

**INTERNAL COMPANY RULES OF MUHARSKI OOD ON THE IMPLEMENTATION AND EXECUTION OF
REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE 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
(General Data Protection Regulation)

I. Preamble. These company rules aim to introduce adequate, legally sound and sustainable intra-institutional norms and technical processes for the administration of personal data carried out by the company **MUHARSKI OOD** (hereinafter referred to as **MUHARSKI OOD**) in accordance with the General Data Protection Regulation. These Company Rules comply with the basic legislative principles on the protection of physical individuals with regard to the processing of their personal data. Irrespective of citizenship and/or the place of residence of the personal data subject, these company policies are in accordance with their fundamental rights and freedoms and, in particular, with the right of personal data protection within the meaning of Article 8 (1) of the Charter of Fundamental Rights of the European Union ("the Charter") and Article 16 (1) of the Treaty on the Functioning of the European Union (TFEU).

II. The protection of personal data in accordance with the General Regulation will be carried out by the controller MUHARSKI OOD with strict adherence to the following company rules:

1. Every client, employee or user who is a registered websites visitor (including affiliate systems where **MUHARSKI OOD** provides information) should be explicitly informed that the protection of personal data in the company **MUHARSKI OOD** (and its co-administrators) is entirely based on the strict observance and protection of the legal interests of natural persons whose data is being processed, and this measure should be technologically neutral and should not depend on the techniques used in the company (or outside). The protection of natural persons in the company **MUHARSKI OOD** should apply to the processing of personal data by automated means, as well as to manual processing, if the personal data are contained or are intended to be contained in a filing system. Files or sets of files, as well as their cover pages, which are not structured according to specific criteria should not fall within the scope of these company rules.

2. The Company Rules for Personal Data Protection by **MUHARSKI OOD** shall apply to any information relating to a natural person – a client, employee or user, registered site visitor (including affiliate systems in which **MUHARSKI OOD** provides information), which is identified or identifiable. Personal data which have undergone pseudonymisation, which could be attributed to a natural person by the use of additional information are considered to be information on physically or technically identifiable natural person. In order to determine whether a natural person is identifiable, **MUHARSKI OOD** takes into account all the means reasonably likely to be used, such as singling out, either by the controller (**MUHARSKI OOD**) or by another person to identify the natural person directly or indirectly. To ascertain whether means are reasonably likely to be used to identify the natural person, **MUHARSKI OOD** takes into account all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at

the time of the processing and technological developments. The principles of data protection should therefore not be applied by **MUHARSKI OOD** to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable.

3. The Company Rules for Personal Data Protection by **MUHARSKI OOD** shall allow for and ensure the protectability of the technical processes where natural persons may be associated with online identifiers provided by their devices, applications, tools and protocols, such as internet protocol addresses (IPs), cookie identifiers or other identifiers such as radio frequency identification tags. Technically, this means to allow leaving traces which, in particular when combined with unique identifiers and other information received by the servers of **MUHARSKI OOD**, may be used to create profiles of the natural persons and identify them.

4. The Company Rules by **MUHARSKI OOD** shall ensure for the creation and availability of explicit option for giving consent for personal data administration. Consent shall be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her, such as by a written statement, replying to automatically generated email, forwarding a statement, including by electronic means, or an oral statement. This shall include ticking a box when visiting **MUHARSKI OOD**'s website, choosing technical settings for information society services or another statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of his or her personal data. Consent shall cover all processing activities carried out for the same purpose or purposes. When the processing has multiple purposes, consent should be given for all of them separately. If the data subject's consent is to be given following a request by electronic means, the request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided. In co-administration hypotheses, in case of shared data administration, any data subject may be explicitly informed that a procedure for personal data administration has been initiated in respect of him or her even when he or she is not a registered user on a site (owned by **MUHARSKI OOD**) or an affiliate system (to which **MUHARSKI OOD** is associated as a business software publisher).

5. In connection with the employment and insurance relations of its employees, **MUHARSKI OOD** is also the controller of a special category of personal data, namely those concerning their health status. The personal data in question is used with special protection in **MUHARSKI OOD** as they are separated into a separate register for special category personal data, including all data pertaining to the health status of a data subject which reveal information relating to the past, current or future physical or mental health status of the data subject. This includes information about the natural person collected in the course of the registration for, or the provision of, health care services as referred to in Directive 2011/24/EU of the European Parliament and of the Council, to that natural person; a number, symbol or particular assigned to a natural person to uniquely identify the natural person for health purposes; information derived from the testing or examination of a body part or bodily substance, including from genetic data and biological samples; and any information on, for example, a disease, disability, disease risk, medical history, clinical treatment or the physiological or biomedical state of the data subject independent of its source, for example from a physician or other health professional, a hospital, a medical device or an in vitro diagnostic test.

