PPF Banka

INFORMATION ON PERSONAL DATA PROCESSING

The purpose of this document is to provide information and guidance to natural persons (**"individuals"**) on the matters below in connection with the use of banking and/or investment services and products, or in connection with the provision of support for such services and products or their development, in accordance with Regulation (EU) 2016/679 of the European Parliament and of the Council 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 (the General Data Protection Regulation or the **"GDPR"**):

1. Identity and contact details of the personal data controller

PPF banka a.s., having its registered office at Praha 6, Evropská 2690/17, 160 41, incorporated in the Companies Register of the Municipal Court in Prague, Section B, File 1834, Company No: 47116129.

Contact details: the Data Protection Officer can be contacted by email at: DPO@ppfbanka.cz

2. Legal basis and purposes of processing personal data

The controller is obliged to ensure the lawfulness of the processing of personal data. The controller may process personal data pursuant to applicable laws and regulations, including, but not limited to, Act No 21/1992 on banks, as amended (the **"Banking Act"**), Act No 256/2004 on capital market business, as amended (the **"Capital Markets Act"**) and Act No 253/2008 on certain measures against the legalisation of the proceeds of crime and the financing of terrorism, as amended, (the **"Anti-Money Laundering Act"**). Processing of personal data is also lawful if it is necessary for the performance of a contract or in order to take steps prior to entering into a contract, (e.g. contracts with clients or suppliers of the controller), or if it is carried out with the consent of individuals. The controller may also process data on the basis of its legitimate interests. In specific cases, the processing of personal data may be necessary to protect the vital interests of individuals or to perform a task carried out in the public interest.

2.1 Categories of data processed

The controller collects and processes individuals' personal data primarily so that they can be clearly identified and contacted (basic data). The personal data processed by the controller includes, in particular (scope of personal data processed): given name, surname, title, personal identification number (if assigned), date of birth, sex, place of birth, citizenship, address of permanent or other residence, and identity document number, date of issue and period of validity. Contact details consist of a mailing address, telephone number, fax number, email address, and any other relevant information such as login names.

The controller also collects and processes personal data for the performance of contracts on the provision of services and products, or in order to take steps, at the request of the relevant individual, prior to entering into such contracts (information about products and services). These data include payment attributes, e.g. account number, payment card number; investment attributes, e.g. investment profile, transactions and contracts; or credit attributes, e.g. information about creditworthiness, debt or outstanding amounts. The data processed in relation to communications include complaints and service requests. Additional and other data include, for example, records from business premises, telephone calls, and access to the controller's information systems, including the storage of data on devices in the form of cookies.

In justified cases and to the extent necessary for the provision of services, compliance with legal obligations, and ensuring security, the controller may collect and retain records of communications with the data subject (e.g., telephone calls, email correspondence, messages via electronic channels) and technical data regarding the communication channels and end devices used (e.g., login data, IP address, session identifiers, application and device data). This data may be used in particular to handle requests and complaints, fulfill

obligations in the provision of investment or payment services, and to prevent and investigate fraud and security incidents.

The controller also collects and processes personal data, such as given name, surname, email, telephone number, job title, behaviour logging, email messages, IP addresses and username for the performance of a contract or in order to take steps prior to entering into a contract with a supplier.

As a general rule, the controller does not process special categories of personal data as defined in Article 9 of the GDPR (sensitive data), unless required to do so by specific legislation or unless such data is provided by data subjects in connection with the exercise of their rights, complaints, or other communications. In such cases, the controller acts in accordance with the GDPR and applies the relevant exception under Article 9(2) of the GDPR.

The controller processes data on bank transactions in its endeavour to execute these without undue legal and material risks and also to protect its rights, and for its internal requirements (in particular to monitor the quality of service provision and to evaluate potential risks).

