the related operation more efficient, and to share knowledge about DD audits within the OTP Group. For this purpose, a database will be created in which the DD documents requested by the members of the OTP Group will be available in full to the central DDU area of the Bank and, in justified cases (if a correspondent banking relationship is established or has been previously established at the subsidiary bank), to the authorised employees of the DD areas of the OTP Group. Given that DD documents also contain personal data, the sharing of the documents necessarily entails the transmission of the data of the Data Subjects (beneficial owners, executive officers and their relatives, persons with influence on profit generation, politically exposed persons, persons on the sanction list, contact person, compliance/AML manager) and their sharing within the group.

In order to achieve the purpose of joint data processing, joint data processing agreements have been concluded between the Bank and the companies belonging to the OTP Group (separately with each member of the OTP Group), i.e., data controllers listed in section 1, with the exception of JSC OTP Bank (Russia), considering that JSC OTP Bank (Russia) acts as sole data controller and does not transfer data to the Bank in accordance with national legislation, however, it has access to the Bank's data.

4. Legal background and legal ground of the processing

4.1. Legal ground of the processing for the purpose defined under Section 3.1

Requests for documents and the processing of the data are mandatory under the relevant EU Directive (Directive (EU) 2015/849 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL (20 May 2015) on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No. 648/2012 of the European Parliament and of the Council, and Repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC), and should take into account the provisions of Act LIII of 2017 on the prevention and combating of money laundering and terrorist financing (hereinafter: 'AML Act') and the AML legal regulations applicable to the group member, the DD assessment requirements for correspondent banking relationships, which, when establishing and maintaining a correspondent banking relationship, requires the monitoring, evaluation, and documentation of the results of the evaluation of counterparty money laundering and terrorist financing prevention and compliance.

Pursuant to AML Directive 4, the **processing of the data for AML/CFT purposes** is of public interest, with the data received by obligated service providers during the customer due diligence measures able to be transferred within

the group - not only within the EU - (the receipt of the result of the third party customer due diligence is applied), and data protection is ensured within the bank group.

4.2. Legal background supporting the justification of group-level processing and the legitimate interest of the OTP Group (Legal background ground of the joint data processing for the purpose defined under Section 3.2)

The AML Directive 4 specifies that the money laundering policies (i.e. regulations) and procedures (the methods and systems used) **should be implemented at group level.** These policies should ensure an adequate level of data protection and data sharing within the group in the area of combating money laundering and terrorist financing (AML/CFT). Such policies and procedures shall be carried out and implemented effectively at the branch and majority-owned subsidiary level within the Member States and in third countries.

A 4. The AML Directive allows for the transfer of the results of third-party customer due diligence measures and requires that this also be applied to intra-group data sharing.

In order to achieve the above, the OTP Group introduced joint data processing at Group level, the **legal ground** of which is justified by the legitimate interest of the OTP Group pursuant to Article 6 (1) f) of the GDPR:

Pursuant to the legislation detailed in Section 3.1, banks are required to carry out tasks related to money laundering and terrorist financing **and to harmonise and coordinate the related processes at group level within the group**.

The legal ground for the sharing of data at the group level is the **legitimate interest of the OTP Group** to act consistently at OTP bank group level in fulfilling the obligations in accordance with the above legal regulations, and to have processes for DD documents based on uniform principles at OTP group level, and to not have the data of a partner requested repeatedly if a DD audit has already been performed in relation to the partner at an OTP bank group member. This avoids the duplication of activities and the processing of different data at group level for a particular partner (otherwise, the same partner may provide different data to each of the subsidiary banks of the group during the DD assessments). In this way, the data processing also ensures that the data is accurate and up to date.

Considering that according to the legal requirements DD documents contain personal data, they cannot be deleted during the transmission, because in the absence of these the documents cannot be accepted. Sharing of DD documents thus necessarily involves the transfer of personal data.

