NOTICE ON PERSONAL DATA PROCESSING

AT INDEPENDENT SYSTEM OPERATOR IN BOSNIA AND HERZEGOVINA

EU General Data Protection Regulation (hereinafter the GDPR) is Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC which regulates data protection and natural persons privacy within the European Union and adopts regulations concerning the transfer of personal data to third countries.The GDPR's primary aim is to enhance individuals' control and rights over their personal data and to simplify the regulatory environment for international business by harmonization of the regulations across the Union. The General Data Protection Regulation which entered into force in 2016 superseded Directive 95/46/EC and, following a two-year transition period, became directly applicable in all Member States of the European Union of 25 May 2018.

In Bosnia and Herzegovina this field is governed by the Law on Personal Data Protection ("Official Gazette BiH", 49/06, 76/11 and 89/11 – correction).

Unlike applicable laws in Bosnia and Herzegovina, the General Data Protection Regulation has the intention to enhance the effectiveness of data protection in such a manner that risky processing are additionaly monitored.

By signing the Stabilisation and Association Agreement, Bosnia and Herzegovina has been obliged to ensure that its existing legislation is made compatible with the EU's acquis *(*due date 1st June 2021), and this obligation also pertains to the harmonization of the Law on Personal Data Protection with the EU's new legislation on personal data protection.

Having in mind the stated facts and a broad scope of the General Data Protection Regulation as determined in Article 3, Independent System Operator in Bosnia and Herzegovina (hereinafter NOSBiH) takes care of personal data protection and respects requirements set out in the General Data Protection Regulation and in the applicable laws although giving some preference to the General Data Protection Regulation.

The following text will give you information on the manner in which NOSBiH deals with personal data.

This notice is informative and should be understood as such.

1. Important terms

The Law on Personal Data Protection defined the terms, but General Data Protection Regulation provides broader definitions of the terms important for privacy.

Personal data, as defined by the Regulation, "means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person."

However, *personal data* is a very broad term, simply speaking it includes: name and surname, identification number, photo, voice, address, phone number, IP address, if such data can lead to direct or indirect identification of a natural person. We emphasise here that the data collector, even before the collection process starts, is obligated to provide the data subject with the following information: the purposes of the collecting, the legal basis for the collecting, the recipients of the data, and the existence of the right to request from the controller access to and rectification or erasure of his/her personal data.

Consent of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her. Where legal issue is based on consent, it must be explicit for collected data and for explicit purposes (Article 7; defined in Article 4). According to Article 7 it is the organization's liability to demonstrate that the data subject has consented to processing of his or her personal data. The consent must be freely given.

Pseudonymisation means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.

GDPR defines pseudonymisation as the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information. There is also encryption that render the personal data unintelligible to any person who is not authorised to access it without the decryption key. GDPR provides that additional information (such as the decryption key) is to be kept away from personal data which have undergone pseudonymisation.

Another approach is tokenisation, which is a non-mathematical approach to protecting data at rest that replaces sensitive data with non-sensitive substitutes, referred to as tokens. The tokens have no extrinsic or exploitable meaning or value as data. They do not alter the type or length of data, which means it can be processed by legacy systems such as databases that may be sensitive to data length and type. This approach also requires much fewer computational resources to process and less storage space in databases than traditionally-encrypted data. This is enabled by keeping certain data partially or completely visible for the processing and analytic, while sensitive data is hidden.

Pseudonymisation is recommended to reduce the risks to the concerned data subjects and also to help controllers and processors to meet their data protection obligations (Recital 28).

Although the GDPR encourages pseudonymisation with the purpose of reducing the risks to the concerned data subjects, data which have undergone pseudonymisation is still considered as personal (Recital 28) and is under the GDPR's supervision.

Communication of a personal data breach - personal data breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

The communication to the data subject is not required if the the controller has implemented appropriate technical and organisational protection measures, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption (Article 34).

Filing system means any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis.

2. Principles relating to processing of personal data

According to the General Data Protection Regulation these are the principles relating to processing of personal data:

- **lawfulness, fairness and transparency of the processing** − which means that the processing should have a specific legal basis and that the data subject is informed of the existence of the processing operation and its purposes because the controller must provide the data subject with any further information necessary to ensure fair and transparent processing taking into account the specific circumstances and context in which the personal data are processed. Furthermore, the data subject should be informed of the existence of profiling and the consequences of such profiling.
- **purpose limitation –** which means that the data should be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest; scientific or historical research purposes or statistical purposes is possible.
- **data minimisation** – which means that the data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
- **accuracy** – which means that the data must be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.
- **storage limitation** – which means that the data must be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes with

implementation of the appropriate technical and organisational measures required by the Regulation.

