Data Protection Policy

2019

Contents

1. General (introductory) provisions

In accordance with Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 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 (General Data Protection Regulation), OTP banka d.d., with head office in Split, Domovinskog rata 61, adopted the Data Protection Policy with goal of clear communication on how the Bank manages personal data protection.

The Bank, as the controller, with the following contact information:

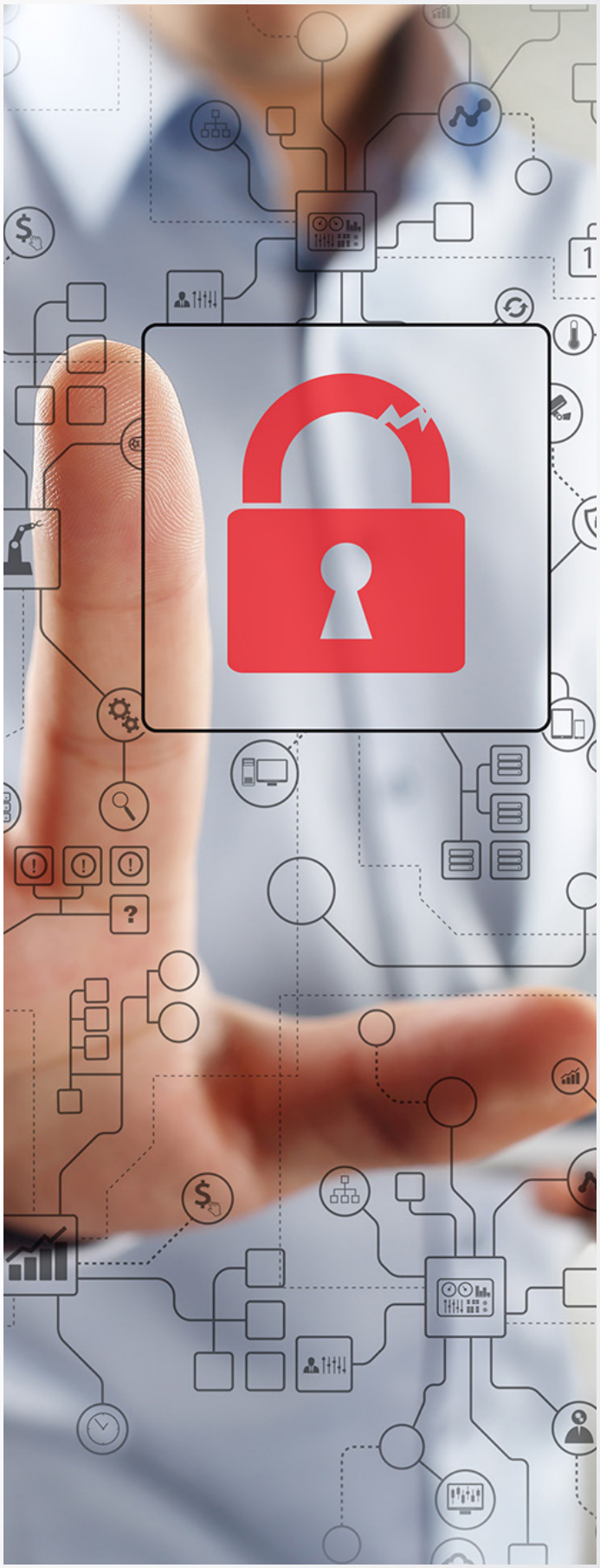
OTP banka d.d.,
Domovinskog rata 61, 21 000 Split,
Personal Identification Number (OIB): 52508873833,
Telephone: 0800 21 00 21,
E-mail: info@otpbanka.hr

shall collect, use, transmit and otherwise process personal data of its clients, employees and business partners and other natural persons whose identity can be determined directly or indirectly (hereinafter: Data subjects).

2. Principles of personal data processing

The General Data Protection Regulation provides for the following principles relating to the processing of personal data:

- **Lawfulness, fairness, transparency** – personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject;
- **Purpose limitation** – personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, in accordance with provisions of the General Data Protection Regulation providing for the safeguards and derogations relating to processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, shall not be considered to be incompatible with the initial purposes;
- **Data minimization** – personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- **Accuracy** – personal data shall be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
- **Storage limitation** – personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods in so far as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with the provisions of the General Data Protection Regulation providing for the safeguards and derogations relating to processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject;
- **Integrity and confidentiality** – personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures;
- **Accountability** - the controller shall be responsible for, and be able to demonstrate compliance with the mentioned principles.