2.2 Purposes of personal data processing

The controller processes personal data for the following purposes:

(a) to identify and authenticate clients in order to prepare and enter into contracts for the provision of products and services in compliance with the **Anti-Money Laundering Act** and the **Banking Act**;

(b) to provide products and investment services on the financial markets: accepting, transmitting and executing client orders; activities as an administrator, security agent or calculation agent; trading with counterparties, settlement on financial markets, portfolio valuation, for the purposes of client and regulatory reporting, and to check compliance with the Capital Markets Act, including the control and prevention of market abuse;

(c) to provide credit products and services: loan approval, credit risk management, loan utilisation, monitoring, restructuring and recovery, management of security (including receivables used as collateral to secure loans) and regulatory reporting;

(d) to provide payment services: account management, issuing electronic payment instruments their tokenization and security, and making payments via all electronic channels, regulatory reporting;

(e) to control and prevent money laundering and financing of terrorism in compliance with the Anti-Money Laundering Act;

(f) to comply with statutory obligations in relation to accounting and taxes, e.g. FATCA;

(g) to handle claims and complaints;

(h) to communicate with regulators and authorised auditors;

(i) to report to competent authorities on matters relating to data subjects that are covered by banking secrecy;

(j) to defend the controller’s rights, e.g. during debt collection by legal means;

(k) to manage suppliers, e.g. suppliers of information systems, for the purpose of the provision of support for services and products provided by the controller or their development, and security, including the testing of software modifications that cannot be implemented without effective testing on the specific data processed by the controller;

(l) for security and risk management, including prevention, e.g. protection of individuals and tangible assets using camera systems to prevent illicit activities, investigation of security incidents, control, prevention and detection of fraud, control and assessment of risks to prevent money laundering and financing of terrorism, prevention, monitoring, and detection of cyber threats; ensuring security in accordance with the Cyber Security Act and the EU Regulation on the Digital Operational Resilience of the Financial Sector; mitigating other risks; As part of security and risk management, the administrator may monitor and evaluate transactions and the use of electronic channels (including technical security indicators of devices and access data) for the purpose of preventing, detecting, and investigating fraud, account misuse, and other security incidents, and for the purpose of protecting clients and the administrator.

(m) for archiving and statistical purposes.

2.3 Sources of personal data

The controller processes personal data provided by an individual, data generated by the activity of an individual, and other data obtained in the provision of products and investment, credit and payment services. In addition to the above, the controller processes data obtained from publicly available sources and registers (information from companies registers, information about enforcement and insolvency proceedings, information from the beneficial ownership registry, e.g. given name, surname, date of birth, residential address). These data are used in compliance with the purposes for which the registers were established, on the basis of the controller's legitimate interests, with a view to assessing risks and thereby complying with its statutory duty of prudence, e.g. to assess the ability to repay debts. The controller processes data obtained from other entities–registers where permitted to do so by specific legislation (e.g. the **Banking Act**).

The controller processes personal data obtained in connection with the conclusion and performance of contracts under which it is the recipient of a service or product, or under which it is a service provider, and from other sources, if obtained in accordance with binding legislation. Personal data must be provided in order to conclude and perform contracts, to comply with the controller's legal obligations, and to protect the controller's legitimate interests. If an individual fails to provide data as requested, the respective product, service or other deliverable cannot be provided by the controller. A further option is for personal data to be provided on the basis of the relevant individual's consent. In such a case, provision is voluntary. Consent may be withdrawn at any time.

Personal data are strictly protected by the controller. The controller processes personal data in electronic information systems that are subject to constant and stringent physical, technical and procedural checks, including their testing. All persons who come into contact with personal data in the performance of their professional duties or contractual obligations are bound by confidentiality. All information on individuals is subject to banking secrecy, which applies to all bank transactions and bank financial services, including account balances and deposits. Personal data are processed directly by the controller or by an entity contracted by the controller for this purpose which provides sufficient and reliable guarantees that technical and organisational measures are in place to protect the data provided.

3. Legitimate interests pursued by the controller or by a third party where processing is based on legitimate interests

In those cases where the controller relies on its legitimate interests in the processing of personal data, this primarily means the exercise of professional care in the provision of banking and investment services, or the performance of such obligations via selected suppliers or providers of support services, including information systems. Examples include for purposes related to bank transactions and services, the evaluation of requests for a bank transaction to be executed or a service to be provided, for the arrangement of all other activities relating to a transaction or service, and for new service development, including related testing of relevant information systems; also to protect the controller's rights and legally protected interests, in particular for the analysis and assessment of potential risks stemming from the services provided by the controller and services that the controller makes use of to secure the provision of services and products.

