

Personal data processing policy
in Tinkoff Bank



TINKOFF

Contents

1.	Terms, definitions and abbreviations.....	3
2.	General provisions.....	3
3.	PD processing principles.....	3
4.	PD processing conditions.....	4
5.	Rights of the PD subject.....	5
6.	Obligations of the Bank.....	5
7.	Measures to ensure personal data security while processing.....	6

1. Terms, definitions and abbreviations

- 1.1. The following terms, definitions and abbreviations shall be used in this Personal data processing policy in Tinkoff Bank (hereinafter referred to as the “Policy”):

Bank, Tinkoff Bank	Tinkoff Bank
IS	Information security
ISM	Information security management
ITD	Information Technology Department
Personal data (PD)	Any information related directly or indirectly to an identified or identifiable individual (personal data subject)
Personal data subject	An individual, who is directly or indirectly identified or identifiable through personal data
Personal data information system (PDIS)	The total of personal data contained in databases, as well as information technologies and facilities, which ensure its processing
Personal data processing	Any action (operation) or set of actions (operations) conducted with personal data with or without the use of automation facilities, including collection, recording, systematization, accumulation, storage, validation (updating, modification), extraction, use, transfer (distribution, provision, access), blocking, deletion, and destruction of personal data.
Operator	Tinkoff Bank independently or together with other persons organizing and (or) conducting personal data processing, as well as defining purposes of personal data processing, scope of personal data, which is subject to processing, actions (operations) conducted with personal data

2. General provisions

- 2.1. This Policy defines PD processing principles and conditions, as well as responsibilities of the Bank upon processing thereof.
- 2.2. This Policy has been developed in accordance with the current legislation of the Russian Federation on personal data, regulatory and procedural guidelines of executive authorities relating to PD security, including its processing in PDIS.
- 2.3. Pursuant to the Federal Law dated 27.07.2006 No. 152 “On Personal Data” this Policy shall be made available without any restrictions to PD subjects, including through its publication on the Bank website in the Internet.
- 2.4. This Personal data processing policy shall apply to all processes on collection, recording, systematization, accumulation, storage, validation (updating, modification), extraction, use, transfer (distribution, provision, access), blocking, deletion, destruction of personal data implemented with or without the use of automation facilities.

3. PD processing principles

- 3.1. Personal data shall be processed in the Bank according to the following principles:
- 3.1.1. personal data shall be processed on legitimate and equitable basis;
 - 3.1.2. personal data processing shall be limited to achievement of specific predefined legitimate objectives. No personal data processing shall be allowed, which is inconsistent with objectives of personal data collection;
 - 3.1.3. no integration of databases shall be allowed, which contain personal data processed for the purposes, which are inconsistent with each other;
 - 3.1.4. only that personal data shall be subject to processing, which meets the purposes of processing;
 - 3.1.5. content and volume of personal data processed shall meet the declared purposes of processing;
 - 3.1.6. personal data processed shall not be redundant in relation to the declared purposes of processing;
 - 3.1.7. while personal data processing accuracy and sufficiency of personal data shall be ensured, as well as its relevancy, if necessary, with regard to the declared purposes of processing;

- 3.1.8. personal data shall be stored in the form allowing to identify a personal data subject only as long as is needed for personal data processing, unless a period for retaining personal data is established by the federal law or an agreement, a party, a beneficiary or a surety to which the personal data subject is.
- 3.2. Personal data processed shall be subject to destruction or anonymization after the purposes of processing are achieved, or when there is no further need to achieve such purposes, unless otherwise provided for by the federal law.

4. PD processing conditions

- 4.1. Personal data shall be processed in compliance with the policies and guidelines established by the Federal Law dated 27.07.2006 No. 152-FZ "On Personal data". Personal data processing in the Bank shall be allowed in the following cases:
 - 4.1.1. personal data shall be processed with consent of the personal data subject to his personal data processing;
 - 4.1.2. personal data processing is necessary for achievement of purposes provided for by international treaties to which the Russian Federation is a signatory, or by law, for exercise and fulfilment of functions, authorities and responsibilities imposed on the operator by legislation of the Russian Federation;
 - 4.1.3. personal data processing is necessary for administration of justice, enforcement of judicial acts, acts of any other bodies or officials, which are subject to enforcement in accordance with legislation of the Russian Federation on enforcement proceedings;
 - 4.1.4. personal data processing is necessary for performance of an agreement a party, a beneficiary or a surety to which the personal data subject is, and for execution of an agreement at the initiative of the personal data subject or an agreement under which the personal data subject shall be a beneficiary or a surety;
 - 4.1.5. personal data processing is necessary for protection of life, health or other vital interests of the personal data subject, if it is impossible to secure consent of the personal data subject;
 - 4.1.6. personal data processing is necessary to implement rights and legitimate interests of the operator or third parties, or to achieve socially significant objectives, provided that no rights or freedoms of the personal data subject are violated;
 - 4.1.7. personal data shall be processed for statistical or other research purposes, subject to obligatory anonymization of personal data. An exception is personal data processing for market promotion of products, works, services through direct contacts with potential consumers by use of communications facilities, and for political agitation;
 - 4.1.8. personal data shall be processed, access to which is granted to the general public by the personal data subject or at his request (hereinafter referred to as the "personal data made public by the personal data subject");
 - 4.1.9. personal data shall be processed, which is subject to publication or compelling disclosure in accordance with the federal law;
 - 4.1.10. databases used for collection, recording, systematization, accumulation, storage, validation (updating, modification) and extraction of personal data of the Russian Federation citizens shall be located in the territory of the Russian Federation.
- 4.2. If there is no necessity to obtain consent of the personal data subject to PD processing in written form prescribed by the Federal Law dated 27.07.2006 No. 152-FZ "On Personal Data", consent of the personal data subject may be granted by the personal data subject or his representative in any form allowing to confirm the fact of the consent receipt, including the electronic form.
- 4.3. The Bank shall be entitled to assign personal data processing to any other person with consent of the personal data subject, unless otherwise provided for by the federal law, on the terms of an agreement concluded with such person (hereinafter referred to as the "operator's assignment"). A person, who processes personal data on behalf of the Bank, shall comply with the personal data processing policies and guidelines provided for by this Policy and the Federal Law dated 27.07.2006 No. 152-FZ "On Personal Data".
- 4.4. In the event that the Bank assigns personal data processing to any other person, the Bank shall be liable to the personal data subject for any actions of such person. A person processing personal data on behalf of the Bank shall be liable to the Bank.
- 4.5. The Bank and other persons, who gained access to personal data, shall not disclose to any third parties and shall not distribute personal data without the consent of the personal data subject, unless otherwise provided for by the federal law.