5. Source of data

The source of the data is OTP Bank Nyrt. and the areas of the subsidiaries defined in section 1 that process DD inquiries, i.e. the Group Members indicated below:

OTP Alapkezelő Zrt., as Controller	1026 Budapest, Riadó utca 1-3, Hungary
JSC OTP Bank (Ukraine), as Controller	01033, Kiev, Zhylianska Str. 43, Ukraine
DSK Bank EAD, as Controller	1000 Sofia, Oborishte District, 19, Moskovska Str., Bulgaria
OTP banka Serbia A.D , as Controller	21000 Novi Sad, Trg slobode 5, Serbia
Crnogorska komercijalna banka a.d., as Controller	81000 Moskovska bb, Podgorica, Montenegro
OTP banka Hrvatska d.d., as Controller	21000 Split, Domovinskog rata 61, Croatia
OTP Bank Albania, as Controller	Blv. Deshmoret e Kombit, Twin Towers, 1st Tower, 9th Floor, Tirana Albania
Mobiasbanca – OTP Group S.A., as Controller	MD-2012, Chisinau A, Stefan cel Mare si Sfint av., mun. 81, Moldova

6. Implementation of joint data processing, guarantees for proper data processing and prevention of unauthorised or unjustified access

Joint data processing is implemented in relation to the data stored in the system used jointly by the members of the OTP Group. The DD documents requested by the Bank and the other companies of the OTP Group are uploaded into a common system used by the OTP Group (except for JSC OTP Bank (Russia), which company does not

transfer data into the central database), and is supervised by the Bank's central DDU area based on a decision of the OTP Group and ensures, through the management of rights and authorisations, that the DD officers of the OTP Group have access to the documents only when warranted. Accesses are logged so that the data processed and stored in the system can only be accessed by the competent staff of the subsidiaries when justified and that subsidiaries do not have access to each other's data (i.e., the data for which they are the source of the data) and the use of the system can be verified subsequently.

The access rights of the Bank's central DDU area are managed as follows:

- Access is provided for specific individuals.
- Access is granted to specific databases, folders, and documents.
- Access is granted for the period of 1 year (annual review required).
- As a general rule, the DD areas of the companies belonging to the OTP Group can only see their own data or the data of OTP Bank Nyrt. (i.e., the data where they or OTP Bank Nyrt. is the source of the data), but they cannot see not each other's data.
- Only the Bank's central DD area has access to the data of the Bank's subsidiaries (except for JSC OTP Bank (Russia)). Therefore, the Bank's central DDU area can only provide additional access to the data and documents requested by it.

It is a general principle that subsidiaries do not have access rights to each other's data relating to partners with whom they do not have a correspondent banking relationship, therefore they cannot see or process it. Where appropriate (correspondent banking relationship with both parties, i.e. both with the Bank and the given subsidiary), the DD areas of the subsidiaries see and fully process the data of the shared questionnaires and the results of the assessments.

In order to comply with the principles set out in the data protection regulation (GDPR), a joint data processing agreement was concluded with the members of the OTP Group, supplemented by guarantee principles in accordance with the provisions of the GDPR for non-EU group members (with general data protection stipulations pursuant to Article 46 of the GDPR).

Enforcement of purpose limitation and data minimisation: The members of the OTP Group shall use the data solely for the achievement of the purposes set out in this document (section 3.), shall not process them for any other purpose, and shall not process any data that is not necessary to achieve the objectives, i.e. the data processing is limited to the most essential data.

Duration of the processing: The personal data are processed in accordance with the legal requirements (AML Act) for 8 years from the date of termination of the relationship, after which the documents are erased.

Enforcement of the principle of storage limitation: The DD documents are stored on the Bank's own servers, and the recorded data, as detailed above, is accessible only to the employees of the eligible OTP Target Group.

7. Recipients of data transfer

OTP Bank Nyrt. transfers the personal data of Data Subjects in respect of which it is the direct source of the data to the following third parties and organisations with the exception of those public authorities specified in law or in a binding legal act of the European Union, which request personal data from OTP Bank Nyrt for their inspections in individual cases:

OTP Alapkezelő Zrt., JSC OTP Bank (Ukraine), DSK Bank EAD, OTP banka Serbia A.D, Crnogorska komercijalna banka a.d., OTP banka Hrvatska d.d., OTP Bank Albania and Mobiasbanca OTP Group S.A. joint controllers with OTP Bank Nyrt.

JSC OTP Bank (Russia), individual/sole data controller.

By transferring personal data to JSC OTP Bank (Russia), a JSC OTP Bank (Ukraine), a OTP banka Serbia A.D, a Crnogorska komercijalna banka a.d., OTP Bank Albania and Mobiasbanca - OTP Group S.A., OTP Bank Nyrt. transfers the data of data subjects to third countries (Russia, Ukraine, Serbia, Montenegro, Albania, Moldova) outside the states of the Euopean Economic Area (i.e., the Member States of the European Union, Iceland, Norway and Lichtenstein).