4. Categories of recipients of personal data

The controller provides personal data to the following categories of recipients:

(a) to persons or entities when performing duties imposed on the controller under specific legislation, including, without limitation, the **Banking Act**, i.e. primarily to courts, law enforcement and criminal justice authorities, tax authorities, bailiffs and enforcement officers, the Financial Arbitrator, social security bodies, and oversight bodies in the discharge of their statutory powers, or external auditors, and also under the **Anti-Money Laundering Act**.

(b) under the **Banking Act** the controller has the authority to obtain personal data and provide it to other banks, either directly or via third parties established to maintain client registers.

(c) to suppliers and administrators of information systems, and to security service providers and administrators in accordance with the Cybersecurity Act and the EU Regulation on the digital resilience

of the financial sector, i.e. entities contracted by the controller to process personal data which provide sufficient guarantees that technical and organisational measures are in place to protect the data provided (**"processors"**).

(d) to other entities, where required for the provision of services and products provided by the controller (for example the performance of payments and operations using payment cards and digital wallets), and to protect the controller's rights and legally protected interests, to the extent necessary for the assertion of its claims.

(e) to other entities under the conditions of binding legal regulations or with an individual's consent.

5. Potential for the controller to transfer personal data to third countries or international organisations

In connection with the processing purposes described above, the controller may provide personal data to relevant recipients (typically these are external entities such as providers of IT services, whom it contracts to process personal data, courier or archiving services, foreign securities registers, correspondent banks, etc.) in third countries (i.e. countries that are not EU/EEA Member States), exclusively within the scope permitted and requirements stipulated by applicable law and regulations; the controller exercises due consideration to select as processors only entities offering it the highest guarantees that technical and organisational measures are in place to protect the personal data transferred.

6. Duration of personal data processing

The controller is required to retain processed personal data for the period prescribed by applicable legislation, which is generally for the duration of the contractual relationship between the controller and an individual, or an entity represented by an individual, plus up to 10 years following the end of the calendar month in which the last action within the transaction was executed or that transactional relationship was terminated (unless binding regulations lay down another period), or up to 10 years following the performance of all relevant financial commitments to the controller under established contractual relationships, or, where data are associated with the keeping of investment instrument records, up to 10 years from the end of the calendar year in which the data are recorded (unless binding regulations lay down another period).

7. Processing of personal data with consent

In situations where personal data are not processed by the controller for statutory reasons or on other legal grounds, such as the controller's legitimate interests, the processing of such personal data is subject to the individual's consent as the legal grounds (**"processing subject to consent"**). In cases of processing subject to consent, it is entirely at the discretion of the individual whether such personal data may be processed by the controller. Data subjects have the right to withdraw their consent at any time.

Where processing is subject to consent, if personal data necessary for fulfilment of the purpose of processing are not provided to the controller, or that consent is (partially or fully) withdrawn, the controller may not be able to carry out the specified purpose of such processing.

8. Information on other rights of individuals as data subjects

8.1 Access to personal data

Individuals have the right to request the controller, or the processor directly, for information on the processing of their personal data, and this must be provided to them without undue delay. In all cases that information must state: (i) the purpose of personal data processing; (ii) the personal data and/or categories of personal data subject to processing, including all information available on their sources; and (iii) the recipient and/or categories of recipients. Where individuals make requests electronically, unless requested otherwise the information must be provided in a commonly used electronic form. For the provision of this information the controller, or a processor acting on the controller's behalf, may charge a reasonable fee not exceeding the costs required to provide the information.

8.2 Right to the rectification of personal data and the possibility of lodging a complaint with a supervisory authority

If individuals discover or suspect that the controller or a processor is processing their personal data in a way that is contrary to the protection of their private and personal life or that is in contravention of the law, in particular where the personal data are inaccurate in relation to the purpose of processing, they may: (i) demand an explanation from the controller or processor; or (ii) demand that the controller or processor rectify the situation. In particular, this may entail the blocking, rectification, supplementation or erasure of the personal data in question. If such a request is found to be justified, the controller or processor must immediately remedy the situation. If the controller or processor does not comply with a request, individuals may contact the Office for Personal Data Protection (*website: www.uoou.cz*).

