



ANNOUNCEMENT

Annex I

TO THE INVESTMENT SERVICES BUSINESS REGULATIONS

Privacy Notice

Effective from: 6 March 2025

Published on: 6 March 2025

OTP Bank Plc.

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

Registered with the Company Registry Court of Budapest-Capital Regional Court under no. 01-10-041585

Central mailing address: H-1876 Budapest

Website: <https://www.otpbank.hu>

OTP BANK PLC.

PRIVACY NOTICE

for investment services and ancillary services, private banking, prestige private banking, direct private banking, portfolio management services and Global Markets Services

This Privacy Notice is issued by OTP Bank Plc. as a supplement to Annex 5 of the General Business Regulations, supplementing the terms and conditions of data processing in the provision of investment services and ancillary services, private banking, prestige private banking, direct private banking, portfolio management services and clarifying the conditions of data processing in the provision of Global Markets Services. This Privacy Notice shall be applied in conjunction with Annex 5 of the General Business Regulations of OTP Bank Plc. on data processing.

1. Controller and contact details

Controller's name: OTP Bank Plc. (hereinafter: **"Controller"**)
Registered office: H-1051 Budapest, Nádor u. 16, Hungary
Postal address: OTP Bank Plc. Central Customer Relations Department, H-1876 Budapest
E-mail: informacio@otpbank.hu; information@otpbank.hu
Phone number: (+36 1/20/30/70) 3 666 666
Website: <http://www.otpbank.hu>

The details of the Data Protection Officer appointed by the Controller are as follows:

Name: Zoárd Gázmár
Postal address: H-1131 Budapest, Babér u. 9.
E-mail: adatvedelem@otpbank.hu

2. Processing of Client data

2.1. Categories of Clients

In the course of providing investment services and ancillary services, private banking, prestige private banking, direct private banking, portfolio management services and Global Markets Services, or in preparation for the provision of services, the Controller shall process the personal data of the following natural persons (hereinafter: Data Subject):

- a) Client holding or co-holding (if applicable) the account,
- b) ad hoc and permanent authorised person,

- c) statutory representative,
- d) guardian, deputy guardian and custodian,
- e) Authorised Representative,
- f) witness.

2.2. Scope of the data processed

In addition to the categories of data set out in Section 2 of Annex 5 to the General Business Regulations, the Controller processes the following categories of data relating to Data Subjects in the course of providing investment and ancillary services, private banking, prestige private banking, direct private banking, portfolio management services and Global Markets Services, or in preparation for the provision of services:

- a) transaction data, account and service characteristics,
- b) data relating to individual premium discounts (e.g. employer's name, Family package),
- c) National Client Identifier,
- d) risk profile,
- e) data necessary to fulfil the obligation to obtain prior information (e.g. financial expertise/experience, wealth/income dynamics, risk appetite, risk tolerance, transaction patterns, financial and wealth situation, savings goals and other needs),
- f) the results of the suitability and appropriateness test (MiFID test),
- g) data to assess suitability and appropriateness,
- h) data needed to define the target market (expertise and experience, financial position, risk tolerance, savings goals and other needs),
- i) data needed for the provision of a personalised offer (financial situation, assets, savings goals),
- j) data on financial situation, economic situation,
- k) insider category,
- l) login ID used to query the MNB balance,
- m) any other relevant data provided to the Controller in relevant communications (which may be telephone conversations, emails, chats, face-to-face meetings) relating to the provision of investment services covered by MiFID II,
- n) data required to use private banking, prestige private banking, direct private banking, portfolio management services and related value proposition elements and Global Markets Services,
- o) identification data of the data subject (e.g. name, address, account number, position)
- p) contact details (e.g. email address, phone number, fax number, etc.),
- q) identification data related to the use of the online trading system (OTP Trader).