- **integrity and confidentiality** – which means that the data must be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage.
- **accountability**– which means that the controller is responsible for, and should be able to demonstrate compliance with the principles.

3. Legal basis for personal data processing

The processing of personal data includes operations such as collection, recording, storage, consultation, disclosure, transmission or destruction.

According to the General Data Protection Regulation the data may not be processed unless there is at least one of the following legal basis to do so (Article 6, paragraph 1):

- the data subject has given consent to the processing of his or her personal data for one or more specified purposes.
- The processing is necessary to fulfill contractual obligations with a data subject or for tasks at the request of a data subject who is in the process of enetering into a contract.
- The processing is necessary to comply with a data controller's legal obligations.
- The processing is necessary to protect the vital interests of a data subject or another individual.
- The processing is necessary to perform a task in the public interest or in official authority of the data collector.
- The processing is necessary for the legitimate interests of a data controller or a third party, unless these interests are overridden by interests of the data subject or her or his rights, especially in the case of children.

4. Rights of the data subject

According to the General Data Protection Regulation data subjects whose data are processed at NOSBiH should be able to exercise these rights:

- **Transparency** (Articles 12-14) – which means that the controller will provide the data subject with the information related to his/her identity and the contact details, the purposes of the processing as well as the legal basis for the processing, the recipients of the personal data, the transfer of personal data to a third country, the period for which the personal data will be stored, the existence of the right to withdraw consent at any time etc.
- **Right of access by the data subject** (Article 15) It gives people the right to access their personal data and information about how this personal data is being processed. A data controller must provide, upon request, an overview of the categories of data that are being processed as well as a copy of the actual data. Furthermore, the data controller has to inform the data subject on details about the processing, such as the purposes of the processing, with whom the data is shared and how the data collector acquired the data.

- **Right to rectification** (Article 16) – which means that the data subject has the right to obtain from the controller the rectification of inaccurate personal data concerning him or her and taking into account the purposes of the processing, the data subject has the right to have incomplete personal data completed, including by means of providing a supplementary statement.
- **Right to erasure ('right to be forgotten')** (Article 17) **–** which means that the data subject has the right to obtain from the controller the erasure of personal data concerning him or her without undue delay if, inter alia, the personal data are no longer necessary in relation to the purposes for which they were collected.
- **Right to restriction of processing** (Article 18) - which means that the data subject has the right to obtain from the controller restriction of processing in specific situations for example when the accuracy of the personal data is contested by the data subject with the exception of storage and certain types of processing.
- **Right to data portability** (Article 20) **-** which means that the data subject has the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and has the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided if the processing is carried out by automated means and is based on consent or on a contract.

  The data subject also has the right to transmit the personal data to another controller without hindrance from the controller to which the personal data have been provided. This right does not encompass data that has been sufficiently anonymised, but it does include data that has no identificators but can help to identify the data subject with additional data. This right implies data "provided by" data subjects and data resulting from the monitoring of their behaviour. Furthermore, the controller must provide the personal data in a structured, commonly used format (Article 20).

- **Right to object** (Article 21) – which means that the data subject has the right to object to processing of personal data concerning him or her when the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or for the purposes of the legitimate interests pursued by the controller (including profiling), and the controller may no longer process the personal data of the data subject unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.
- **Right to object to automated individual decision-making (profiling)** (Article 22) – which means that the data subject has the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her unless such decision is necessary for entering into, or performance of, a contract between the data subject and a data controller, if it is authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, and if the decision is based on the data subject's explicit consent.

5. Information on a data protection officer

Within the implementation of standards on personal data protection NOSBiH, as the data controller, designated a data protection officer. This person will provide you with any information and answer your requests pertaining to the processing of your personal data. Please direct your inquiry to:

- E-mail: info@nosbih.ba
- Address: Nezavisni operator sistema u Bosni i Hercegovini, Hifzi Bjelevca 17, Sarajevo, Bosna i Hercegovina

6. The data subject's rights in case of unauthorised processing

The data subject will exercise all rights under the General Data Protection Regulation in case of unauthorised processing of his or her data as well as the right to lodge a complaint to the competent supervisory authority.