5. Rights of the PD subject

- 5.1. The personal data subject shall be entitled to request from the Bank to validate, block or destruct his personal data in the event that his personal data is incomplete, obsolete, inaccurate, unlawfully received or is not necessary for the declared purpose of processing, and to assume statutory measures for protection of his rights.
- 5.2. The personal data subject shall be entitled to receive information related to his personal data processing, including information, which contains:
- confirmation of the fact of personal data processing by the Bank;
 - legal foundation and purposes of personal data processing;
 - purposes and personal data processing procedures used by the Bank;
 - name and location of the Bank, information on the persons (except for the Bank employees), who have access to personal data or to whom personal data may be disclosed according to an agreement with the Bank or FZ-152;
 - personal data processed, which relates to the relevant personal data subject, source of its origin, unless other procedure for presentation of such data is provided for by FZ-152;
 - time limit for personal data processing, including storage time;
 - procedure for implementation by the personal data subject of his rights provided for by the Federal Law No. 152-FZ "On Personal Data";
 - information on any previous or estimated cross-border data transmission;
 - name or surname, name, patronymic and address of a person processing personal data on behalf of the Bank, if the processing is assigned to such person;
 - other information provided for by FZ-152 and other federal laws.

6. Obligations of the Bank

- 6.1. In accordance with the Federal Law dated 27.07.2006 No. 152-FZ "On Personal Data" the Bank shall:
- provide the PD subject at his request with information related to his PD processing or lawfully refuse;
 - at the request of the personal data subject validate, block or destruct PD processed in the event that PD is incomplete, obsolete, inaccurate, unlawfully received or not necessary for the declared purpose of processing; or the Bank shall ensure personal data blocking, destruction, if other person, who acts on the operator's behalf, processes personal data;
 - notify the PD subject of PD processing in the event that PD was received not from the PD subject (except when the PD subject has been already notified of his personal data processing by the relevant operator);
 - if the purposes of personal data processing are achieved, immediately cease personal data processing and destruct personal data within a period of up to thirty days after achievement of purposes of personal data processing, unless otherwise provided for by federal laws; or the Bank shall ensure the destruction, if other person, who acts on the operator's behalf, processes personal data. The Bank shall notify the personal data subject or his legal representative thereof, and if a request or a letter of inquiry is sent by an authorized body on protection of rights of personal data subjects, such authority as well;
 - if the personal data subject withdraws his consent to personal data processing, cease personal data processing and destruct personal data within a period of up to thirty days after receipt of such withdrawal, unless otherwise provided for by agreement between the Operator and the personal data subject; or the Bank shall ensure termination of PD processing and PD destruction, if other person, who acts on the operator's behalf, processes personal data. The Bank shall notify the personal data subject of personal data destruction;
 - if a request is received from the personal data subject to cease personal data processing for market promotion of products, works, services, immediately cease personal data processing; or the Bank shall ensure termination of PD processing, if other person, who acts on the operator's behalf, processes personal data;
 - when collecting personal data, including through the use of the information and telecommunication Internet network, ensure recording, systematization, accumulation, storage, validation (updating, modification), extraction of personal data of the Russian Federation citizens with the use of databases located in the territory of the Russian Federation, except as otherwise provided by the Federal Law No. 152.

7. Measures to ensure personal data security while processing

7.1. While processing personal data, the Bank shall assume required legal, organizational and technical measures to protect personal data from unauthorized or accidental access, destruction, modification, blocking, copying, disclosure, distribution, and from any other inappropriate actions in relation to personal data.

7.2. Personal data security shall be achieved in particular by the following means:

- identification of security threats in relation to personal data while processing it in personal data information systems;
- taking organizational and technical measures to ensure personal data security while processing it in personal data information systems required to meet the requirements to personal data protection, whose application provides the personal data protection levels established by the Government of the Russian Federation;
- evaluation of efficiency of the measures taken to ensure personal data security prior to putting the personal data information system into operation;
- recording computer-based personal data storage media;
- detection of facts of unauthorized access to personal data and taking measures;
- recovery of personal data modified or deleted due to unauthorized access;
- establishment of rules of access to personal data processed in the personal data information system, assurance of registration and recording of actions committed with personal data in personal data information systems;
- control over the access to the premises, where personal data is processed;
- control over the efficiency of the employed personal data security measures and facilities and over the level of personal data information system security.