

In accordance with the Law on Personal Data Protection (*Zakon o zaštiti podataka o ličnosti "Official Gazette of Republic of Serbia", no. 87/2018*) (hereinafter "**the Law**") and in accordance with Article 28 of the Statute of the Foreign Investors Council association adopted on 12 December 2019, the Board of directors of the Foreign Investors Council association, with its business seat in Belgrade, Gospodar Jevremova no. 47/IV, registration number 17411888 (hereinafter "**the Association**"), at the extraordinary session held on June 9th, 2020 adopts the following:

RULEBOOK ON THE PROTECTION OF PERSONAL DATA
(hereinafter "**the Rulebook**")

I Introductory provisions

Article 1

The Rulebook regulates the protection of personal data that is processed by the Association, the purpose and objective of the personal data processing, meaning of used terms, principles of processing, retention policy, legal basis for processing, consent for processing, rights of the data subject, obligations of the controller and processor, data protection impact assessment, records of personal data processing activities, transfer of personal data to third countries and international organizations, data protection officer, remedies in case of personal data breach, as well as the amendments to the Rulebook.

This Rulebook is the basic internal act that in general regulates personal data protection of the employees, external consultants and other persons who engage in contractual and other legal relationships with the Association, as well as other persons whose data is processed by the Association (users/clients, business partners etc.), in accordance with the Law and other legislative provisions regarding personal data protection. The purpose of this Rulebook is to ensure legal security and transparency during personal data processing.

Article 2

The Association processes the personal data of its employees, associates, candidates who apply for job, representatives of members and representatives of potentially interested parties, representatives of public administration, international organizations and diplomacy representatives, representatives of suppliers and visitors of the events organized by the Association.

II Objective and purpose of the Rulebook

Article 3

The purpose of this Rulebook is to ensure the protection of fundamental rights and freedoms of natural persons, in particular their right to the protection of personal data.

The Association collects personal data and processes it as the controller with the purpose of establishing employment and with the objective of exercising rights on work and regarding work, with the purpose of engaging persons on other legal basis, exercising rights and fulfilling obligations regarding employment, organizing job applications, fulfilment of its legal obligations and other purposes which are directly related to work, engagement or any other kind of collaboration with persons whose data is processed. Collection and processing of personal data of representatives of members of the Association and potentially interested parties, the Association does to contact, inform and invite them to the events the Association organizes. Collection and processing of the personal data of the visitors to the events of the Association is done in order to keep record of the attendance to the events and to send letters

of appreciation for attendance. Photographs and audio recordings from events are used for informing about the event and are uploaded to the Association's webpage: www.fic.org.rs.

The Association processes the personal data as the controller in order to fulfill its obligations from the legal relationship with associates and partners.

III Definition of the terms

Article 4

Terms in this Rulebook have the following meaning:

- **"personal data"** means any information relating to the natural person who is identified or identifiable, directly or indirectly, in particular based on identifier, such as name and identification number, location data, an online identifier or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity;
- **"data subject"** means the natural person whose data is processed;
- **"processing"** means any operation or set of operations which is performed automated or not automated on personal data or sets of personal data, such as collection, recording, organization, grouping i.e. structuring, storage, adaptation or alteration, disclosure, insight, usage, disclosure by transmission i.e. delivery, multiplying, spreading or otherwise making available, alignment, restriction, erasure or destruction (hereinafter: processing);
- **"pseudonymization"** means processing in such manner that the personal data can no longer be attributed to a specific person without the use of additional information, provided that such additional information is kept separately and is subject to technical, organizational and personnel measures to ensure that the personal data cannot be attributed to an identified or identifiable natural person;
- **"data collection"** means any structured set of personal data which is accessible according to specific criteria, regardless the filing system is centralized, decentralized or dispersed on a functional or geographical basis;
- **"controller"** means the natural or legal person, who alone or jointly with others determines the purpose and means of processing;
- **"processor"** means the natural or legal person who processes personal data on behalf of the controller;
- **"recipient"** means the natural or legal person, public authority to which the personal data are disclosed, regardless if it is a third party or not, unless it is public authority which, in accordance with law, receive personal data in the framework of investigating a particular case and are processing those data in compliance with the personal data protection rules according to the purposes of the processing;
- **"third party"** means a natural or legal person, i.e. public authority, who is not the data subject, controller or processor, nor the person authorized to process personal data under the direct supervision of the controller or processor;
- **"consent"** of the data subject means any freely given, specific, informed and unambiguous indication expression of the data subject's will, by which he or she, by a statement or by a clear affirmative action, gives consent to the processing of personal data relating to him or her;
- **"personal data breach"** means a breach of security of personal data leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed;
- **"Commissioner for Information of Public Importance and Personal Data Protection"** (hereinafter: **"the Commissioner"**) is independent public authority established in accordance with the law, who is in charge of supervising the implementation of the Law and carrying out