3. Personal data processed and the purposes of the processing

Depending on the nature of their business relationship, the Bank may dispose of various personal data of the data subject. This includes identification and contact data, financial data, transaction data, data on contracted services and products and how they are used, socio-demographic data, data on the location and devices used to access the bank's applications, communication sent to the Bank through available channels, and documented (such as the copy of the ID card or passport) and publicly available data.

Privacy of the data subject is protected by European Union regulations, as well as by the regulations of the Republic of Croatia. The Bank processes personal data and may only use them for the purposes for which they were collected. Personal data processing is allowed only to the extent that at least one of the following conditions is met:

- Processing is necessary in order to comply with the Bank's legal obligations;
- Processing is necessary in order to execute the contracts the data subject is a party to or in order to take steps at the request of the data subject prior to entering into a contract;
- Processing is necessary for the purposes of legitimate business interests pursued by the Bank or a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data;
- The data subject has given his/her explicit consent based on the information on the extent of processing.

Data processed by the Bank are collected from the data subject when establishing a business relationship or in the course of a business relationship, from conversations with data subjects in branch offices, from the use of the Bank's web site and mobile phone banking application, from e-mails and letters and other documents, through the video surveillance system, from application forms for various products, from customer satisfaction polls, when concluding employment contracts with the employees and at participation in prize games or marketing campaigns of the Bank, as well as in the course of performing other operations for which the Bank is authorized.

The Bank processes data available during the data subject's use of the Bank's products and services, e.g. data on the amount, frequency, type and payee of transactions initiated by the client, data on the account balance, data on the frequency of using the Bank's products and other data the Bank may obtain during the use of the Bank's products and services.

At the time when personal data are collected, the Bank shall inform the data subject about the data it collects and the purposes and legal basis of processing.

If personal data are not obtained from the data subject, the Bank shall additionally inform the data subject about the categories of the subject personal data, the source of personal data and whether such data originate from publicly accessible sources.

The data subject shall receive the above information:

- within a reasonable period after obtaining the personal data, but at the latest within one month, having regard to the specific circumstance in which the personal data are processed;
- if the personal data are to be used for communication with the data subject, at the latest at the time of the first communication with that data subject; or
- if a disclosure to another recipient is envisaged, at the latest when the personal data are first disclosed.

4. Processing personal data based on the consent of the data subject

In certain cases, where the provision of data is not necessary for the establishment or continuation of a business relationship with the data subject, the Bank may request the data subject's consent for the processing of personal data for certain purposes. Where the processing of the data subject's personal data is based on consent, the data subject can withdraw the consent at any time, which shall however not affect the lawfulness of the processing based on consent before it was withdrawn. Withholding consent or subsequent withdrawal thereof shall not affect the possibility of concluding a contractual relationship with the Bank nor result in the termination of an existing contractual relationship with the Bank.

5. Processing personal data based on legitimate interest

According to General Data Protection Regulation the Bank has assessed and defined its legitimate interests, taking into consideration rights and freedoms of data subjects. The relevant legitimate interests relate to:

- Data processing with purpose to protect persons, property, work environment and ensure safety of all persons in business premises of the Bank and external ATMs, including video surveillance and record of visitors.
- Data processing with purpose to prevent and investigate fraud or other criminal offenses and all types of misuse of bank's services.
- Data processing with purpose of transparency, traceability and consumer protection, also including audio records.
- Data processing with purpose of detailed analysis of credit exposure, including shared credit exposure of client and his/her spouse regarding the Bank, and processing related to requests for clients with high risk indicator, in aim of minimizing manifestation of financial loss, and mitigating of potential operational, reputational and credit risk in order to improve long-term quality of credit portfolio.
- Data processing of public information in order to perform debt recovery activities.
- Data processing in terms of client segmentation with purpose to offer products and services to existing clients at Bank's sales point, through bank's service channels or inbound calls.
- Data processing for purpose of direct marketing when the offer is made for equal or comparable products and services of the Bank that data subjects already use, considered by the Bank as better suited to the needs of certain categories of clients or intended as easier access or product /service management, as much as data subjects don't oppose this processing.

