PERSONAL DATA PROCESSING AND PROTECTION POLICY

and rules for using the web resource of the Bank of Russia Financial Congress,

July 3-5, 2024

1 GENERAL PROVISIONS

1.1. This Policy on the processing and protection of personal data during the Financial Congress of the Bank of Russia, to be held on July 3-5, 2024 (hereinafter referred to as the Policy) defines the principles, objectives, conditions, deadlines and methods of personal data processing (hereinafter referred to as personal data), the list of categories of personal data subjects, the list of personal data handling operations, the rights of personal data subjects, measures to monitor compliance with the requirements of the legislation of the Russian Federation on the processing of personal data, as well as measures to protect personal data.

1.2. This Policy shall apply to

- personal data processing procedures in accordance with the requirements of current legislation;
- measures for timely detection of unauthorized access to personal data and actions to prevent unauthorized access to personal data;
- monitoring compliance with the established level of personal data protection.

1.3. This Policy is drawn up in the Russian language. The text of this Policy in English is available at https://ifcongress.ru/en.

1.4. The Director General is responsible for compliance with the requirements of the legislation of the Russian Federation and the Organization's internal regulations on personal data.

1.5. The Organization's officials shall be bound by the personal data processing and protection requirements of this Policy.

2 KEY TERMS AND DEFINITIONS

2.1 The following terms and definitions are used in this Policy:

- information – information (messages, data) regardless of the form of its presentation;
- documented information – information stored on physical media by means of recording information with reference details that allow to identify such information or its physical medium;
- personal data – any information directly or indirectly related to a particular or definable natural person (the subject of personal data);
- confidentiality of personal data – a mandatory obligation of the designated person in charge who has access to personal data not to allow their dissemination without the consent of the data subject or in the absence of any other legitimate reason to disclose such data;
- operator – EFFECTCOMM LLC (INN (Tax Identification Number) 7716792536, OGRN (Primary State Registration Number): 5147746475058, address: 127006, city of Moscow, 11/2 Vorotnikovsky Pereulok, Floor 1, Unit 1, Office 1), which independently or jointly with other persons manages and/or processes personal data, as well as determines the purposes of personal data processing, the composition of personal data to be processed, and actions (operations) performed with personal data;

- processing of personal data – any computerized or non-computerized action (operation) or a set of such actions (operations) with personal data, including collection, recording, systematization, accumulation, storage, validation (updating, modification), retrieval, use, communication (dissemination, provision, access), blocking, deletion, or destruction of personal data;
- computerized processing of personal data – processing of personal data with the use of computer equipment;
- dissemination of personal data – actions aimed at disclosing personal data to an unspecified number of persons;
- provision of personal data – actions aimed at disclosure of personal data to a particular person or a particular group of persons;
- blocking of personal data – temporary suspension of personal data processing (except for cases when processing is necessary to validate personal data);
- destruction of personal data – actions which make it impossible to restore personal data in the personal data information system and/or as a result of which physical media of personal data are destroyed;
- personal data information system – a set of personal data contained in databases and information technologies and hardware that are used to process personal data;
- cross-border transfer of personal data – transfer of personal data to an authority of a foreign state, a foreign natural person or a foreign legal entity;
- biometric badge – a method of issuing a badge to a personal data subject using identification by biometric personal data contained in the Public Unified System of Identification and Authentication of Physical Persons using Biometric personal data (GIS EBS) – a facial image;
- biometric ACS (access control system) – possibility to enter the location of the Financial Congress of the Bank of Russia on July 3-5, 2024, through turnstiles by using biometric personal data and GIS EBS vectors to authenticate the subject of personal data.

3 PERSONAL DATA PROCESSING

3.1 Principles of Personal Data Processing

3.1.1 personal data shall be processed solely to achieve specific, predetermined and legitimate purposes.
3.1.2 Databases containing personal data processed for incompatible purposes may not be merged.
3.1.3 Only personal data that meet the purpose of processing shall be processed.
3.1.4 The content and scope of the personal data processed must be appropriate to the stated purposes of the processing. The personal data processed should not be redundant in relation to the stated purposes of their processing.
3.1.5 When processing personal data, the accuracy of personal data, their sufficiency and, where necessary, relevance for the purposes of personal data processing should be ensured. The Organization shall take measures or undertake to have measures to be taken to delete or validate incomplete or inaccurate data.
3.1.6 Personal data shall be stored in a form that allows identifying the subject of personal data, but for not longer than required for the purposes of personal data processing, unless the

period of storage of personal data is established by federal law or the contract to which the subject of personal data is a party, beneficiary or guarantor.
3.1.7 Processed personal data will be destroyed when the purposes of processing have been achieved or when such purposes are no longer necessary, unless otherwise required by federal law.
3.1.8 Personal data will not be disclosed to third parties and will not be disseminated without the consent of the personal data subject, unless otherwise provided by federal law..