other tasks prescribed in the Law. Contact information of the Commissioner: address of the seat: Bulevar kralja Aleksandra 15, 11120 Belgrade; e-mail: office@poverenik.rs; telephone: +381 11 3408 900;

- **“public authority”** means government body, autonomous province body and local government unit body, state owned enterprise, institution and other public service, organization and other legal or natural person with delegated public authority;
- **“making available”** means any activity enables access of the content to third parties, general public or government bodies.

IV Principles of processing

Article 5

The Association, when processing personal data in the capacity of the controller or processor, complies with the following principles of processing, in accordance with the Law:

- **Lawfulness, fairness and transparency** – personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject. Lawful processing is the processing done in accordance with the Law and other laws relation to processing;
- **Purpose limitation** – personal data shall be collected for specified, explicit, justified and legitimate purposes and shall not be further processed in a manner that is incompatible with those purposes;
- **Data minimization** – personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- **Accuracy** – personal data shall be accurate and, where necessary, kept up to date. Having in mind the purposes for which they are processed, every reasonable step must be taken to ensure that personal data that are inaccurate, are erased or rectified without delay;
- **Storage limitation** – personal data shall be kept in a form which allows identification of data subject for no longer than is necessary for fulfilment of the purpose of processing;
- **Integrity and confidentiality** – personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing, as well as against accidental loss, destruction or damage, using appropriate technical, organizational and personnel measures.

The Association, when processing personal data as the controller, during each personal data processing, shall be responsible for and be able to demonstrate compliance with Article 5 paragraph 1 of the Rulebook (**accountability**).

V Categories of personal data that are processed

Article 6

The Association processes personal data that is necessary for the activities of achieving its objectives listed in its Statute, in accordance with the purpose of processing and legal basis of processing.

The Association will not process data outside of the determined purpose.

Personal data of the employees and potential employees that is processed by the Association as the controller is:

- name and surname,
- date of birth,

- name of a parent,
- personal identification number,
- ID card number,
- place of issuance of ID card,
- address of residence,
- place of birth,
- country of birth,
- number of children,
- name and surname of a child,
- personal identification number of a child,
- date of Patron Saint Day,
- telephone number,
- bank account number,
- education degree and type of education,
- occupation,
- years of service,
- foreign language knowledge.

The Association may process the following personal data of other persons (representatives of the members of the Association and representatives of potentially interested parties):

- name and surname,
- function of the representative,
- business telephone number,
- business e-mail address.

The Association, in accordance with the minimization principle, does not process a larger number or other categories of personal data, than those required for the purpose of processing. In case processing of special categories of data is done based on consent of data subject, the consent must be given in written form which includes detailed information concerning the categories of data that are processed, purpose of processing and manner of usage of those data.

The Association may also process specific categories of special personal data, in accordance with Article 17 of the Law (for example, processing of special categories of personal data of employees and their family members for purposes of fulfilling its obligations or the exercise of official authority in the area of employment, social security and social protection).

