APPROVED BY
Order of the Director
of the Roscongress Foundation

REGULATIONS

determining the Personal Data Processing and Security Policy within the Information System of the XXVI St. Petersburg International Economic Forum

Moscow

2023

1 GENERAL

1.1. These Regulations on Personal Data Processing and Security during Processing within the Information System of the **XXVI St. Petersburg International Economic Forum** (the Regulations) establish the principles, goals, conditions, timing and methods for processing personal data (PD), the list of PD subject categories, the list of actions carried out with PD subjects, the rights of PD subjects, measures to monitor compliance with the requirements of the Russian Federation laws on PD processing, as well as PD security measures.

1.2. These Regulations were created in consideration of the requirements of the following statutory and regulatory instruments of the Russian Federation, as well as local regulatory instruments of the Roscongress Foundation (the Foundation) pertaining to personal data:

— the Constitution of the Russian Federation;

— Federal Law No. 152-FZ on "Personal Data" dated 27 July 2006;

— Federal Law No. 149-FZ on "Information, Information Technologies and the Protection of Information" dated 27 July 2006;

— Russian Presidential Decree No. 188 "On Approving the List of Confidential Information" dated 6 March 1997;

— Russian Government Decree No. 1119 "On Approving the Requirements for Personal Data Security during Processing within Personal Data Information Systems" dated 1 November 2012;

— Russian Government Decree No. 687 "On Approving the Regulations on Aspects of the Personal Data Processing without Automation" dated 15 September 2008;

— FSTEC of Russia Order No. 21 "On Approving the Scope and Content of Organizational and Technical Measures to Ensure the Personal Data Security during Processing in Personal Data Information Systems" dated 18 February 2013;

— the Personal Data Processing Policy of the Foundation.

1.3. These Regulations constitute a guidance document that may be used to:

— organize PD processing in line with current legal requirements;

— formulate measures for timely detection of unauthorized access to PD and

identification of steps to prevent such unauthorized access to PD;

— exercise control to ensure the prescribed level of PD security.

1.4. The Director of the Foundation is hereby charged with procuring compliance with the requirements of the Russian Federation laws and the Foundation's local regulatory instruments applicable to PD.

1.5. These Regulations are binding on officials dealing with PD processing and security.

2 BASIC TERMS AND DEFINITIONS

2.1 These Regulations use the following terms and definitions:

— information – any information (communications, data), irrespective of its transformation format;

— documented information – information with appropriate details that enable identification of such information or its physical storage media and documented on physical storage media;

— personal data – any information that pertains, directly or indirectly, to aspecific or identifiable individual (personal data subject);

— confidentiality of personal data – a binding requirement on a designated allowed access to the personal data of personal data subjects to prevent distribution of personal data without the consent of the personal data subject or in the absence of other legal grounds;

— operator – a government or municipal agency, legal entity or individual that, whether acting independently or together with other entities, organizes and/or carries out personal data processing and determines the purposes of personal data processing, the scope of the personal data to be processed, and the actions (operations) to be performed with personal data;

— processing of personal data – any automated or unautomated action (operation) or series of actions (operations) performed with personal data, including collection, recording, classification, accumulation, storage, refinement (updating, revision), extraction, use, transfer (distribution, provision, access), blocking, deletion, anddestruction of personal data;

— automated processing of personal data – processing of personal data by computer;

— distribution of personal data – actions to disclose personal data to the general public;

— provision of personal data – actions to disclose personal data to a specific person or a specific group of persons;

— blocking of personal data – suspension of personal data processing (except when processing is essential for refinement of personal data);

— destruction of personal data – actions precluding restoration of the content of personal data in a personal data information system, and/or causing destruction of the physical storage media with personal data;

— personal data information system – a set of personal data contained in databases and IT and technical aids providing for processing of such personal data;

— cross-border transfer of personal data – transfer of personal data to an agency of a foreign state, a foreign individual or a foreign legal entity on the territory of a foreign state.

3 PERSONAL DATA PROCESSING

3.1 Personal data processing principles

3.1.1 PD are to be processed on a legal and fair basis.

3.1.2 PD processing is limited to fulfilling specific, predetermined and lawful purposes.

3.1.3 Databases containing PD processed for purposes incompatible with one another may not be combined.

3.1.4 Only PD that meet the relevant purposes of their processing may be processed.

3.1.5 The scope and content of the processed PD must meet the stated processing purposes. Processed PD must not be superfluous for the stated processing purposes.