3.2 Purposes of Personal Data Processing

3.2.1 During the Financial Congress of the Bank of Russia, to be held on July 3-5, 2024, personal data shall be processed for the purposes of:
- ensuring compliance with laws and regulations of the Russian Federation;
- preparation, conclusion, execution and termination of contracts with counterparties;
- issuance of badges to allow participation in the Financial Congress of the Bank of Russia, to be held on July 3-5, 2024;
- providing access to the Financial Congress of the Bank of Russia, to be held on July 3-5, 2024, through biometric access control stations;
- supporting entry and onsite access control procedures at locations and business and cultural events of the Financial Congress of the Bank of Russia, to be held on July 3-5, 2024, as well as at receptions, exhibitions and business meetings;
- informing potential participants of the Financial Congress of the Bank of Russia, to be held on July 3-5, 2024, about its dates and venue;
- mailing out informational messages.

3.3 List of Personal Data Subjects

3.3.1 During the Financial Congress of the Bank of Russia, to be held on July 3-5, 2024, the following categories of personal data subjects will be processed:
- participants of the Financial Congress of the Bank of Russia, to be held on July 3-5, 2024;
- speakers of the Financial Congress of the Bank of Russia, to be held on July 3-5, 2024.

3.4 List of Processed Personal Data

3.4.1 The list of processed personal data is determined in accordance with the purposes of processing personal data as specified in this Policy and includes the following data:
- last name, first name, second name (if any);
- contact information (cell phone number, e-mail address);
- information on current place of work and position held;
- photo; and
- data cookies.

3.5 Deadlines of Personal Data Processing

3.5.1 Personal data shall be processed until the established purposes of personal data processing have been achieved, unless federal laws or an agreement to which the personal data subject is a party, beneficiary or guarantor prescribe a time limit for personal data processing.

3.6 Terms and Conditions of personal data Processing

3.6.1 Processing of personal data shall be done with the consent of the subject of personal data to the processing of his/her personal data.
3.6.2 The consent of the data subject signed with a simple electronic signature will be recognized as an electronic document equivalent to the consent signed with the data subject's handwritten signature.
3.6.3 The consent shall be deemed to have been signed by a simple electronic signature and to be fully identical to a similar document in paper form, and the simple electronic signature of the data subject shall have the same validity (including legal value) as his/her handwritten signature; and such consent shall be deemed to have been signed from the moment of receipt of an authorization code in an SMS message or e-mail, if the code is sent to the telephone number or e-mail address provided by the data subject.
3.6.4 The fact that an electronic document has been signed by the data subject is established by comparing the following data: last name, first name, surname (if any), the authorization code used to sign the electronic document, the date and time of receipt by the Operator of the code sent to the telephone number or e-mail address provided by the data subject; and the telephone number or e-mail address provided by the data subject.
3.6.5. The personal data subject shall bear the risk of any and all adverse consequences that may result from the transfer to third parties of a SIM card that allows the use of the telephone number provided by him/her, as well as the risk of access to the e-mail account provided by him/her, including the risks related to unfair or illegal actions by third parties that may have been able to gain access to the above information.
3.6.6 The Organization is entitled to delegate the processing of personal data to another person with the consent of the personal data subject, unless otherwise provided by federal law, on the basis of an agreement concluded with such person (hereinafter referred to as the Operator's agency agreement). The person who processes personal data on the basis of a contract of agency shall comply with the principles and purposes of personal data processing specified in this Policy and the Federal Law *On Personal Data*. The contract of agency contains a list of actions (operations) with personal data to be performed by the person processing personal data and the purposes of processing, establishes the obligation of such person to ensure the confidentiality of personal data and provide for the security of personal data during their processing, as well as establishes the requirements for the protection of personal data being processed in accordance with Article 19 of the Federal Law *On Personal Data*.

3.7 Methods of personal data Processing

3.7.1 Processing of personal data may be computerized or non-computerized (mixed mode).
3.7.2 Personal data shall not be subject to cross-border transfers.

3.8 List of Actions to Handle personal data

3.8.1 The processing of personal data includes the collection, systematization, accumulation, storage, validation (updating, modification), use, communication (provision, distribution, access), blocking, erasure, destruction of personal data and the correction of errors.