Article 7

The Association performs the activities of processing such as: collecting, recording, organizing, storage, adaptation or alteration, disclosure, insight, usage, disclosure by transmission i.e. delivery, multiplication, spreading and otherwise making available, alignment, restriction, erasure and destruction, as well as any other activities by automated or not automated means and are necessary for the performance of activities.

The Association is obliged to regularly update and check the need for personal data processing and undertakes every necessary activity in order to erase and destruct the data which is no longer necessary for the purpose of processing.

VI Data retention

Article 8

Personal data that is processed by the Association as the controller concerning the employment is kept permanently, in accordance with the current legislation regulating the records in the area of employment.

Other personal data is processed by the Association as long as it is necessary, at the latest as long as there is legal basis for data processing or justified interest for its storage.

Personal data processed by the Association as the processor, based on legal transaction with other subjects, is kept in periods of time prescribed in applicable legislation.

VII Legal basis for processing

Article 9

The Association processes personal data in accordance with the principle of lawfulness and rules prescribed in the Rulebook.

The Association processes data lawfully when the purpose of processing is:

- compliance with a legal obligation,
- performance of a contract concluded with data subject or performing activities per request of the data subject made before the contract was concluded,
- consent of data subject,
- achievement of the legitimate interests of the Association.

The Association lawfully processes personal data when the processing is done in order to perform contractual obligation to others subjects, when it has the role of the processor while doing business.

Before processing, the Association is obliged to deliver notice to the data subjects whose data is processed based on their consent, which includes all necessary information concerning processing and which is prescribed by the Law.

Article 10

Consent may be given as written statement or in electronic form.

If the consent of the data subject is given as a part of written statement which relates to other matters as well, the request for consent must be presented in such a way that excludes it from the other matters, in understandable and easily accessible form, using clear and simple terms.

Data subject has the right to withdraw his/her consent at any time, and the withdrawal of consent does not affect the lawfulness of processing based on consent before its withdrawal.

VIII Rights of data subjects

Article 11

When the Association processes personal data as the controller or processor, data subjects has:

- the right to be informed concerning personal data processing and the manner of collecting data in the moment of data collection;
- the right to access and other rights relating to the access to the personal data;
- the right to rectification, amendment, erasure, limitation and portability of the collected personal data;
- the right to be informed about rectification, limitation, erasure and data portability;
- the right to object to processing of personal data to the Association;
- the right to object to automated individual decision-making, if such decision produces legal effects concerning him or her or affects his or her position.

When the Association processes the personal data as the controller or processor, it is required that the data subjects are provided with help with exercising their right to access personal data, right to rectification and amendment, right to erasure of personal data, right to be informed about rectification or erasure of data and limitation of processing, right to data portability, right to object and right to object to automated individual decision-making.

When the Association processes the personal data as the controller or processor, it is required that the data subject is informed about the procedure concerning the request to exercise the right to access personal data, right to rectification and amendment, right to erasure of personal data, right to be informed about rectification or erasure of data and limitation of processing, right to data portability, right to object and right to object to automated individual decision-making, without any delay, at the latest within 30 days since the request was received. That period may be extended up to 60 more days if necessary, having in mind the complexity and number of requests.

Article 12

The Association should provide information to the data subject on:

- the identity and contact details of the controller, as well as its representative, if any;
- contact information of the data protection officer, if any;
- the purpose of the intended processing and the legal basis for the processing;
- the existence of a legitimate interest of the controller or a third party, if the processing is carried out on the basis of processing necessary to achieve the legitimate interests of the controller or a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a minor;
- the recipient, i.e. the group of recipients of personal data, if any;
- the retention period of personal data or, if this is not possible, the criteria for determining it;
- the right to request from the controller to access, correct or delete his or her personal data, or the right to restrict processing, the right to object, as well as the right to data portability;
- the existence of the right to withdraw consent at any time, and that the withdrawal of consent does not affect the lawfulness of processing based on consent before its withdrawal, if it is processed on a base of the consent of a data subject for one or more specifically determined purposes or special types of personal data of the data subject are processed and who have given their explicit consent for processing for one or more purposes;
- the right to lodge a complaint to the Commissioner;
- whether providing information is a legal or contractual obligation or whether providing information is a necessary condition for concluding an agreement, as well as whether the data subjects have an obligation to provide information about their personal data and possible consequences if the information is not provided;

- the existence of automatic decision making.