The precise scope of the data processed in the course of providing investment services and ancillary services, private banking, prestige private banking, direct private banking, portfolio management services and Global Markets Services, or in the preparation of the provision of services, is set out in the General Business Regulations, the Investment Services Business Regulations, the Private Banking Business Regulations, the Investment Services Framework Agreement (Consolidated Securities Account Contract), the Retirement Savings Account (PSA-D) Consolidated Securities Account Agreement, the Long-term Investment Securities Account, (the START Consolidated Securities Account Contract and the Stability Savings Securities Account Contract, which are no longer sold) hereinafter referred to as the Securities Account Contracts, and the Private Banking, the Prestige Private Banking Master Agreement, the Direct Private Banking Contract and the Portfolio Management Contract and the related Supplements, orders, and other documents generated in the course of providing the Financial Planner Service and the Global Markets Framework Agreement, Individual Contract, Collateral Security Agreement, ISDA and GMRA documentation and other documents generated in the course of performing the Global Markets Service Contract.

2.3. Purpose of processing

The Controller processes the data specified in Section 2.2 for the following purposes, in addition to the purposes set out in Section 3 of Annex 5 to the General Business Regulations, and in addition to the purposes set out therein, as follows:

- a) to check eligibility for discounts,
- b) to recommend a tailor-made product and/or portfolio based on an assessment of financial situation, assets, investment objectives, risk tolerance and risk appetite,
- c) to determine the products for which the Controller may or may not provide investment advice to the Client during the contractual relationship,
- d) to ensure compliance with the obligation to obtain prior information,
- e) to provide prestige services,
- f) to improve the quality of service to the Client,
- g) to make an offer,
- h) to produce analyses for product development and business decision support,
- i) direct marketing,
- j) follow-up and regular information provision,
- k) to record communications related to the provision of the service,
- l) to provide and execute individual transactions related to Global Markets Services, and to perform the obligation to provide and obtain prior information,
- m) to send confirmations and other information related to individual transactions under the Global Markets Framework Agreement,
- n) to make offers, provide investment advisory services, send suitability reports,

- o) to monitor and check the continuous provision of liquidity,
- p) internal credit exposure analysis,
- q) to fulfill the reporting obligation defined by law.

2.4. Legal bases for processing

The Controller shall process Clients' data in the course of providing investment services and ancillary services, private banking, prestige private banking, direct private banking, portfolio management services and Global Markets Services or in the preparation of the provision of services, on the basis of the legal grounds listed in Section 4 of Annex 5 to the General Business Regulations.

The Controller processes the personal data specified in Section 2.2 of this notice primarily for the purposes of preparing the conclusion of the contract, the performance of the contract and the performance of legal obligations. In other cases, this Notice identifies the category(ies) of data processed on the basis of the relevant legal title.

2.4.1. Preparation of the conclusion of the contract for the provision of investment services and ancillary services, execution of the contract

The Controller processes personal data provided in the Securities Account Contracts, and in the course of Private Banking, Prestige Private Banking, Direct Private Banking and Portfolio Management Services, the Financial Planner Service, and in the Global Markets Framework Agreement, the Individual Contract, Collateral Security Agreement, ISDA and GMRA documentation, separate contracts, for the purpose of preparing the conclusion of the Contract and the performance of the Contract, including the enforcement of rights, claims and legal actions arising from the Contract.

The detailed terms and conditions of the provision of the services under the Contract are set out in the Business Regulations listed in Section 2.2 and the documents referred to therein.

In order to achieve the above objective, the Controller shall in particular:

- a) identify the Client on the basis of personal data in the context of the preparation of the conclusion of the contract,
- b) process the Client's contact details for the purpose of contacting the Client during the preparation and performance of the contract,
- c) analyse the Client's personal data, financial and income situation, investment objectives, risk-bearing capacity and risk appetite, knowledge and experience of financial instruments in order to provide a personalised product recommendation,
- d) develop personalised offers,
- e) assess requests for individual fees and requests for equitable procedure,
- f) define the transactions subject to reporting and disclosure requirements and the closed periods based on the insider category setting,

- g) process the data necessary for the conclusion and performance of the contract, used for contact and client identification purposes in the course of providing Global Markets Services,
- h) develop personalised offers,
- i) process data relating to the financial status and economic situation of the Data Subject in order to monitor and control the provision of collateral for individual transactions and to mitigate the risk of default,
- j) in the case of contracts that have not been concluded, record and process the Data Subject's data as defined in Section 2 of the General Privacy Notice and in this Notice, even after the failure of the contract, for the purpose of enforcing, presenting or defending any claims relating to the failure of the contract. Unless otherwise provided for by law, the normal limitation period of five years defined in the Civil Code shall apply to the enforcement of claims.
- k) process the data of the Debtor(s) in the course of the enforcement of the claim in order to recover the claim,
- l) define the transactions subject to reporting and disclosure requirements and the closed periods based on the insider category setting,
- m) where the Bank acts as a client or (second or third level) indirect client within the meaning of Regulation (EU) No 149/2013¹ and Regulation (EU) No 2017/2154² in connection with the Client's order, it may be obliged to provide information and data (where applicable, data concerning the Client's identity and contact details) concerning the Client to a central counterparty (CCP), clearing member or client or (second level) indirect client as defined in these Regulations in the cases specified in these Regulations.