Processing of data in cases of legitimate interest does not require consent of data subject. However, data subjects can use their rights as described in chapter 10.

6. Special categories of personal data

Personal data falling under a special category are considered to reveal racial or ethnic origin, political opinion, religious or philosophical beliefs or trade union membership. This category includes genetic data, biometric data for the purpose of identifying the data subject, data concerning health or data concerning a natural person's sex life or sexual orientation. These data shall not be processed except in cases where the data subject has given his/her explicit consent for such a processing or in other cases prescribed by the General Data Protection Regulation.

7. Personal data recipients/categories of recipients

Personal data provided to the Bank by the data subject or available to the Bank based on its business relationship with the data subject may be rendered accessible or transmitted to business partners of the Bank (Data Processors) based on contract. Data Processors provide various services to the Bank in order to enable the Bank to carry out its activities (e.g. IT support, marketing cooperation, recovery activities, legal assistance, procurement of goods and services for the Bank's requirements etc.). The Bank also exchanges personal data within its banking group and other business partners (e.g. insurance companies) when offering their products and services based on a business relationship with them, where such exchange is necessary in order to provide the requested product or service to the client.

Personal data of the data subject can be also transmitted to the Ministry of Finance, Croatian National Bank, Financial Agency, Croatian Financial Services Supervisory Agency or another competent body for the purpose of submitting reports or meeting other legal requirements, when the requirement of sending such data has been prescribed by the law, and other recipients in accordance with Article 156 and Article 157 of the Credit Institutions Act regulating the banking secrecy and exceptions to the banking secrecy obligation.

8. Data retention period

Pursuant to the article 160 Credit Institutions Act (OG 159/13, 19/15, 102/15, 15/18), the Bank shall store for a period of at least eleven years documents relating to the opening, closing and recording of changes in payment accounts and deposit accounts, documents relating to other changes not covered on the basis of which data have been entered in the credit institution's business books, contracts and other documents relating to the establishment of a business relationship. The time limit referred to shall mean the period following the end of the year in which the business change occurred, i.e. in which bookkeeping documents were prepared. Where such documents relate to long-term business activities, they shall be kept for the duration of the business relationship and at least eleven years following the end of the year in which the business relationship was terminated. The Bank shall also keep the data subject's personal data 10 years from the occasional transaction that amounts to HRK 105,000.00 or more, or 10 years from the occasional transaction that constitutes a transfer of funds exceeding EUR 1,000.00, or the data on other transactions, within the meaning of the Anti-Money Laundering and Terrorist Financing Act (OG 108/17).

In certain cases, the Bank may keep the data subject's personal data for a shorter or longer period than above mentioned, depending on the purpose of data processing and the nature of the business relationship with the Bank.

9. Marketing purposes

If the Bank has obtained the explicit consents given freely by the data subjects, it may use the personal data to inform the data subjects about its products, services and offers that might be important or interesting for them.

The data subject may at any time request the Bank to stop sending marketing information.

10. Rights of the data subject

Right to information
The data subject shall have the right to information regarding the processing of his or her data. Communication regarding personal data processing to the data subject shall be always provided in concise, transparent, intelligible and easily accessible form, using clear and plain language.

Right to erasure (Right to be forgotten)
The data subject shall have the right to obtain the erasure of personal data if one of the following conditions is met:

- the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
- the data subject withdraws consent on which the processing is based;
- the data subject objects to processing of personal data based on the legitimate interest of the Bank or a third party, including profiling based on such grounds, and to processing of personal data for marketing purposes, which includes profiling to the extent that it is related to such direct marketing. In the former case, data shall not be erased if the Bank's legitimate interest overrides the interests, rights and freedoms of the data subject or where they are necessary for the establishment, exercise or defence of legal claims;
- the personal data have been unlawfully processed;
- the personal data have to be erased for compliance with legal obligations further to other legal regulations.

