



PERSONAL DATA PROTECTION POLICY

Ver. 300421

I INTRODUCTORY PROVISIONS

OTP banka Srbija a.d. Novi Sad, Trg Slobode no. 5, Novi Sad (hereinafter referred to as “**the Bank**”) handles personal data of natural persons which it processes in line with applicable regulations, i.e. pursuant to the Law on Personal Data Protection ("RS Official Gazette", no. 87/2018, hereinafter referred to as: the Law) and Regulation (EU) 2016/679 of the European Parliament and of the Council as of 27th 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 (in cases when applicable).

The Bank processes personal data in accordance with the Personal Data Protection Policy (hereinafter referred to as: Policy) and General Terms and Conditions.

II GENERAL PROVISIONS

2.1. Document purpose and main terms

The present Policy aims to clearly, in an understandable and easily accessible manner explain what personal data we collect, for what purpose, how we protect such data and how you may exercise your rights. In order to be fully aware of the rights you have and manner of exercising such rights, it is required that you know the following definitions of certain terms herein:

- Personal data processing means each action performed in an automated or non-automated way with personal data or sets thereof, such as collecting, using, recording, sorting, grouping i.e. structuring, storing, adjusting, modifying, detecting, transmitting, submitting, giving for insight, copying or duplicating, comparing, limiting, deleting or destroying, performed directly by the Bank or through its partners and related parties.
- Personal data is each data pertaining to a natural person whose identity has been established or can be established, directly or indirectly (hereinafter referred to as personal data).
- Person to whom data pertain is each natural person (individual) whose personal data are processed by the Bank.
- Special type of personal data are personal data revealing racial or ethnic origin, political opinion, religious or philosophical beliefs or union membership, as well as the processing of genetic data, biometric data for the sole identification of a person, health information or sexual life or sexual orientation data of a natural person.

2.2. Scope of application

The Policy shall be applied to all personal data of a Bank’s Client that are processed by the Bank, i.e. for which it determined the manner of processing and purpose, as well as to other persons stated in this Item.

The Policy shall be applied to all services and products of the Bank that involve personal data processing. if the legal ground for processing of data is consent, the last expression of will of a person to whom data pertain,

by which such person gives consent to personal data processing, shall be applied to all services and products of the Bank which are used by that person.

The Policy is primarily intended for and pertains to:

1. Natural persons submitting an application or who are using services and products of the Bank (hereinafter referred to as: **Client**):
 - 1) Natural persons submitting an application or who are using services and products of the Bank on their behalf and for their account;
 - 2) Natural persons establishing relationship with the Bank on behalf legal entities, organisations, associations and other organisational forms which may enter into a contractual relationship with the Bank (authorised representatives, procura holders, legal representatives, proxies, etc.)
 - 3) Natural persons (legal representative, parent, guardian, protector, authorised representative, signatory) who represent, or act on behalf of persons stated in Item 1),
 - 4) Inheritor of a person stated in Item 1),
 - 5) Other natural persons (e.g. unconditional guarantor, owner or beneficial Client of real estate serving as collateral, dependent person, other persons in common household, Client) who are exercising rights, i.e. for whom conclusion of an agreement with the Bank or utilisation of its products creates certain liabilities.
2. Natural persons who are interested in using services and products of the Bank (hereinafter referred to as: **Prospective Client**),
3. Other natural persons whose data the Bank comes into possession in the course of its operations in accordance with applicable statutory regulations.

The Policy shall not be applied to anonymised data i.e. to data based on which the identity of a person is neither directly or indirectly determinable. An anonymised data is a data which has been modified in such a way that it cannot be linked to a certain natural person, in line with applicable regulations, it shall not be deemed as personal data.

The Bank processes personal data for various purposes, while the means of collection, legal grounds for processing, utilisation, disclosing and timeframes for keeping thereof may differ depending on the purpose.

III DETAILED PROVISIONS

3.1. What personal data does the Bank process?

The Bank collects and processes the following categories of personal data:

- 1.1. Information contained in agreements with Clients and application forms of Prospective Clients.