An adequate level of protection of personal data in a third country is ensured by standard data protection clauses concluded with these group members in accordance with Article 46 of the GDPR. Copies of documents proving the appropriate guarantees can be obtained by the Data Subject in the following ways: sending an application to the address of the Bank stated in section 1. (postal address, email address)

8. Data Subject's rights and legal remedies relating to processing

Pursuant to Articles 12-21 of the GDPR, the Data Subject may request the Controllers to grant them access to, rectify, erase or restrict the processing of the personal data relating to them, and is also entitled to object to the processing.
In the event of a violation of the data subject's rights under the GDPR, the Data Subject may lodge a complaint with the Controllers at the contact details set out in Section 1.

The Data Subject has the following rights:

8.1 Right to access

The Data Subject has the right to be informed about the essential characteristics of the processing contained in this document (whether the Controllers are processing their personal data, the purpose of the processing, categories of personal data processed, addressees of data transfers (in particular when personal data are transferred to a third country or to an international organisation), the planned duration of the processing, the administrative or judicial bodies with which the Data Subject may lodge a complaint).

8.2. Right to rectification

The Data Subject shall have the right to request the Controllers to rectify the inaccurate personal data relating to them without undue delay, and they may also request that the incomplete personal data be supplemented, taking into account the purpose of the data processing.

8.3. Right to erasure

The Data Subject has the right to request the Controllers to immediately **erase their personal data from the group-level data sharing database**, taking into account that the sharing and recording of the data in a common database is **based on a legitimate interest** as detailed in Section 4.2. Pursuant to the relevant provisions of the GDPR, the Controllers, if the legal ground for the data processing is a legitimate interest, are obliged to immediately erase the personal data relating to the Data Subject.

However, the Data Subject **may not request the erasure** of their personal data **from all databases**, given that the data collection is the statutory responsibility of the individual Controllers pursuant to the legal regulations specified in Section 4.1. Under the relevant provisions of the GDPR, a request for erasure **cannot be complied with** if data processing is necessary, for example, when the processing of the personal data is performed to fulfil an obligation of the Controllers based on legislation of the European Union or a Member State thereof, or out of public interest.

8.4. Restriction of processing (blocking)

Upon the request of the Data Subject, the Controllers restrict the data processing, if:
- the accuracy of the personal data is contested by the Data Subject (in which case the restriction related to the period during which the Controllers can verify the accuracy of the personal data);
- the Data Subject objects to processing (in this case the restriction applies to the period while it is verified whether the legitimate grounds of the Controllers override those of the data subject).

8.5. Objecting to data processing

The Data Subjects may object to the sharing of their data at OTP Bank Group level. Depending on the place of receipt of the request, the Bank or the company belonging to the OTP Group shall provide written information regarding the group-level data sharing within the shortest period of time from the submission of the request, but not later than within 1 month.

8.6. Enforcement

In the event of a violation of their rights under the GDPR, the Data Subject may lodge a complaint with the Bank or the company belonging to the OTP Group at the contract details indicated above.

The Data Subject may also lodge a complaint against the group-level data processing with the National Authority for Data Protection and Freedom of Information ((http://naih.hu/; 1125 Budapest, Szilágyi Erzsébet fasor 22/c; Postal address: 1530 Budapest, PO Box 5.; Phone: +36-1-391-1400; Fax: +36-1-391-1410; E-mail: ugyfelszolgalat@naih.hu). The Data Subject has the right to submit a complaint to other supervising authorities established in the European Union Member State where they habitually reside.

A legal action may also be initiated against the Controllers for the violation of the rules regarding the processing of personal data. The Data Subject may initiate the legal action through the Budapest-Capital Regional Court or the competent court according to their place of residence. The contact details of the general courts in Hungary can be found on the following link: http://birosag.hu/torvenyszekek. If the Data Subject has their habitual residence in another Member State of the European Union, the legal action may also be brought before the competent court of the Member State of habitual residence.

In the case of OTP Group companies outside the European Union listed in Section 5 of this document, the national legislations on data protection shall govern the lodging of complaints.