3.9 Rights of the Subject of Personal Data

3.9.1 Personal data subjects have the right to receive information regarding the processing of their personal data, including:

- confirmation of the fact of personal data processing by the operator;
- legal grounds and purposes of personal data processing;
- purposes and methods of personal data processing as used by the operator;
- name and location of the operator, information about persons (except for the operator's employees) who have access to personal data or to whom personal data may be disclosed under a contract with the operator or by virtue of federal law;
- processed personal data of a subject and the source of obtaining such data, unless otherwise provided for by federal law;
- deadlines of personal data processing, including period of data storage;
- procedure for the exercise by the subject of personal data of the rights provided for by the Federal Law *On Personal Data*;
- corporate name or last name, first name, second name and address of the person who processes personal data on behalf of the operator, if the processing is or will be delegated to such a person;
- other information stipulated by the Federal Law *On Personal Data* or other federal laws.

3.9.2 A data subject's right to access his or her personal data may be limited by federal law, including where the data subject's access to his or her personal data would violate the rights and legitimate interests of third parties.

3.10 Procedure for Personal Data Processing

3.10.1 Sources of personal data:

- subject of personal data;
- legal representative of the subject of personal data.

3.10.2 The organization is not authorized to obtain and process data about the subject's race, ethnicity, political opinions, religious or philosophical beliefs, or sex life..

3.10.3 If personal data are collected using the forms from the website of the Financial Congress of the Bank of Russia, to be held on July 3-5, 2024, and available at: https://ifcongress.ru/ru, then:

- the subject of personal data shall be provided unhindered access to the personal data Processing and Protection Policy and the rules of using the web resource of the Financial Congress of the Bank of Russia, to be held on July 3-5, 2024;
- personal data are transferred for processing only after obtaining the consent of the subject of personal data to the processing of his/her personal data, with such consent recognized to have been given when the subject ticks off the registration form on the relevant page of the website of the Financial Congress of the Bank of Russia to be held on July 3-5, 2024.

3.10.4 The Organization obtains personal data from the data subject or his or her representative after obtaining the data subject's or his or her representative's consent to process his or her personal data, unless otherwise provided by the current legislation of the Russian Federation.
3.10.5 Personal data may only be processed for the purposes specified in Para 3.2. of this Policy.
3.10.6 Personal data are processed and stored in the personal data information system of the Financial Congress of the Bank of Russia to be held on July 3- 5, 2024.
3.10.7 Users of the personal data information system of the Financial Congress of the Bank of Russia to be held on July 3-5, 2024, shall be prohibited from copying to or storing personal data on external (removable) media.
3.10.8 When making decisions that affect the interests of the data subject, the Organization may not act on personal data obtained solely as a result of computerized processing.
3.10.9 When transferring personal data, the Organization undertakes to comply with the following requirements:
- not to disclose personal data to a third party without consent of their subject, except in cases when such disclosure is required to prevent a threat to the life and health of the subject of personal data, as well as in cases stipulated by federal laws;
- warn persons who have received personal data that such data may be used only for the purposes for which such data were disclosed, and to require these persons to confirm that this rule has been complied with.
3.10.10 If unlawful processing of personal data is discovered, the Organization is required to remedy the breach. If it is not possible to remedy such breaches, the Organization shall destroy the mishandled personal data within no more than 3 (three) working days from the date of discovery of the unlawful processing of personal data.
3.10.11 The Organization is obliged to notify the data subject that the breaches have been remedied or that the mishandled personal data have been destroyed, and if an appeal or request has been sent by the authorized body for the protection of the rights of personal data subjects, such body must also be notified.
3.10.12 Personal data shall be destroyed:
- when personal data processing purposes have been achieved;
- when the personal data subject recalls his/her consent to the processing of his/her personal data.

3.11 Personal Data Updates, Correction, Deletion and Destruction, and Responses to personal data Queries

3.11.1 If personal data are found to be incorrect or were processed unlawfully, such personal data shall be updated by the operator, or their processing shall be terminated.
3.11.2 If personal data are found to be inaccurate and/or unlawfully processed, the data subject (or authorized entity) shall send a request (application) stating that "personal data are inaccurate" and/or "processing of personal data is unlawful" and indicating the name of the data subject and the composition of the inaccurate information..
3.11.3 The subject of personal data withdraws his/her consent in person or by way of sending a written request indicating the last name, first name, second name, date and place of birth of the subject of personal data.
3.11.4 The subject of personal data can send a written request:

- electronically, including in the form of an electronic document signed with a simple electronic signature or an enhanced qualified electronic signature, to info@ifcongress.ru;
- by regular mail to the following address: 127006, city of Moscow, 11/2 Vorotnikovsky Pereulok, Floor 1, Unit 1, Office 1.