The personal data that are contained in agreements/application forms from the pre-contractual phase, which are necessary for the provision of a service, fulfilment of contractual liability or conclusion of agreement. This can imply processing of the following data: name and surname, unique personal identification number, name

of one parent, address of residence, citizenship, number of identification document, place and date of issuing identification document, country of birth, telephone number (landline, mobile), address for sending mail, contact details, details on the manner and history of paying services (amount of debt, existence of a standing order, current account number and similar), details from account specification, etc.

- 1.2. Financial data – details on earnings, other income of person’s household, details on other accounts and liabilities, details from the Credit Bureau of the Association of Banks, account number, card number, batch number, insurance policy number, to whom data pertain, details on tax residency and tax identification number etc.;
- 1.3. Property details (for certain types of placements) – real estate and movable assets in the ownership of the person to whom data pertain;
- 1.4. Special type of personal data – political affiliation (status of official), data on disability (in order to determine income of a person or employee qualifications), details on whether criminal proceedings have been initiated against the person (if it is the case of employees in order to fulfil regulatory requirements in accordance with regulations);
- 1.5. Information on spouse – details on employment of a spouse, number of children, number of household members;
- 1.6. Details on related persons – relatedness based on management function, relatedness based on kinship and other relatedness in accordance with the Law;
- 1.7. Details required for credit products – activities and business activity, data on employer, including employment agreement, credit history, prior use of banking products, and similar.
- 1.8. Information submitted by Clients and/or Prospective Clients by completing corresponding forms on our website.
This includes data obtained for the purpose of creating accounts to access web pages, portals and applications of the Bank, subscriptions to the *newsletter* (monthly brochure), when sending inquiries, when lodging claims or complaints, sending requests, for additional services such as, including but not limited to, participation in competitions, promotions and similar. Personal data that are processed for these purposes may include but are not limited to: name, surname, address, mobile phone number, landline phone number and e-mail address.
- 1.9. Information contained in records on communication and correspondence in situations related to establishment of contact by the Client, Prospective Clients and other natural persons.
These data include recordings of conversations with the Contact Centre, written or electronic communication.
- 1.10. Information collected from the Client and which are processed in order to enhance communication, transfer contacts, and with the aim of raising quality of products and services.
This includes data on professional interests, experience in using services of the Bank, database containing landline telephone number, name and surname and address of residence, used by the service for searching telephone numbers and details on owners thereof, so called “white pages”.
- 1.11. Data of Clients, Prospective Clients and/or other natural persons from surveys used for research purposes, if persons wished to be surveyed.
- 1.12. Data on visits to our internet portals and data on resources being accessed or downloaded.

These data are processed in accordance with the General Terms and Conditions and Privacy Policy, available by way of this link https://www.otpbanka.rs/pravila_privatnosti

- 1.13. Information collected and processed by the Bank for the purpose of direct marketing and profiling, by virtue of a freely given consent of a person to whom data pertain.
This implies processing of the following personal data: name and surname, e-mail address, manners of using Bank's services and other details. Only in exceptional cases shall the Bank process personal data by virtue of consent because the processing is largely based on other legal grounds (statutory obligation or contractual relationship).
- 1.14. Information collected for the purpose of fulfilment of statutory obligations.
This implies personal data which the Bank is obligated to collect, keep and process in accordance with the applicable laws of the Republic of Serbia and submit to competent state bodies (courts, state authorities, investigative authorities and similar).
- 1.15. Other information collected in order to realise a certain legitimate interest of the Bank.
When personal data are processed by virtue of legitimate interest, the Bank shall, with special care, take into consideration the impact of processing on rights and freedoms of persons to whom data pertain. Legitimate interests of the Bank are not assumed by interests of the persons to whom data pertain. In the event that in relation to the legitimate interest of the Bank there exist prevailing interests or fundamental rights and freedoms of persons to whom data pertain which require personal data protection, and especially if the person to whom data pertain is a minor, the Bank will not process data, save for if it receives an explicit consent from the person to whom data pertain, i.e. consent of a parent exercising his/her parental right, i.e. other legal representative of the minor in accordance with the relevant regulations.