6. The Company Rules for Personal Data Protection by **MUHARSKI OOD** shall ensure that any personal data processing shall be lawful and fair. The Company rules shall provide for transparency to natural persons regarding the way the personal data concerning them are collected,

used, consulted or otherwise processed and to what extent the personal data are or will be processed. The principle of transparency adopted by **MUHARSKI OOD** requires that any information and communication relating to the processing of those personal data be easily accessible and easy to understand, and that clear and plain language be used. That principle concerns, in particular, information to the data subjects on the identity of the controller and the purposes of the processing and further information to ensure fair and transparent processing in respect of the natural persons concerned and their right to obtain confirmation and communication of personal data concerning them which are being processed.

7. **MUHARSKI OOD** shall make natural persons aware of risks, rules, safeguards and rights in relation to the processing of personal data and how to exercise their rights in relation to such processing. **MUHARSKI OOD** shall provide complete transparency regarding the specific goals for which personal data is processed, these goals being defined at the moment of personal data collection. The personal data administrated by **MUHARSKI OOD** shall be adequate, relevant and limited to what is necessary for the purposes for which they are processed. Personal data shall be kept by **MUHARSKI OOD** for a period of five years since the initial administration, after which the data shall be deleted. Personal data shall be processed by **MUHARSKI OOD** only if the purpose of the processing could not reasonably be fulfilled by other means. Incorrect personal data shall be corrected or deleted.

8. Personal data administrated by **MUHARSKI OOD** shall be processed on the basis of strictly implemented technological measures that ensure appropriate security and confidentiality of the personal data, including for preventing unauthorised access to or use of personal data and the technological equipment used for the processing.

9. The Company Rules for Personal Data Protection by **MUHARSKI OOD** shall ensure the interests and fundamental rights of the personal data subject which could in particular override the interest of the data controller where personal data are processed in circumstances where data subjects do not reasonably expect further processing. The processing of personal data strictly necessary for the purposes of preventing fraud also constitutes a legitimate interest of **MUHARSKI OOD** as a data controller. The processing of personal data for direct marketing purposes shall be regarded as carried out for a legitimate interest.

10. The processing of personal data to the extent strictly necessary and proportionate for the purposes of ensuring network and information security, i.e. the ability of a certain server, network or an information system to technically resist, at a given level of confidence, accidental events or unlawful or malicious actions that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted personal data, and the security of the related services offered by, or accessible via, those networks and systems, by public authorities, by computer emergency response teams (CERTs), computer security incident response teams (CSIRTs), by providers of electronic communications networks and services and by providers of security technologies and services, constitutes a legitimate interest of **MUHARSKI OOD**. This could also include preventing unauthorised access to electronic communications networks and malicious code distribution to servers and databases of **MUHARSKI OOD**, stopping 'denial of service' attacks and damage to computer and electronic communication systems related to or making possible the storing and processing of personal data by **MUHARSKI OOD**.

11. **MUHARSKI OOD** shall provide for specialized technological measures regarding personal data which are, by their nature, particularly sensitive in relation to fundamental rights and freedoms as the context of their processing could create significant risks to the fundamental rights

and freedoms. Those personal data shall include personal data revealing racial or ethnic origin, sexual orientation, political opinion and biometric data. The processing of photographs shall not systematically be considered by **MUHARSKI OOD** to be processing of special categories of personal data as they are covered by the definition of biometric data only when processed through a specific technical means allowing the unique identification or authentication of a natural person. This data shall not be processed by **MUHARSKI OOD** unless processing is not authorized in certain cases, provided for in the General Regulation or the Law on Personal Data Protection. In this case administration shall be carried through a specific information array (database) of **MUHARSKI OOD** concerning the special categories personal data. In addition to the specific requirements for such processing, the general principles and other rules of the General Regulation and the Law on Personal Data Protection should apply, in particular as regards the conditions for lawful processing. Derogations from the general prohibition for processing such special categories of personal data should be explicitly provided for by **MUHARSKI OOD**, *inter alia*, where the data subject gives his or her explicit consent in this regard.