4 PERSONAL DATA PROTECTION

4.1 Main Measures to Secure Personal Data

4.1.1 During processing, personal data will be secured by preventing unauthorized, including accidental, access to personal data that could result in the destruction, alteration, blocking, copying or dissemination of personal data, as well as other unauthorized treatment of personal data.
4.1.2 Measures to ensure the security of personal data shall be selected according to the level of protection of personal data in the personal data information system, taking into account possible threats to the vital interests of individuals, society and the State.
4.1.3 Measures aimed at ensuring compliance with the requirements set forth by the Federal Law *On Personal Data* are implemented by:
- obtaining the consent of the subjects of personal data for processing their personal data, except for cases stipulated by the legislation of the Russian Federation;
- appointing a person responsible for personal data processing;
- appointing a person responsible for personal data security;
- adopting local regulatory acts on the processing and protection of personal data;
- applying legal, organizational and technical measures to protect personal data in accordance with the requirements for protecting personal data;
- establishing internal control over compliance of personal data processing with the Federal Law *On Personal Data* and its bylaws, as well as with the requirements to personal data protection, the Organization's policy on personal data processing, as well as the Organization's internal regulations on personal data processing and protection;
- assessing possible harm that may be caused to the subjects of personal data in case of violation of the Federal Law *On Personal Data*;
- familiarizing the persons who are directly involved in the processing of personal data with the provisions of the Russian Federation legislation on personal data, including requirements to the protection of personal data, and with the policy on personal data processing, and internal regulations on personal data processing;
- applying measures to recover personal data that have been modified or destroyed due to unauthorized access to them;
- prohibiting the transfer of personal data via open telecommunications channels outside the controlled area without applying the prescribed measures to ensure the security of personal data.

4.2 Personal Data Protection Measures

4.2.1 Delimitation of access authority to personal data processed in the personal data information system of the Financial Congress of the Bank of Russia to be held on July 3-5, 2024.

4.2.2 Login and password, individual for each user, are used to protect access to the automated workplace. Unauthorized access is prevented by information protection tools.

5 PERSONAL DATA PROTECTION ARRANGEMENTS

5.1 Personal data protection shall be based on the following key principles:
- comprehensive approach to building a system personal data protection;
- use of protection means that do not materially degrade the basic features of the personal data information system;
- reliable efficiency of the means of personal data protection.

5.2 The person responsible for the development, operation and fine-tuning of the personal data protection system of the Financial Congress of the Bank of Russia to be held on July 3-5, 2024, shall also be responsible for ensuring the security of personal data.

5.3 The person in charge of personal data security shall also be responsible for installation, configuration and commissioning of software and hardware-software means of personal data protection, development of personal data protection regulations and control over the status of the personal data protection system in the personal data information system of the Financial Congress of the Bank of Russia to be held on July 3-5, 2024.

6 MONITORING COMPLIANCE WITH THE REQUIREMENTS OF THE LEGISLATION OF THE RUSSIAN FEDERATION ON PERSONAL DATA PROCESSING

6.1 Compliance with the requirements of the legislation of the Russian Federation shall be monitored in order to:
- verify compliance of personal data processing with these requirements;
- verify compliance of the applied measures to protect personal data with these requirements;
- take measures aimed at detecting and preventing violations of these requirements;
- identify possible channels of personal data leakage;
- eliminate the consequences of possible violations.

Compliance with the requirements of the legislation of the Russian Federation on personal data processing shall be vested in the person responsible for the management of personal data processing.

7 MONITORING PERSONAL DATA PROTECTION STATUS

7.1 The status of personal data protection is monitored to ensure timely detection and prevention of unauthorized access to personal data, intentional software and hardware manipulation of personal data and assessment of the effectiveness of their protection.

7.2 Monitoring consists of verifying compliance with laws and regulations governing the protection of personal data and assessing the validity and effectiveness of personal data protection measures.

7.3 Based on the results of this monitoring, the effectiveness of the measures taken to protect personal data will be assessed. The protection of personal data shall be considered effective if the measures taken comply with the established requirements and standards. Non-compliance of said

measures with the established requirements and standards for the protection of personal data constitutes a violation. The results of regular monitoring analysis, identified causes of violations and recommendations for their correction will be used to inform further decisions.