As a rule, the Bank shall not process special types of personal data. Exceptionally, the Bank may process these data solely if the person to whom data pertain gave its explicit consent in accordance with the Law, if such processing is necessary for execution of statutory obligations of the Bank, if it is in the capacity of protecting vital interests of the person to whom data pertain, if data are obviously available to the public, if processing is done with the aim of realising a legal claim, for the purpose of realising public interest defined by Law.

3.2. Manners of collecting personal data

The Bank collects personal data as follows:

- a) Directly from a Client or Prospective Clients**, direct submission by Client and/or Prospective Client (for example in submitting an application for a service at points of sale, in communication of the Client/Prospective Client with the Contact Centre or by way of web page and social networks, in submitting complaints and similar).
- b) Automatically when using products and services of the Bank.**
- c) From publicly available sources** such as, for example, data from publicly available services.
- d) By other handlers by virtue of corresponding contractual relationship.** In situations when another handler entrusts a certain activity of personal data processing to the Bank, by virtue of a previously concluded

agreement, the Bank in the capacity of a processor may process all those personal data entrusted to the Bank for processing by another handler.

Prerequisite for each collection of personal data is the existence of corresponding legal grounds in accordance with the Law.

3.3. Recording telephone conversations

The Bank is entitled to record telephone conversations with Clients and Prospective Clients and present telephone numbers in the following cases:

- calls received or performed from the Bank's Contact Centre;
- calls performed for the purpose of telephone sale of the Bank;
- calls performed for the purpose of management of Bank's receivables;
- calls for the purpose of adjusting details related to Bank's card and transactions on bank account;
- calls with reference to reporting on violation of personal data;
- in other cases when legal grounds exist in accordance with the Law.

In order to maintain balance between the position of a Client/Prospective Clients and the Bank, the Client/Prospective Client who is conducting the telephone conversation may also record the conversation. This activity by the Client may be only for the same purpose due to which the Bank is recording the conversation. In the beginning of the conversation the Bank is obligated to notify the Client/Prospective Client that the conversation is being recorded. The Client/Prospective Client may not publish the audio recording made by the Bank or the very Prospective Client, and he/she may use it solely during a potential legal dispute with the Bank. In case of dispute, the Bank shall, in all cases, take into consideration the audio recording which it created.

3.4. Principles of processing personal data

The Bank shall perform personal data processing in a lawful, transparent and fair manner by conducting the following activities:

- The Bank shall inform the persons to whom data pertain on the purpose of processing and legal grounds for processing in a clear, simple and transparent way;
- Only necessary data processing shall be conducted, namely with the aim of realising the agreement being concluded with the person to whom data pertain (e.g. Clients, Prospective Clients, engaged associates and similar), then processing required by corresponding statutory regulations and which represents a statutory obligation of the Bank as the handler, processing necessary in order to realise legitimate interest of the Bank, but only in events when such interest is prevailing in relation to the interest of the person to whom data pertain, as well as processing performed by virtue of explicit and freely given consent of a person to whom data pertain.

The Bank shall process personal data for the purposes that are specifically determined, explicit, justified and lawful. Personal data may not be further processed in a manner which is not in accordance with such purposes.

In collecting personal data the Bank shall adhere to the principle of minimum scope of data, hence only such personal data that are required for fulfilling the purpose for which they are processed shall be collected from persons to whom data pertain. Should additional personal data be required, they shall be collected with the consent of the person to whom data pertain.

The Bank shall ensure accuracy of personal data by applying technical and organisational measures and periodical updating of data.

Timeframes for data keeping are determined by internal acts of the Bank, namely in a manner that data are kept within a timeframe necessary for realising the purpose of processing and in line with statutory requirements.

The Bank shall observe the principle of integrity and confidentiality of personal data. The Bank has implemented technical and organisational measures for personal data protection following thereby statutory provisions, good business practice and internationally recognised standards.

The Bank may engage a processor for personal data processing, namely by virtue of an agreement which, inter alia, also governs duties of the processor in terms of personal data protection.