3.1.6 The accuracy, sufficiency and, where appropriate, applicability of personal data to the purposes of personal data processing must be ensured during personal data processing. The Foundation shall take or arrange for the necessary steps to delete or refine incomplete or inaccurate data.

3.1.7 Personal data must be stored in a manner enabling identification of thepersonal data subject and no longer than required for the purposes of the personal data processing, unless a specific personal data storage period is prescribed by federal law or an agreement to which the personal data subject is party, beneficiary or guarantor.

3.1.8 Processed personal data must be destroyed once the processing purposes have been achieved or when there is no longer any need to achieve such purposes unless federal law stipulates otherwise.

3.1.9 PD must not be disclosed to third parties or distributed without the consent of the PD subject unless federal law stipulates otherwise.

3.2 Personal data processing purposes

3.2.1 During the XXVI St. Petersburg International Economic Forum, PD are to be processed in order to:

— ensure compliance with the statutory and regulatory instruments of the

Russian Federation;

— protect the life, wellbeing or other vital interests of personal data subjects;

— prepare, conclude, discharge and terminate agreements with contracting parties;

— preparation, receipt and activation an accreditation badge;

— obtain entry visa support;

— implement access control and site security policy at:

— XXVI St. Petersburg International Economic Forum venues;

— XXVI St. Petersburg International Economic Forum business and cultural events, social functions, expositions and business meetings;

— inform potential XXVI St. Petersburg International Economic Forum participants of the Forum dates and venues;

— provide information about the procedure for participating in the Forum as an exhibitor;

— reserve spaces for regular participants in the XXVI St. Petersburg International Economic Forum.

3.3 Personal data subject list

3.3.1 The following categories of PD subject are to be processed during the XXVI St. Petersburg International Economic Forum:

— Foundation personnel;

— contracting party personnel;

— media representatives;

— organizers;

— XXVI St. Petersburg International Economic Forum participants (visitors).

3.4 Processed personal data list

3.4.1 Processed PD will be listed with due regard for the PD processing purposes listed herein and will include the following data:

- last name, first name and patronymic;
- gender;
- date, month, year and place of birth;
- citizenship certificate (if required);
- ID details (series, number, issuing authority and date of issue);
- ID scan (series, number, issuing authority and date of issue);
- residential and registration address and (or) address of place of stay;
- telephone numbers (home and mobile);
- photo;
- employer/training provider information;
- Email;
- Information about the results of a laboratory test on COVID-19.

3.5 Personal data processing timeline

3.5.1 PD processing will continue until the identified purposes of the personal data processing are achieved unless a specific personal data processing period is prescribed by federal law or an agreement to which the personal data subject is party, beneficiary or guarantor.

3.6 Personal data processing conditions

3.6.1 PD must be processed in compliance with the rules and principles outlined in Federal Law No. 152-FZ on “Personal Data” dated 27 July 2006 (the Federal Law on “Personal Data”).

3.6.2 PD must be processed only with the consent of the PD subject to processing of their personal data.

3.6.3 The Foundation may assign PD processing to another person with the consent of the PD subject, unless federal law stipulates otherwise, under an agreement made with the given person (hereinafter the operator's assignment). The person that processes PD

under an operator's assignment shall comply with the principles and purposes of PD processing as per these Regulations and the Federal Law on “Personal Data”. The operator’s assignment lists the actions (operations) with PD to be performed by the PD processing person and the purposes of such processing, prescribe the given person's obligation to ensure confidentiality and security of the PD during their processing, and point out the security requirements for processed PD under Article 19 of the Federal Law on “Personal Data”.

3.7 Personal data processing methods

3.7.1 PD will be processed using automated and non-automated (combined) personal data processing methods.

3.7.2 There is no need for cross-border transfer of personal data.

3.8 List of actions with subjects' personal data

3.8.1 PD processing will include collection, recording, classification, accumulation, storage, refinement (updating, revision), extraction, use, transfer (provision, access), blocking, deletion, and destruction of PD.