Article 13

The data subject has the right to request and obtain information from the Association on whether it processes his/her personal data, has the right of access to such data, as well as the following information:

- purpose of processing;
- the types of personal data being processed;
- the recipient or types of recipients to whom personal data have been or will be disclosed, and in particular to recipients in other countries or international organizations;
- the envisaged retention period for personal data, or if this is not possible, the criteria for determining that period;
- the existence of the right to request correction or deletion of his/her personal data, the right to restrict processing and the right to object;
- the right to lodge a complaint to the Commissioner.

Article 14

The data subject has the right to have his or her inaccurate personal data corrected without undue delay. Depending on the purpose of the processing, the data subject has the right to amend his/her incomplete personal data, which includes giving an additional statement.

The data subject has the right to have his/her personal data deleted by the Association.

The Association is obliged to delete the data referred to in paragraph 2 of this Article without undue delay in the following cases:

- personal data is no longer necessary to achieve the purpose for which it was collected or otherwise processed;
- the data subject withdrew his or her consent to the processing of his or her personal data for one or more specific purposes;
- the data subject has filed an objection to the processing in accordance with this Rulebook and the Law.

The data subject has the right to restrict the processing of his/her personal data by the Association if one of the following cases is met:

- the data subject challenges the accuracy of the personal data, within a time limit that allows the controller to verify the accuracy of the personal data;
- the processing is unlawful and the data subject opposes the deletion of the personal data and instead of deleting restricts the use of the data;
- the Association no longer needs personal data for the purpose of processing, but the data subject has requested it in order to submit, realize or defend a legal claim;
- the data subject has filed an objection to the automated decision-making decisions, and an assessment is underway as to whether the legal basis for processing by the controller overrides the interests of the data subject.

The controller is obliged to inform all recipients to whom personal data have been disclosed of any correction or deletion of personal data or restriction of their processing, unless this is impossible or requires an excessive expenditure of time and resources.

IX Obligations of the controller

Article 15

In the event that the Association is the controller it will take appropriate technical, organizational and personnel measures aimed to ensure the effective application of the principles of personal data protection, and to ensure that processing is carried out in accordance with the Law and this Rulebook, making this Rulebook available to the data subject, taking into account the nature, scope, circumstances and purpose of the processing, as well as the probability of occurrence of the risk and the level of risk for the rights and freedoms of natural persons.

The Association as the controller applies protection measures in accordance with the level of technological achievements and costs of its application, nature, scope, circumstances and purpose of processing, as well as the probability of risk and the level of risk for personal data protection. Protection measures are applied in order to achieve an appropriate level of safety in relation to risk.

The Association, as the controller, undertakes protection measures so that every natural person who is authorized to access personal data by the Association, processes that data only by order of the Association or if required by the law.

Article 16

When the Association acts as the controller, it will ensure that without the participation of a natural person, personal data cannot be made available to an unlimited number of natural persons.

For the purpose of exercising the rights of the data subject, the Association, when acting as the controller, will make available a special mean of communication for the protection of rights.

Any data subject who submits a request for the exercise of rights in accordance with this Rulebook and the Law, should submit it by sending a letter to the e-mail address: koviljka.nikolic@fic.org.rs.