3.5. Timeframes for keeping personal data

Personal data shall be kept as long as necessary to realise the purpose of processing, save for if applicable regulations do not envisage a longer or shorter timeframe for a certain purpose or in other cases explicitly prescribed by Law. After this, details shall be permanently deleted or anonymised. In the event of processing personal data upon expiry of the timeframe for keeping thereof (for example forming a base of historical data for the purpose of drawing up statistical analyses), the Bank shall anonymise personal data (permanently) in a manner in which it is not possible to identify a natural person to whom personal data pertain.

Timeframes for keeping personal data are prescribed by the internal rulebook governing protection and processing of archive and registry material, in accordance with the Law regulating the given area.

3.6. Purpose of processing personal data

The Bank shall process personal data of a person to whom data pertain only when such processing is lawful. Processing is lawful in the following cases:

- a) Processing is necessary for execution of agreement concluded with the person to whom data pertain or to undertake actions upon a request of the person to whom data pertain prior to conclusion of agreement. With the aim of providing services to Clients, the minimum set of data shall be processed necessary for provision of an individual service, i.e. sale of product. Otherwise, i.e. if the person to whom data pertain refuses to submit the requested set of data, the Bank will not be in the possibility to conclude an agreement with the Client and enable use of product or service. The minimum set of data implies the use of data for the purpose of verifying identity of Client and/or Prospective Client, as well as the use of contact and financial data of the person, for the purpose of account submission, assessment of financial solvency, calculation and collection of costs, submission of ordered products, contacting related to rendering of the service, verification

and creating technical possibilities for realising the service, installation of devices, corrections and removal of impediments, customer support and other actions related to conclusion and execution of agreement.

- b) Processing is necessary in order to observe statutory obligations of the Bank (applicable statutory regulations according to which the Bank must act).
By virtue of a written request based on applicable statutory regulations, in certain situations the Bank is obligated to submit or enable to competent state bodies (e.g. courts, police, etc.) access to certain Client's personal data.
- c) Processing is necessary for the purpose of realising legitimate interests of the Bank or third party, except if interests or basic rights and freedoms of a person to whom data pertain, which require personal data protection, are stronger from such interest, and in particular if the person to whom data pertain is a minor. Legitimate interest of the Bank implies processing which serves to enhance the process, for product development and enhancement of operations, modernising services, offering products and services for which it is expected to enhance operations with Clients. This for example, may include the use of Client's data to prevent, detect and process misuses to the detriment of the Client or of the Bank, to protect property of the Bank, create services and offers satisfying needs and wishes of Clients, market research and analysis etc.
- d) The person to whom data pertain gave its consent for processing of his/her personal data for one or more specially determined purposes, whereby such consent must be demonstrable and voluntary, written in an easily understandable language, while the person to whom data pertain is entitled to withdraw his/her consent at any moment.
- e) Processing is necessary for the purpose of vital interests of the person to whom data pertain or another natural person.
- f) Processing is necessary for the purpose of executing affairs in public interest or execution of authorisations of the Bank as prescribed by Law.

3.7. Automated decision-making

Decision-making by virtue of automatic data processing, including profiling, is an integral part of operations of the Bank, and is conducted in accordance with the:

- a) applicable laws;
- b) execution of contractual obligations;
- c) explicit consent of the person to whom data pertain;
- d) legitimate interests of the Bank.

The person to whom data pertain is entitled that the decision which was made exclusively based on automatized processing, including profiling, is not applied to him/her, if legal consequences upon such person arise by that decision or if such decision significantly impacts his/her position, except if that decision:

- 1) is necessary for conclusion or execution of agreement between the person to whom data pertain and the handler;
- 2) is based on law, if such law prescribes corresponding measures of protecting rights, freedoms and legitimate interests of persons to whom data pertain;

3) is based on explicit consent of the person to whom data pertain.

The Bank shall not reach decisions based on automatic data processing if such decision is based on automatic processing of special types of personal data except if the person has given his/her explicit consent or if such data are obviously available in the public. In the event that the person has given his/her explicit consent, the Bank shall apply enhanced measures of protecting these types of data.

In line with the Law, the Bank shall enable to persons to whom data pertain to exercise the right to object to automatic processing, including profiling. The objection may be submitted either in relation to initial or further processing, at any time and free-of-charge.