Right to access
The data subject has the right to request from the Bank the access to personal data and detailed information on how his/her personal data are processed at any time. The exercise of the right to access data shall not adversely affect the rights or freedoms of others.

Right to rectification
The data subject shall have the right to obtain from the Bank the rectification of inaccurate personal data. The data subject shall also have the right to complete personal data, which can be made by means of providing a supplementary statement. The Bank shall take the necessary measures reasonably expected from it, to verify the accuracy of data and to rectify them.

Right to lodge an objection with the competent body
The data subject is entitled to file a complaint with the supervisory body, Croatian Personal Data Protection Agency, Martićeva ulica 14, 10 000 Zagreb.

Right to restriction of processing
The data subject is entitled to obtain restriction of processing where one of the following applies:

- the accuracy of the personal data is contested by the data subject, for a period enabling the Bank to verify the accuracy of the personal data;
- the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead;

- the Bank 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;
- the data subject has objected to processing based on legitimate interest, including the profiling based on such data, pending the verification whether the legitimate grounds of the controller override those of the data subject.

A data subject who has obtained restriction of processing shall be informed by the Bank before the restriction of processing is lifted.

Right to data portability

The data subject shall also have the right to portability of his or her personal data. This means that the Bank can provide the data subject's personal data at the data subject's request in a structured, commonly-used and machine-readable format and the data subject shall have right to transmit those data to another controller provided that the processing is based on consent or necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract or where the processing is carried out by automated means. In exercising his or her right to data portability, the data subject shall have the right to have the personal data transmitted directly from one controller to another, where technically feasible.

Right to object

The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her, when the data is processed based on the legitimate interest of the Bank or a third party, including profiling based on such grounds. In this case, the Bank shall no longer process the personal data unless it demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defense of legal claims.

Moreover, where personal data are processed for direct marketing purposes, the data subject shall have the right to object at any time to processing of personal data concerning him or her for such marketing, which includes profiling to the extent that it is related to such direct marketing, in which case the Bank may no longer process data for such purposes.

Rights related to the automated decision-making and profiling

In certain cases, the Bank uses the systems for the automated-decision making based on the available personal data. Such processing enables quick, fair and efficient decision-making.

The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her, unless such decision is necessary for entering into, or performance of, a contract between the data subject and the Bank, or it is authorized by another law, or based on the data subject's explicit consent.

11. Protection of privacy

11.1. Data security

The Bank takes adequate technical and organizational measures to ensure the necessary security of data. These measures relate in particular to computers (servers and work stations), networks, communication links and applications, and are a part of the Bank's IT security system.

The essential measures taken in the Bank in order to avoid the unauthorized processing of personal data, include, among other things, the following:

- control of physical access to the data processing systems;
- control of logical access to the data processing systems;
- control of logical access to the data processing applications;
- control of data entry to the processing data systems;
- control data transfer in the data transfer systems.

Additionally, adequate measures must be taken to protect such data from accidental and unauthorized deletion and loss.

Only authorized employees acquainted with the data confidentiality conditions are involved in the data processing. They are not allowed to use such data for personal purposes or disclose such data to any unauthorized party. In this context, unauthorized parties are considered be all also employees who do not need access to such data for completion of their work assignments. The confidentiality obligation remains in force even after the termination of the employment contract.

11.2. Technical and organizational measures

Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons, the Bank shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

- the pseudonymisation and encryption of personal data;
- the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
- a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.

11.3. Notification of a personal data breach to the supervisory authority

In the case of a personal data breach, the Bank shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the competent supervisory authority, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons.
Personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed.

11.4. Communication of a personal data breach to the data subject

When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the Bank shall communicate the personal data breach to the data subject without delay.

The communication to the data subject shall not be required if any of the following conditions are met:

- the Bank has implemented appropriate technical and organizational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorized to access it, such as encryption;
- the Bank has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects referred to in paragraph 1 is no longer likely to materialize;
- it would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.

10.1. Data protection impact assessment

According to the General Data Protection Regulation, where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the Bank shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks. The controller shall seek the advice of the data protection officer when carrying out a data protection impact assessment.

A data protection impact assessment shall in particular be required in the case of:

- a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;
- processing on a large scale of special categories of data or of personal data relating to criminal convictions and offences or
- a systematic monitoring of a publicly accessible area on a large scale.