Article 17

When processing is performed on behalf of the Association as the controller, the Association will designate as a processor only the person who fully guarantees the application of the provisions of the Law and the rules prescribed by this Rulebook, in a manner that ensures that processing is performed in accordance with the provisions of the Law and provides protection to data subjects as prescribed herein.

X Obligations of the processor

Article 18

The Association acts as the processor when it processes personal data in the name and on behalf of clients and service users as a controller in accordance with the contract between them.

The contract between the controller and the processor determines the subject and duration of processing, the nature and purpose, the types of personal data and the types of persons whose data is processed, as well as the mutual rights and obligations.

When the Association acts as the processor, it is obliged to:

- process data in accordance with the Law and principles of processing;
- implement organizational, technical and personnel measures for the protection of personal data;
- act in accordance with the order given by the controller.

XI Data Protection Impact Assessment

Article 19

Before processing personal data, the Association, as the controller, will assess the impact of the planned processing operations on the protection of personal data if it is likely that some kind of processing, especially using new technologies and taking into account the nature, scope, circumstances and purpose of processing, could cause a high risk for processing. During impact assessment, the Association will request the opinion of the data protection officer, if any.

XII Records of processing operations

Article 20

The Association may keep records of collected personal data, as well as of the processing operations for which it is responsible, in writing, including electronic form.

When the Association acts as the controller, the records refer to actions that contain information:

- names and contact details of the controller and data protection officer, if designated;
- purpose of processing;
- type of data subjects;
- the type of recipients to whom the personal data have been or will be disclosed;
- the deadline after which certain types of personal data would be deleted;
- transfer of personal data to other countries;
- description of protection measures.

When the Association acts as the processor, the duty of recording refers to all processing operations on behalf of the controller, which contains the following information:

- names and contact details of each controller on whose behalf the processing is performed;
- the type of processing performed on behalf of each controller;
- transfer of personal data to other countries;
- description of protection measures.

XIII Transfer of personal data to other countries and international organizations

Article 21

Any transfer of personal data whose processing is ongoing or intended for further processing after its transfer to another country or international organization, can be done only if in accordance with other provisions of this Law 6he Association as the controller and/or processor acts in accordance with the conditions prescribed by the Law, which includes the further transfer of personal data from another country or international organization to a third country or international organization, in order to ensure an appropriate level of protection of natural persons equal to the level guaranteed by the Law.

The Association may, as a part of international cooperation, disclose personal data out of the Republic of Serbia, in accordance with the Law and other regulations.

XIV Data Protection Officer

Article 22

The Association may appoint a data protection officer by a decision, and in that case it will be obliged to submit the contact information of the appointed person to the Commissioner.

In order to perform the obligations related to the protection of personal data, the data protection officer, if designated, is obliged to comply with this Rulebook and the Law.

All persons whose data is processed by the Association, in the capacity of the controller or processor, may contact the data protection officer, if designated, in order to obtain all information regarding the processing of their data, as well as regarding the exercise of rights that belong to them.

Data protection officer is obliged to keep the confidentiality of all data obtained in the performance of his/her duties related to the processing and protection of personal data.

XV Remedies

Article 23

The data subject has the right to file an objection to the data protection officer within the Association, if designated, if he/she considers that his/her rights established by this Rulebook and the Law have been violated.

The data subject has the right to file a complaint to the Commissioner, if he/she considers that his/her rights established by this Rulebook and the Law have been violated.

The data subject has the right to judicial protection, by filing a lawsuit, if he/she considers that his/her rights established by this Rulebook and the Law have been violated.

XVI Amendments to the Rulebook

Article 24

The Association reserves the right to amend the Rulebook in accordance with applicable regulations.

XVII Final Provisions

Article 25

For all issues that are not regulated by this Rulebook, the Law applies, as well as other legally relevant regulations that contain provisions on personal data protection.

The Rulebook is published on the notice board of the Association, and enters into force and applies on the eighth day from the day of its publication.

President of the Board of Directors of the Association

Mike Michel