2.4.2. Mandatory data processing

In addition to the legal obligations set out in Section 7 of Annex 5 to the General Business Regulations, the Controller shall process the personal data of the Data Subjects for the purposes of fulfilling the following legal obligations:

- a) On the basis of Act CXXXVIII of 2007 on Investment Firms and Commodity Dealers, and on the Regulations Governing their Activities (hereinafter: Investment Firms Act), the Controller, in compliance with its obligation to obtain prior information, processes the personal data of the Data Subjects provided in the suitability/appropriateness test (MiFID test) or in the declaration refusing to complete the MiFID tests. The retention period for data processed in the MiFID test is 8 years after the termination of the legal relationship. The retention period for the data processed in the declaration of refusing

¹ Commission Delegated Regulation (EU) No 149/2013 of 19 December 2012 supplementing Regulation (EU) No 648/2012 of the European Parliament and of the Council with regard to regulatory technical standards on indirect clearing arrangements, the clearing obligation, the public register, access to a trading venue, non-financial counterparties, and risk mitigation techniques for OTC derivatives contracts not cleared by a CCP.

² Commission Delegated Regulation (EU) 2017/2154 of 22 September 2017 supplementing Regulation (EU) No 600/2014 of the European Parliament and of the Council with regard to regulatory technical standards on indirect clearing arrangements

to complete the MiFID tests is the general limitation period (5 years) after the termination of the legal relationship pursuant to Section 6:22 of the Civil Code.

- b) On the basis of **Investment Firms Act**, it processes the personal data of the Data Subjects, and determines, based on the results of the Client suitability/appropriateness test (MiFID test), which Risk Profile the Client belongs to (profiling), and determines accordingly which Product Groups of securities and financial instruments the Client is suitable/appropriate to purchase.
- c) It processes the personal data of the Data Subjects pursuant to Act CXX of 2001 on the Capital Market.
- d) Pursuant to Government Decree 285/2001 (XII. 26.) on Bonds, claims against the issuer based on bonds are not subject to a statute of limitations. In this respect, no personal data relating to the provision of the bonds will be deleted.
- e) Pursuant to Article 106(1) of Act XVI of 2014 on Collective Investment Trusts and their Managers and on the Amendment of Financial Regulations, the Controller processes the personal data of the Data Subjects for the purpose of providing information to the investment fund manager.
- f) Pursuant to the rules of Commission Delegated Regulation (EU) 2017/590 of 28 July 2016 supplementing Regulation (EU) No 600/2014 of the European Parliament and of the Council with regard to regulatory technical standards for the reporting of transactions to competent authorities, the Controller processes the personal data of the Data Subjects for the purpose of reporting transactions to the competent authorities.
- g) On the basis of Act V of 2013 on the Civil Code and Government Decree 67/2014 (III. 13.), the Company processes the personal data of the Data Subjects for the purpose of registration in the shareholder register in connection with the keeping of the shareholder register and the related exercise of ownership rights.
- h) Pursuant to the provisions on Unjustified Possession in Act V of 2013 on the Civil Code, OTP Bank Plc. is obliged to keep the data of transactions executed on the terminated account and the Personal Data of the Data Subject for 8 years after the termination of the legal relationship in accordance with the rules on responsible custody, delay and default of the Investment Services Business Regulations.
- i) Pursuant to Articles 59, 60 and 62 to 63 of Commission Delegated Regulation (EU) 2017/565 of 25 April 2016 supplementing Directive 2014/65/EU of the European Parliament and of the Council as regards organisational requirements and operating conditions for investment firms and defined terms for the purposes of that Directive, it processes the personal data of the Data Subjects for the purpose of subsequent and regular information.
- j) Pursuant to Commission Delegated Regulation (EU) 2016/1052 of 8 March 2016 supplementing Regulation (EU) No 596/2014 of the European Parliament and of the Council with regard to regulatory technical standards for the conditions applicable to buy-back programmes and stabilisation measures, it processes the personal data of the Data Subjects for the purpose of recording data processing in relation to insider dealing.