8.3 Right to the erasure of personal data

Individuals are entitled to have the controller erase relevant personal data without undue delay for any of the following reasons:

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

(b) the individual withdraws consent, if processing is subject to consent, and there are no other legal grounds for the processing;

(c) the individual objects to the processing pursuant to Article 21(1) of the GDPR and there are no overriding legitimate grounds for the processing, or the individual objects to the processing pursuant to Article 21(2) of the GDPR;

(d) the personal data have been processed unlawfully;

(e) the personal data must be erased for compliance with a legal obligation under European Union or EU Member State law to which the controller is subject.

The foregoing regarding the right to erasure does not apply to the extent that personal data processing is necessary:

(a) for exercising the right of freedom of expression and information;

(b) for compliance with a legal obligation that requires processing under European Union or EU Member State law to which the controller is subject, or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

(c) for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) of the GDPR;

(d) for the establishment, exercise or defence of legal claims.

8.4 Right to the restriction of personal data processing

Individuals have the right to obtain from the controller restriction of processing where any of the following applies:

(a) the accuracy of the personal data is contested by the individual, for a period enabling the controller to verify the accuracy of the personal data;

(b) the processing is unlawful and the individual 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 processing, but requests them for the establishment, exercise or defence of legal claims;

(d) the individual has objected to processing pursuant to Article 21(1) of the GDPR pending verification whether the legitimate grounds of the controller override those of the individual.

Where processing has been restricted under the sub-paragraphs above, such personal data may, with the exception of storage, be processed only with the individual's consent or for the establishment, exercise or defence of legal claims, for the protection of the rights of another natural or legal person, or for reasons of important public interest of the European Union or of an EU Member State.

The controller must communicate any rectification or erasure of personal data or restriction of processing to each recipient to whom the personal data have been disclosed, unless this proves impossible or involves disproportionate effort.

8.5 Right to data portability

Individuals have the right to receive personal data concerning them, and which they have provided to the controller, in a structured, commonly used and machine-readable format, and the right to transmit such data to another controller without hindrance from the controller, provided that the processing is carried out by automated means. In exercising their right to data portability under the preceding sentence, individuals have the right to have the personal data transmitted directly from the controller to another controller, where technically feasible.

8.6 Right to object

Individuals have the right to object, on grounds relating to their particular situation, at any time to the processing of their personal data on the basis of Article 6(1)(f) of the GDPR. The controller will no longer process such personal data unless it demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of individuals or for the establishment, exercise or defence of legal claims.

8.7 Right Not to Be Subject to Automated Decision-Making

An individual has the right not to be subject to a decision based solely on automated processing, including profiling or language models using generative/artificial intelligence (AI), which produces legal effects concerning him or her or similarly significantly affects him or her, unless otherwise provided by applicable law. - The Bank does not carry out such processing as part of its standard practices.

8.8 Notification of personal data breaches

Where a personal data breach is likely to result in a high risk to the rights and freedoms of individuals, the controller must communicate this breach to the individual without undue delay. Notification is not required, however, if any of the following conditions are met: (a) the controller has implemented appropriate technical and organisational protection measures, and those measures have been applied, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption; (b) the controller has taken subsequent measures ensuring that a high risk to the rights and freedoms of individuals is no longer likely to materialise; (c) disproportionate effort would be involved.

This information is available at PPF banka's registered office, client centres and on its website (*www.ppfbanka.cz*).

Individuals are informed of the rules on personal data processing and protection when they enter into a bank transaction or when a banking service is provided, as well as when negotiating and entering into relevant contractual relationships with the suppliers of the respective services or products.

8.9 Information on the right to lodge a complaint with the supervisory authority

The data subject has the possibility to lodge a complaint with the supervisory authority (the Office for Personal Data Protection) if he/she believes that the processing of his/her personal data has violated the rules of personal data protection at the following address:

Office for Personal Data Protection

Pplk.Sochora 27

170 00 Praha 7