Personal Data Processing Policy Moscow Exchange

Content

1. General provisions

1.1. This document sets forth the policy of Moscow Exchange in processing personal data.

1.2. This Policy has been designed in accordance with the then current Russian law on personal data.

1.3. This Policy applies to any confidential information treated as personal data under Russian law.

1.4. This Policy applies to any actions performed both by automated means and manually with personal data, including collection, recording, systematisation, accumulation, storage, specification (updating, modification), retrieval, use, transfer (including distribution, provision and access), depersonalisation, blocking, deletion and destruction thereof.

2. Principles of personal data processing

2.1. Processing of personal data by Moscow Exchange is based on the following principles:

1) Personal data is processed fairly and lawfully.

2) It is processed only for specified, predetermined and lawful purposes.

3) Data cannot be subject to processing in a manner incompatible with those purposes.

4) Databases with personal data processed for inconsistent purposes cannot be merged.

5) Personal data can be processed only if it serves the relevant processing purposes.

6) Content and volume of personal data must conform to the processing purposes declared.

7) Personal data must not be excessive to the purposes for which it is processed.

8) It must be ensured that personal data is kept accurate, complete and, where necessary, kept up-to-date with regard to the processing purposes declared.

9) Data is kept in a manner that allows identifying the subject of such data until it is necessary for the purposes for which it is processed; provided that the period for retaining the data has not been established by federal law or a contract to which the subject is a party, or under which he is a beneficiary or guarantor.

10) Personal data must be destroyed or depersonilised when the purpose it was collected for is met or no longer urgent unless federal law sets forth otherwise.

3. Terms of personal data processing

3.1. Personal data is processed in compliance with principles and rules set forth in Federal Law No. 152-FZ "On personal data" dated 27 July 2006. Personal data processing is permitted if it is:

1) Done with the consent from the subject of personal data.

2) Necessary to meet objectives defined by an international treaty of the Russian Federation or under law to allow the operator to perform its functions, powers and obligations pursuant to Russian law.

3) Necessary to administer justice, execute a legal process or an act of other authority or official that is subject to execution under Russian law on enforcement proceedings.

4) Necessary to perform a contract to which the subject of personal data is a party, or under which he is a beneficiary or guarantor, or to enter into a contract on the initiative of that person or a contract under which he is a beneficiary or guarantor.

5) Necessary to protect the life, health or other vital interests of the subject of personal data where consent cannot be reasonably obtained.

6) Necessary for exercising rights and legitimate interests of the operator or any third parties, or for reasons of substantial public interest provided that this does not violate rights and freedoms of the data subject.

7) Necessary for statistical or other scientific purposes subject to data depersonalisation. This is not applied to direct marketing of goods, works and services via telecommunication facilities, and to political agitation.

8) Done with regard to personal data made publicly available by the data subject or on his initiative (the "data made publicly available by the subject").

9) Done with regard to personal data to be published or disclosed mandatorily due to federal law.

3.2. Moscow Exchange may add personal data to publicly available databases with personal data pursuant to federal law or upon receiving the written consent of the data subject.

3.3. Moscow Exchange processes sensitive personal data related to health status, pursuant to federal law or upon receiving the written consent of the data subject.

3.4. Moscow Exchange does not process biometric personal data.

3.5. Moscow Exchange does not make cross-border personal data transfers.

3.6.	No decision is made solely on the basis of automated means if it might lead to legal consequences for the personal data subject or otherwise affect his rights and legitimate interests.

3.7.	If there is no necessity for consent to personal data processing to be made in writing, the personal data subject or his representative may give his consent in any way that allows for confirmation of the consent submission.

3.8.	Moscow Exchange may commission any third party to process personal data upon approval from the data subject unless federal law provides for otherwise. In this case, the exchange must enter into a contract with such third party to ensure that the party complies with principles and rules of personal data processing as stated in federal law.

3.9.	If Moscow Exchange commissions any third party to process personal data, it is liable to the data subject for actions of such third party. The commissioned party is liable to Moscow Exchange.

3.10.	Moscow Exchange must not, and must ensure that other parties with access to personal data must not, disclose and disseminate personal data without consent of the data subject unless federal law states otherwise.