- k) It processes the personal data of the Data Subjects under Act CLVI of 2005 on Pension Savings Accounts.
- l) It processes the personal data of the Data Subjects on the basis of Act CXVII of 1995 on Personal Income Tax.
- m) It processes the personal data of the Data Subjects on the basis of Act CXCIV of 2011 on the Economic Stability of Hungary and Decree 62/2013 (XII. 17.) NGM of the Minister of National Economy on detailed rules.
- n) It processes the personal data of the Data Subjects on the basis of Act CLXXIV of 2005 on Start of Life Allowance for Young People.
- o) It processes the personal data of the Data Subjects pursuant to Act LII of 2018 on Social Contribution Tax.
- p) It processes the personal data of the Data Subjects on the basis of Act XXXI of 1997 on the Protection of Children and the Administration of Guardianship.
- q) It processes the personal data of the Data Subjects on the basis of Government Decree 149/1997 (IX. 10.) on Guardianship Authorities and on Child Protection and Guardianship Procedures.
- r) On the basis of MNB Decree No. 36/2015 (IX. 24.) on the methodology of generating the login ID and password for securities accounts and client accounts, the related data reporting and mandatory elements of the regulation on data security requirements, as from 1 January 2016, account managers shall provide Business Partners with a login ID, which, together with the password valid for the given month, enables Business Partners to obtain information on the current status and balance of their securities account and client account on the MNB website for the last day of the previous month.
- s) It retains the personal data recorded for the purposes of identification as per Section 7 of Act LIII of 2017 on the Prevention and Combating of Money Laundering and Terrorist Financing (hereinafter: **AML Act**) for 8 years after the termination of the legal relationship or until the end of the statute of limitations of the legal relationship for the prevention and combating of money laundering and terrorist financing.
- t) It processes the personal data of the Data Subjects under Act CXXXVIII of 2007 on Investment Firms and Commodity Dealers, and on the Regulations Governing their Activities: it determines according to the results of the Client's suitability/appropriateness test (MiFID Test), to which of the Global Markets Services the Client is suitable/appropriate for; it determines whether the Global Markets Service is included in the Client's target market and, for the purposes of the preparation of the Data Subject's suitability report, uses the information which are not specified in Commission Delegated Regulation 2017/565 (Articles 54 and 55) but are necessary for the preparation of the suitability report; such data will be kept by the Controller for 8 years after the termination of the legal relationship or until the statute of limitations of the legal relationship.
- u) In order to fulfil the legal obligation provided for in Section 49(2)–(4) of Act CXXXVIII of 2007 on Investment Firms and Commodity Dealers, and on the

Regulations Governing their Activities, the knowledge and experience of the Data Subject shall be taken into account during the provision of Global Markets Services, which data shall be retained by the Data Controller for 5 years after the termination of the legal relationship or until the end of the limitation period of the legal relationship.