3.9 Personal data subject rights

3.9.1 PD subjects are entitled to receive information regarding the processing of their personal data, including information containing:

— confirmation that the personal data are processed by the operator;

— the legal basis and purposes of the personal data processing;

— the purposes and methods of personal data processing employed by the operator;

— the operator's name and location, as well as information about the persons (other than the operator's staff) who have access to the personal data or to whom personal data may be disclosed under an agreement with the operator or as per federal law;

— processed personal data pertaining to the relevant personal data subject, as well as the source of such data, unless federal law prescribes a different procedure for submission of such data;

— the personal data processing timeline, including their storage period;

— the manner in which the personal data subject may exercise their rights under the Federal Law on "Personal Data";

— information about potential cross-border transfer of data;

— the legal name or last name, first name, patronymic and address of the person who processes personal data under the operator's assignment, if the processing has been

or will be assigned to such a person;

— other information required by the Federal Law on “Personal Data” or by other federal laws.

3.9.2 The PD subject's right to access their PD may be restricted under applicable federal laws, including if such access interferes with the rights and legitimate interests of third parties.

3.10 Personal data processing procedure

3.10.1 PD sources:

— PD subject;

— PD subject’s legal representative.

3.10.2 The Foundation is not entitled to receive or process PD of a PD subject concerning their race, nationality, political views, religious or philosophical convictions, or personal life.

3.10.3 Where the forms posted on the XXVI St. Petersburg International Economic Forum website are used to obtain PD:

— the PD subject is at liberty to read the XXVI St. Petersburg International Economic Forum Personal Data Processing Policy;

— the PD will be handed over for processing only after the PD subject's consent has been obtained to the processing of their PD, for which purpose, the PD subject must tick the corresponding checkbox on the registration form on the corresponding page of the XXVI St. Petersburg International Economic Forum website.

3.10.4 The Foundation shall obtain PD from a PD subject or from their representative after receiving the given PD subject or their representative’s consent to processing of personal data, unless current Russian law stipulates otherwise.

3.10.5 PD may be processed exclusively for the purposes listed in Clause 3.2 hereof.

3.10.6 The PD of subjects will be processed and stored in the XXVI St. Petersburg International Economic Forum Personal Data Information System.

3.10.7 Users of the XXVI St. Petersburg International Economic Forum Personal Data Information System shall not record information containing personal data or store it on external (transferable) media.

3.10.8 When making decisions that affect the interests of a PD subject, the

Foundation may not rely on personal data obtained exclusively through their automated processing.

3.10.9 When transferring PD, the Foundation shall abide by the following requirements:

— not to disclose personal data of a personal data subject to a third party without the consent of the former, except when such disclosure is required to avert dangers to the life and health of the personal data subject, as well as in other instances prescribed by federal law;

— notify the persons who received personal data of a personal data subject that these data may only be used for the purposes for which they are communicated, and demand that these persons confirm their compliance with this requirement.

3.10.10 If the Foundation detects any cases of misconduct involving personal data, it shall remedy such violations. Where the Foundation is unable to remedy identified violations within 3 (three) business days of detecting the misconduct involving personal data, it shall destroy such personal data.

3.10.11 The Foundation shall notify the personal data subject about the completed remediation of violations or destruction of personal data and, if the relevant enquiry or request was submitted by a designated agency for protection of the rights of personal data subjects, also to the given designated agency.

3.10.12 Personal data must be destroyed if:

— the purposes of personal data processing have been achieved;

— the personal data subject has withdrawn their consent to processing of their personal data.

4 SECURITY OF SUBJECTS' PERSONAL DATA

4.1 Key personal data security provisions

4.1.1 The security of PD during their processing is to be guaranteed by preventing unauthorized access, including inadvertent access, to personal data that might entail destruction, modification, blocking, copying or distribution of PD, as well as other unauthorized manipulations with the PD.

4.1.2 PD security provisions will be determined depending on the security level of the personal data in the Personal Data Information System taking into account potential emergence of threats to the vital interests of individuals, the general public and the state.