3.8. Access to personal data and personal data transfer

Access to personal data shall be given only to employees of the Bank, as well as to associates engaged in accordance with the affairs they perform based on corresponding authorisations set by the Bank and only to the extent which is minimally required, with the obligation of acting in accordance with the normative acts of the Bank governing the personal data protection area.

Personal data shall be available to third parties outside the Bank only in the following cases:

- if there is a statutory obligation or explicit authorisation based on law (e.g. court request);
- if for executing certain affairs a third person, i.e. subcontractor (processor) has been engaged, whereby such processor shall act solely in accordance with and upon the order of the Bank, and the Bank shall ensure all data protection measures as if it was performing these affairs on a standalone basis;
- to related companies of the Bank providing that legal grounds (consent of the person or legitimate interest) exist for such transfer or access;
- if data should be forwarded to execute the agreement;
- Banking group members;
- other persons outside the Bank for which there is an explicit consent of the person to whom data pertain.

As a rule, the Bank shall process Client's personal data in the Republic of Serbia. Exceptionally, the Bank may process personal data in other countries or international organisations as well, which ensure an appropriate personal data protection level (e.g. when a subcontractor from another country is engaged for the provision of a certain service or portion of a service involving personal data processing).

It is deemed that the appropriate protection level has been ensured in countries and international organisations which are members of the Council of Europe Convention on the protection of persons in relation to automatic personal data processing, i.e. in countries, in parts of their territories or in one or more sectors of certain activities in those countries for which the European Union determined that they ensure the appropriate level of protection or in the case when the Republic of Serbia concluded an international agreement on personal data transfer with another country or international organisation.

3.9. Security and personal data protection

Personal data should be treated as a business secret of the Bank and are accordingly classified as confidential, i.e. strictly confidential details. In accordance with their classification, adequate protection measures shall be applied thereto which protect these data from violation, unauthorised access, accidental loss, destruction, damage, hence any other threat to security. Technical and organisational measures such as control of access right, establishing and implementing the information security policy and other appertaining internal acts, establishment of a system of segregation of responsibilities, establishment and ensuring fulfilment of confidentiality liability and harmonisation with the Law of all third parties having access to personal data in the information system of the Bank, application of methods of monitoring access and activities in the information systems, as well as the application of software solutions for protecting information resources, shall be applied for such purposes.

The Bank has an implemented system for information security management and established adequate measures for protection of confidentiality, integrity and/or availability of personal data within. In the event of breach of personal data which results in or may result in accidental or intentional destruction, loss, modification or unauthorised revealing of personal data in the course of processing thereof, which may cause high risk to the rights and freedoms of natural persons to whom data pertain, the Bank shall immediately upon becoming aware of such violation, without unnecessary delay, inform the Commissioner and person to whom data pertain in a clear and understandable way, mandatorily stating contact details of the authorised Personal Data Protection Officer, description of possible consequences as well as the description of measures undertaken. In the event of violation of personal data, the Bank will immediately undertake corresponding measures so as to prevent further damage to the rights and freedoms of persons to whom data pertain and to mitigate the consequences that arose from such violation.

3.10. Rights of persons to whom data pertain

Clients, Prospective Clients and other persons to whom personal data pertain, may exercise the following rights:

- a) **Right to access personal data** – the applicant for exercising this right is entitled to receive information on the existence of personal data processing pertaining to him/her, purpose of such processing, type of personal data being processed, recipients or categories of recipients to whom personal data are revealed or may be revealed, on timeframes for keeping personal data, on the existence of right to request a correction or deletion of personal data, i.e. right to restrict processing of such data, on the existence of right to submit a complaint to the Commissioner.
- b) **Right to correct personal data** – right to request correction of inaccurate personal data, as well as the right to supplement incomplete data.
- c) **Right to restrict processing** personal data in the following cases:
 - when accuracy of personal data is disputed, the Bank will temporarily restrict processing in the period which is sufficient to verify accuracy of personal data;
 - when there are no legal grounds for personal data processing, and the person to whom data pertain opposes to deleting data in order to submit, exercise or defend legal claim;