4. Data processing obligations on Moscow Exchange

4.1.	According to Federal law "On personal data", Moscow Exchange must:

1) provide the personal data subject, upon his request, with information related to the data processing or send the refusal to do so.
2) Upon the request of the data subject, specify, block or delete personal data that is incomplete, out-of-date, inaccurate, obtained unlawfully or is not necessary for the purpose of the processing.
3) Keep records of inquiries from personal data subjects.
4) Notify the personal data subject of the data processing if such data was received from a person or entity other than the subject. This does not applied if:

- The personal data subject was notified of the processing by the operator;
- Moscow Exchange receives personal data pursuant to federal law or in relation to a contract to which the personal data subject is a party or under which he is a beneficiary or guarantor.
- Personal data was produced by a publicly available subject or received from a publicly available source.
- The notice contains information that cannot be disclosed to the data subject without infringing rights and legitimate interests of third parties.

5) Cease processing personal data and destroy or depersonilise it within thirty days after the task for which personal data was collected is completed. This does not applied if otherwise provided by a contract to which the data subject is a party or under which he is a beneficiary or guarantor, other contract between the data subject and Moscow Exchange, or if Moscow Exchange is not entitled to process personal data without consent of the data subject due to Federal Law "On personal data" or other federal laws.

6) Cease processing personal data and destroy or depersonilise it within thirty days after receiving a request from the data subject to withdraw his consent to the processing of his personal data unless a contract between the data subject and Moscow Exchange provides for otherwise. Moscow Exchange must notify the data subject of the data destruction.

7) Cease processing personal data immediately after receiving a request from the data subject to stop the processing for the purpose of marketing of goods, works or services.

5. Measures to ensure the security of personal data processing

5.1. When processing personal data, Moscow Exchange takes all necessary legal, organisational and technical measures to protect personal data from unlawful or unauthorised access, destruction, change, blocking, copying, provision and distribution and other unlawful actions.

5.2. The personal data **security is ensured through:**

1) Determination of personal data security threats associated with data processing in IT systems.

2) Organizational and technical measures to ensure security of personal data in the course of its processing in the IT systems that are required to comply with protection levels established by the Government of the Russian Federation for personal data.

3) Using information security tools that are verified for their conformity in accordance with the established procedure.

4) The estimation of efficiency of personal data security measures prior the IT system goes in production.

5) Keeping records of mediums with personal data.

6) Identifying unauthorised access to personal data and taking relevant measures.

7) Recovery of personal data modified or destroyed as a result of unauthorised access to such data.

8) Establishment of rules for access to personal data processed in the IT system and compulsory registration and recording of any activities with personal data in the system.

9) Training of employees involved in personal data processing in personal data security issues.

10) Monitoring of measures to ensure the security of personal data and the adequate protection level of IT systems.

Terms and definitions

Term	Definition
Automated processing of personal data	Processing of personal data by computerised means
Biometric personal data	Data describing physiological and biological characteristics of a person which can be used by the operator to identify persona data subjects
Blocking of personal data	Temporary cessation of personal data processing (except for processing for the purpose of data specification)
Personal data security	Protection of personal data by achieving its confidentiality, integrity and availability thereof in processing in the IT systems through capabilities of users, technical facilities and IT component
IT system	Combination of databases with personal data, IT and technical facilities used to process such personal data both automatically and manually
Confidentiality of personal data	Requirement binding upon by the Company or other entity authorised to access personal data to prevent distribution of such data without consent of the data subject or other legal permission
Personal data processing	Any act performed both by automated means and manually with personal data, including collection, recording, systematisation, accumulation, storage, specification (updating, modification), retrieval, use, transfer (including distribution, provision and access), depersonalisation, blocking, deletion and destruction thereof
Publicly available personal data	Personal data that has been made publicly available with consent from the data subject, or is not subject to confidentiality requirements under federal law
Personal data depersonalisation	Actions resulting in impossibility of identification of a data subject by using his personal data without additional information
Operator	State or municipal body, legal or physical person that (alone or jointly with other persons) organises and/or carries out the processing of personal data as well as determines the purposes of personal data processing, the content of personal data, and the actions (operations) related to personal data
Personal data	Any information related (directly or indirectly) to an identified or identifiable individual (data subject)

Provision of personal data	Actions aimed to disclose personal data to a certain person or a circle of persons
Sensitive personal data	Any information that relates to nationality, racial origin, political opinions, religious or philosophical beliefs and the state of a data subject's health or sex life
Destruction of personal data	Any activity resulting in impossibility to restore the content of personal data in the IT system and/or in destruction of mediums containing personal data
Medium	A technical device designed to record, store, accumulate, modify and transmit information