4.1.3 Appropriate measures must be taken to meet the requirements of the Federal Law on "Personal Data":

— obtain the consent of PD subjects to processing of their PD, except as stipulated by applicable laws of the Russian Federation;

— appoint a PD processing coordinator;

— appoint a PD security coordinator;

— adopt local regulatory instruments relating to PD processing and protection;

— implement legal, organizational and technical PD security measures as per the applicable PD security requirements;

— exercise internal control over compliance by PD processing practices with the Federal Law on "Personal Data" and regulatory instruments adopted thereunder, the PD security requirements, the Foundation's Personal Data Processing Policy, as well as the Foundation's local regulatory instruments on PD processing and security;

— assess the potential damage to PD subjects if the Federal Law on "Personal Data" is breached;

— make the persons directly involved in PD processing operations aware of the provisions of Russian Federation laws on personal data, including relevant PD security requirements, documents that govern the PD processing policy, and local regulatory instruments on personal data processing;

— keep a record of machine-readable PD storage media;

— take steps to restore PD that have been modified or destroyed as a result of

unauthorized access;

— store physical PD storage media in a manner that guarantees PD safety and prevents unauthorized access thereto;

— enforce a ban on transferring PD via open communication channels outside the controlled security area without using relevant PD security measures.

4.2 Personal data security measures

4.2.1 Access rights to personal data processed in the XXVI St. Petersburg International Economic Forum Personal Data Information System are to be differentiated.

4.2.2 A personal user login and password will be used for secure access from workstations. Information security tools will be used to preclude unauthorized access.

4.2.3 Antivirus tools will be used to protect the XXVI St. Petersburg International Economic Forum Persona Data Information System against malware.

4.2.4 Multi-functional devices, including a firewall, an intrusion detection tool and a VPN channel configuration tool, will be used to protect the Foundation's network infrastructure during network interaction sessions.

4.2.5 HTTPS / TLS 1.2, SSH, IPSEC and SSL encryption protocols will be used to protect personal data during transmission via open communication networks.

5 PERSONAL DATA SECURITY OPERATIONS

5.1 The Foundation shall manage PD protection operations in line with the following basic principles:

— observe the requirements of PD security guidelines;

— maintain a holistic approach to building the PD protection system;

— ensure security at all PD processing stages and in all Personal Data Information System operation modes,including during repair and scheduled maintenance operations;

— ensure the required PD security level at minimum cost;

— employ security aids that do not significantly impair Personal Data Information System performance;

— monitor the effectiveness of PD security aids.

5.2 The PD security coordinator shall be directly in charge of managing development, operation and improvement of the PD security system at the XXVI St. Petersburg International Economic Forum.

5.3 Applicable laws, decrees, guidelines on PD security, as well as the provisions of these Regulations, are to be referred to when preparing for and performing relevant PD security operations.

5.4 Preparations for installation, configuration and commissioning of personaldata security software and firmware tools, formulation of organizational measures for PD security and monitoring of the PD protection system status in the XXVI St. Petersburg International Economic Forum Personal Data Information System will beassigned to the personal data security coordinator.

6 CONTROL OVER COMPLIANCE WITH THE PERSONAL DATA PROCESSING LAWS OF THE RUSSIAN FEDERATION

6.1 Compliance with Russian personal data laws must be controlled in order to:

— make sure that PD processing practices are in compliance with the applicable requirements;

— ensure that the PD security measures employed comply with the applicable requirements;

— take steps to detect and prevent violations of the applicable requirements;

— identify potential PD leak channels;

— exercise control over damage caused by potential violations.

Control over compliance with Russian personal data laws will be assigned to the PD processing coordinator.

7 CONTROL OVER PERSONAL DATA SECURITY STATUS

7.1 Personal data security status must be controlled in order to ensure timely detection and prevention of unauthorized access to PD and intentional software and hardware manipulations with PD, as well as to assess the effectiveness of PD security.

7.2 Such control involves checking compliance with the statutory and regulatory instruments relating to PD security, as well as assessing the tenability and effectiveness of the PD security measures taken.

7.3 The effectiveness of implemented PD security measures is rated following the relevant control steps. PD security is considered effective if the implemented measures are aligned with the prescribed rules and requirements. If the security measures do not comply with the prescribed PD security rules and requirements, this is deemed a violation. The findings of periodical control evaluation, the identified causes of breaches and recommended remedial actions must be documented in reports or statements to be delivered for the Director of the Foundation to pass relevant decisions.