The assessment shall contain at least:

- a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller;
- an assessment of the necessity and proportionality of the processing operations in relation to the purposes;
- an assessment of the risks to the rights and freedoms of data subjects; and
- the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with the General Data Protection Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned.

11.6. Records of processing activities

The Bank is pursuant to the General Data Protection Regulation required to maintain a record of processing activities. That record shall contain all of the following information:

1. the name and contact details of the controller and, where applicable, the joint controller, the controller's representative and the data protection officer;
2. the purposes of the processing;
3. a description of the categories of data subjects and of the categories of personal data;
4. the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organizations;
5. where applicable, transfers of personal data to a third country or an international organization, including the identification of that third country or international organization and, subject to conditions defined by the General Data Protection Regulation, the documentation of suitable safeguards;
6. where possible, the envisaged time limits for erasure of the different categories of data;
7. where possible, a general description of the technical and organizational security measures referred to in clause 11.2 of the Policy.

12. Data protection officer

In line with the General Data Protection Regulation, the Bank designates a data protection officer. This function includes continuous efforts to implement and improve a comprehensive and efficient system for monitoring the compliance with the General Data Protection Regulation, corresponding to the nature, scope and complexity of data processing carried out by the Bank.

Tasks of the data protection officer are informing and advising the Bank, the processor and the employees of their obligations pursuant to the General Data Protection Regulation and other data protection provisions, monitoring the compliance with this Regulation, and with other provisions and the Policy of the Bank, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits; provision of advice where requested as regards the data protection impact assessment, cooperation with the supervisory authority, and other tasks defined by the General Data Protection Regulation and other internal documents of the Bank. The data protection officer shall be bound by secrecy or confidentiality concerning the performance of his or her tasks.

Contact details of the data protection officer of the Bank are public and communicated to the relevant supervisory authorities.

13. Contact details

If a data subject should have any questions regarding the processing of his or her data by the Bank or would like to file a complaint regarding personal data processing, the data subject may contact:

In writing:
Data Protection Officer of OTP banka d.d.
Domovinskog rata 61, 21000 Split

or via e-mail:
zastita-osobnih-podataka@otpbanka.hr.

The data subject may also request access to personal data or exercise any other right referred to in clause 9 of this Policy by completing the form enclosed hereto and delivering it directly to the data protection officer using the contact details above, or submitting it at any of the branch offices of the Bank.

Pursuant to the General Data Protection Regulation, the Bank shall provide information to the data subject on action taken on a request without undue delay and at the latest within one month of receipt of the request.

That period may be extended by two further months where necessary, taking into account the complexity and number of the requests. The Bank shall inform the data subject of any such extension within one month of receipt of the request, together with the reasons for the delay.

If the Bank does not take action on the request of the data subject, the Bank shall inform the data subject without delay and at the latest within one month of receipt of the request of the reasons for not taking action and on the possibility of lodging a complaint with a competent authority and seeking a judicial remedy.

14. Appendix

Request to Exercise the Right of the data subject

Details of the data subject requesting to exercise a right regarding personal data protection[1]	
Name	
Personal Identification Number (OIB)	
Permanent residence address	

Personal data protection right you wish to exercise (please circle)
1. Right to be forgotten 2. Right of access 3. Right to rectification 4. Right to restriction of processing 5. Right to data portability 6. Right to object 7. Rights related to automated decision-making, including profiling

Note

Date

Signature of the data subject

Request receipt data	
Request received on	
Name and signature of the employee	
Branch office / competent organisation unit of the Bank	

[1] Data collected in this template shall be used by the Bank for the exercise of the rights of the data subject pursuant to the General Data Protection Regulation (EU) 2016/679 and to respond to inquiries and complaints of the data subjects pursuant to the Bank's Data Protection Policy. The data is mandatory and the Bank will not be able to respond to the data subject's request if data are withheld. The collected data shall be considered secret and treated by the Bank in compliance with the data confidentiality obligation. Data shall be retained for a period of 5 years. All other information which the Bank is obliged to provide to the data subject under the above Regulation are included in the Bank's Data Protection Policy, which is published on the Bank's website and available in all branch offices of the Bank.