- The Bank no longer requires personal data for exercising the purpose of processing, but the person to whom data pertain requested them in order to submit, exercise or defend legal claim;
 - when a complaint is filed in respect of processing, but there is an ongoing assessment whether legal grounds for processing by the Bank prevail over the interests of such person.
- d) *Right to object*** pertains to the right of a person that he/she may at any time lodge a complaint to the Bank regarding legality of processing of their personal data which are established based on corresponding legal grounds for processing
- Upon receipt of a complaint the Bank will restrict processing pursuant to Item 10.3. and upon completing the assessment of the merits of the complaint, it will terminate with processing of data in respect of the person who submitted the complaint, unless if it presents that there are statutory reasons for processing that prevail over the interests, rights or freedoms of the person to whom data pertain or are in respect of submitting, exercising or defending a legal claim.
 - The person to whom data pertain is entitled to submit a complaint at any moment to the processing of his/her personal data that are processed for the requirements of direct advertising, including profiling, to the extent in which it is related to direct processing.
 - If the person to whom data pertain submits an objection to processing for the requirement of direct advertising, personal data may no longer be processed for such purposes.
- e) *Right to delete*** (“*right to forget*“) personal data pertaining to the person who submitted the request may be exercised in the following cases:
- personal data are no longer required for realising the purpose due to which they were collected or otherwise processed;
 - the person to whom data pertain recalls the consent based on which the processing was conducted, and there are no other legal grounds for processing;
 - the person to whom data pertain lodged a complaint to processing in accordance with the Law, and there are no other legal grounds for processing which prevail over the legitimate interest, rights or freedom of persons to whom data pertain;
 - data have been processed without a legal ground;
 - data must be deleted to fulfil the requirement under a legislation;
 - data have been collected regarding usage of information society company services.
- f) *Right of a person to transfer data*** means the right that the Bank receives data of a person (or obligation of the Bank) who previously submitted personal data to the Bank in a structured, usually used and electronically legible format, as well as the right that such data of the person to whom such data pertain are transferred from the Bank to another handler, where all following conditions are met:
- processing is based on consent, based on contract or article 17, paragraph 2 point 1 of the Data Protection Law,
 - data has been processed automatically .

g) Manner of exercising rights of persons to whom data pertain

Persons to whom personal data pertain may exercise their rights stated in part 11 of this Policy, by completing the requests for exercising rights.

You may receive the requests for exercising rights in any branch of the Bank or on a Bank’s website in the tab dedicated for data protection. The request being submitted must be legible and duly completed and signed. The signed Request for exercising the right of a person to whom data pertain shall be submitted to any branch of the Bank. The Bank shall respond to the request without delay, but no later within 30 days following receipt of complete and accurate request. Such deadline may be extended for another 60 days if necessary, taking into account the complexity and number of requests. The Bank shall inform the person to

whom data pertain on the extension of the timeframe and reasons thereof within 30 days following receipt of the request.

3.11. Contact details of Handler

Contact details of the Bank are:

Address: OTP banka Srbija a.d. Novi Sad, Trg Slobode no.7, Novi Sad
Contact Centre: 0800 23 23 22
e-mail: info@otpbanka.rs

3.12. Filing a complaint to the Commissioner for Information of Public Importance and Personal Data Protection / competent court

The supervisory body for personal data protection in the Republic of Serbia is the Commissioner for Information of Public Importance and Personal Data Protection, Bulevar kralja Aleksandra no. 15, Belgrade (in this text: Commissioner).

The person to whom personal data pertain is entitled to file a complaint to the Commissioner if he/she deems that processing of his/her personal data by the Bank is contrary to the provisions of the Law.

The person to whom personal data pertain is entitled to a court protection if he/she deems that, contrary to the Law, by processing his/her personal data by the handler or processor, his/her rights as prescribed by the Law have been violated. Submission of a lawsuit to the court shall not affect the right of this person to initiate other proceedings of administrative or court protection. The claim stated in this Item shall be submitted to the competent higher court.

3.13. Personal Data Protection Officer

You may exercise your rights with reference to personal data which the Bank processes on you in all branches. You may refer all additional questions pertaining to processing of your personal data, as well as questions related to exercising your rights to the Personal Data Protection Officer at: zastita_podataka@otpbanka.rs.