- v) Pursuant to Articles 25 and 26 of Regulation (EU) No 600/2014 of the European Parliament and of the Council (hereinafter: **MiFIR**), Article 6 and Annex II of Commission Delegated Regulation (EU) No 2017/590 and Section 55 of the Investment Firms Act, the Controller shall process the national identifier it has generated, which data shall be kept for 8 years after the termination of the legal relationship or until the end of the limitation period of the legal relationship.
- w) Pursuant to Article 26 MiFIR, the Controller shall keep the data transferred to the trading venue for the purpose of executing a transaction order on the trading venue for 8 years after the termination of the legal relationship or until the end of the limitation period of the legal relationship.
- x) Pursuant to the provisions of Article 57 of Directive 2014/65/EU of the European Parliament and of the Council (hereinafter: **MiFID II**), the Controller shall process the data necessary to monitor the position limits of the Data Subject in relation to commodity swaps and shall keep them for 5 years after the termination of the legal relationship or until the end of the limitation period of the legal relationship.
- y) Pursuant to the legal requirements of Article 16 of MiFID II, the Controller records telephone conversations with the Data Subject for the purpose of recording so-called relevant communications, makes notes of face-to-face meetings and stores electronic messages for a period of 5 years after the date of the communication, or up to 7 years if required by the competent authority.
- z) Pursuant to Article 16 of MiFID II and the provisions of the Investment Firms Act, for the purpose of recording relevant communications, it records telephone conversations with the Data Subject on relevant communications within the scope of MiFID II, and suitability reports in the form of a questionnaire, makes notes of face-to-face meetings, and stores electronic messages and keeps them for 5 years after the date of the communication or, if required by the competent authority, for a maximum of 7 years.
- aa) Based on the legal requirements under Articles 54 and 55 of Commission Delegated Regulation (EU) 2017/565, the Controller shall process the data processed for the purpose of preparing the suitability report related to the provision of Global Markets Services and shall keep them for 5 years after the termination of the legal relationship or until the end of the limitation period of the legal relationship.
- bb) Pursuant to Section 106 of Act CCXXXVII of 2013 on Credit Institutions and Financial Undertakings, the Controller shall investigate whether the Data Subject is affected by internal credit.
- cc) Pursuant to Federal Register /Vol. 76, No. 141 / Friday, July 22, 2011 /Rules and Regulations, COMMODITY FUTURES TRADING COMMISSION 17 CFR Parts 15 and 20, RIN 3038–AD17 Large Trader Reporting for Physical Commodity Swaps, the Controller shall prepare and forward the report and shall keep them for 5 years

after the termination of the legal relationship or until the end of the limitation period of the legal relationship.

The Controller does not carry out data processing in connection with this data processing pursuant to the Act on the Central Credit Information System (hereinafter referred to as the "CCIS"), one of the legal provisions described in Section 7 of Annex 5 to the General Business Regulations.

2.4.3. Legitimate interest of the Controller

In addition to the legitimate interests set out in Section 8 of Annex 5 to the General Business Regulations, the Controller also processes the personal data of the Data Subjects as defined in this Section on the basis of the following legitimate interest:

- a) The Controller may analyse the Data Subjects' data for the purposes set out in Section 2.3(a), (i) and (j) in the context of product, business and service development related to the provision of investment services and ancillary services, in order to develop a marketable range of products and services and to maintain its competitiveness, with a view to developing products and services that are better suited to the needs of the Data Subjects.
- b) The purpose of the processing of the data as set out in Section 2.2(m) of this Notice is for the Controller to record and retain communications with the Data Subject (including, but not limited to, telephone conversations), as relevant communications are a broad category and any communication during the course of the communication is already a relevant communication by virtue of its further content. Recorded communications that are subsequently found not to be relevant communications are retained by the Controller in order to use them in the event of a dispute, to justify its actions or services and to pursue its legitimate interest. The Controller shall keep the data processed in accordance with the above for 5 years from the termination of the legal relationship or, if required by the competent authority, for a maximum of 7 years.

2.4.4. Performance of a task carried out in the public interest as a legal basis for data processing

The Controller will not process the personal data of the Data Subjects as defined in this Section on the basis of a task in the public interest apart from the performance of the task in the public interest as defined in Section 9 of Annex 5 to the General Business Regulations.

2.4.5. Consent of the Data Subject

The Controller shall process the personal data of the Data Subjects as set out in this Section, in addition to those set out in Section 10 of Annex 5 to the General Business Regulations, on the basis of the following consent:

- a) The processing of personal data processed by electronic means for the purpose of sending direct marketing information is based on the Data Subject's consent

(voluntary, specific, informed and unambiguous indication of his or her wishes). Consent may be given in a separate declaration.

Consent is given voluntarily and the Data Subject has the right to withdraw consent at any time, without limitation, by notifying the Controller. The Data Subject may send the notification to any of the contact addresses in Section 1 of this Notice.

Withdrawal of consent has no consequences for the Data Subject. However, the withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal.

2.5. Automated decision-making, including profiling for this purpose

The Controller shall also process the Client's personal data in the course of automated processing for the conclusion and performance of the Contract between the Client and the Controller and in the course of providing the Financial Planner services pursuant to Act CXXXVIII of 2007 on Investment Firms and Commodity Dealers, and on the Regulations Governing their Activities, which applies to the Controller, the result of which is that the Bank may provide the Client with investment advisory services only in respect of financial instruments that are suitable and appropriate for the Client.

In the course of the above automated decision-making, the Controller uses the Client's data on financial expertise and experience, wealth and income dynamics, risk appetite and transaction patterns as follows: the MiFID test is completed and evaluated electronically, with IT system support, based on an algorithm. The Client's risk profile is determined on the basis of the weighted score of the answers to the MiFID test questions and the contradiction and consistency check.

The Controller further informs the Business Partner that the decision taken in the course of automated decision-making has the following consequences for the Client: The Bank may not provide investment advice in respect of financial instruments that are unsuitable and inappropriate for the Client.

3. Recipients of personal data

Except for public authorities, defined by the law, or the binding legal acts of the European Union, that demand personal data from the Bank for the purposes of their investigations of individual cases, the Controller shall transfer the personal data of the Data Subjects to the following third parties/entities:

- a) to Government Debt Management Agency Pte. Ltd. (independent controller) as a third party (organisation) in the event that Government Debt Management Agency Pte. Ltd. requests the Subscription Sheet of Government Securities, that is, the personal data of the Business Partners in writing from the Controller for the purpose of assessing the performance of the Distribution Agreement,
- b) to another investment service provider (independent controller) if the Client requests the transfer of his/her securities account (typically PSA-D, LTISA) to another investment service provider,

- c) to Clearstream (as independent controller) if the Client completes the so-called W8-BEN form in connection with the preferential taxation of US financial instruments,
- d) to KELER Ltd. and any other clearing house (independent data controllers) in connection with the maintenance of the shareholder register,
- e) to KELER Ltd. and any other clearing house (independent controller) as part of the transaction report,
- f) to the issuer of the shares (independent controller) in the context of the shareholder register,
- g) to the Magyar Nemzeti Bank (independent controller) as part of the transaction report,
- h) to the Budapest Stock Exchange (independent controller) as part of the transaction report,
- i) to Deutsche Börse AG (independent controller) as part of the transaction report,
- j) to the Commodity Futures Trading Commission (CFTC), the CME Group (CME, CBOT, NYMEX and COMEX), the Intercontinental Exchange (ICE) (independent controllers) as part of the reporting obligation

during which it complies with data transfer obligations.

4. 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:

- a) accessible for the authorised persons (availability);
- b) credible and authenticated (authenticity);
- c) verifiably unchanged (data integrity);
- d) 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 avoid personal data breaches and in the event of a data

breach, it takes action immediately to minimise any risks and eliminate any damage, in accordance with our incident management regulations.

5. 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.

If the processing is based on consent, giving consent is voluntary in all cases and the consent may be withdrawn at any time during the processing. Data subjects may indicate to the Company their intention to withdraw consent at the contact details specified in Clauses 1. The withdrawal of consent shall not affect the lawfulness of processing before its withdrawal.

In accordance with Article 12(3) of the General Data Protection Regulation, the Company shall fulfil the data subject's request to exercise his or her rights without undue delay, but within one month of receipt of the request in any event. 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.

5.1. 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:

- a) which personal data are processed on what legal basis, for what processing purposes and for how long;
- b) 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;
- c) 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.

5.2. 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.

5.3. 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:

- a) 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);
- b) 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;
- c) 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
- d) 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).

5.4. 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:

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

5.5. 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:

- a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;

- b) you have withdrawn your consent and there is no other legal ground for the processing;
- c) 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; or
- d) where personal data are processed for direct marketing purposes, you have the right to object at any time to the processing of your personal data for such purposes;
- e) the personal data have been unlawfully processed.

5.6. OBJECTION TO PROCESSING

You have the right to object to the processing based on legitimate interest using any of the contact details provided in Clauses 1.

6. 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). Data subjects are also entitled to lodge a complaint with other regulators; thus, in particular, with the supervisory authority in the Member State of their habitual residence.

Court proceedings 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-Capital Regional Court or the court of law having jurisdiction over his/her place of residence. The contact details of the courts in Hungary are available at the following link: <http://birosag.hu/torvenyszekek>. If the habitual residence of the data subject is located in another Member State of the European Union, the proceedings may be brought before the courts with competence and jurisdiction in the Member State of his/her habitual residence.