12. Special categories of personal data that need more protection are administered by **MUHARSKI OOD** for health purposes of its employees and in others, statutory cases (public, cultural, museum, educational purposes, cases involving the investigation of crimes against intellectual property and theft/misuse of personal data) but only when it is necessary to achieve these objectives in favour of individual natural persons, in particular within the management of healthcare services and systems, education, culture, social care, as well as ensuring continuity of healthcare or social services for the purpose of prevention and security, and so on. Therefore, these Company Rules provide for harmonized conditions for the processing of special categories of personal data for specific objectives in relation to specific needs, in particular when the processing of these data is carried out for certain specified in The General Regulation, the LPDP and other legitimate purposes of the administrator **MUHARSKI OOD**, bound by the legal obligation of professional secrecy and confidentiality over special categories of personal data of individuals.

13. If the personal data processed by **MUHARSKI OOD** do not permit the controller to identify a natural person, the data controller shall not be obliged to acquire additional information in order to identify the data subject for the sole purpose of complying with any provision of the General Regulation or LPDP. However, **MUHARSKI OOD** shall not refuse to take additional information provided by the data subject in order to support the exercise of his or her rights. The identification shall include the digital identifying the data subject, for example through an online mechanism authentication (fill in a personal data poll, click on declaration of consent for the administration of personal data), as well as the use of the data subject of the identity information on registration for an online service offered by **MUHARSKI OOD** in its capacity of personal data controller.

14. **MUHARSKI OOD** complies strictly with the principle of transparency by providing any information addressed to the public or to the data subject in a concise, easily accessible and easy to understand form, using clear and plain language and, additionally, where appropriate, visualisation. All information regarding company rules and technology measures of **MUHARSKI OOD** related to personal data, is represented in electronic form of the company's website.

15. As an administrator of a different kind of personal data, company **MUHARSKI OOD** has created a framework and conditions for facilitating the exercise of the rights of the data subjects, including mechanisms for requesting and obtaining correction, limiting and the deletion of personal data, as well as the exercise of the right of objection. **MUHARSKI OOD** provides a technological

opportunity for filing claims under the electronic path to this type of personal data that is received and processed electronically. **MUHARSKI OOD** responds to requests from the data subject without undue delay and no later than one calendar month.

16. Any natural person (whether or not an employee or user of the company) the services of **MUHARSKI OOD**) has the right of access to his or her collected personal data, and to exercise this right easily and at reasonable intervals. The company **MUHARSKI OOD**, in its capacity of controller has created a technical opportunity for each individual legal entity to be made aware of the processing of his or her personal data and verify the legality of this process. This includes the right to data subjects to access their health data, for example the data in their medical records that contain information such as diagnoses, results of examinations, opinions of treating doctors and treatments or operations. In this context, **MUHARSKI OOD** has created the opportunity for every data subject to be able to get acquainted with and receive information, in particular, the purposes for which his or her personal data are processed and the time limit for the personal data is processed, the recipients of personal data, the automated processing (if applicable) of personal data and consequences of such processing, at least when carried out on a profiling basis. When necessary, **MUHARSKI OOD** can provide remote access to a secure system to provide the data subject with direct access to his/her personal data. However, this right cannot be used against or influenced adversely affecting the rights or freedoms of others, including trade secrets, intellectual property - in particular copyright or technological protection measures for the software of **MUHARSKI OOD**. These considerations do not constitute a refusal to provide all the information to the relevant data subject. When **MUHARSKI OOD** processes a large quantity of information about the data subject, the controller may request from the data subject before submitting the information, to specify the information or the processing activities to which the request relates.

17. Based on these Company Rules, the subject whose personal data is administrated by **MUHARSKI OOD** has the right to correct the personal data related to him/her, pseudonymization, and the right to be forgotten when the retention of this data is in violation of the LPDP or the General Regulation. The data subject shall have the right to have his or her personal data erased and no longer processed by **MUHARSKI OOD** where the personal data are no longer necessary in relation to the purposes for which they are collected or otherwise processed, where a data subject has withdrawn his or her consent or objects to the processing of personal data concerning him or her, or where the processing of his or her personal data does not otherwise comply with the General Regulation or the LPDP. To strengthen the right to be forgotten in the online environment, the right to erasure shall also be extended by **MUHARSKI OOD** in such a way that if the personal data was made public, the company shall be obliged to inform the controllers or co-controllers which are processing such personal data to erase any links to, or copies or replications of those personal data. In doing so, **MUHARSKI OOD** shall take reasonable steps, taking into account available technology and the means available to the controller, including technical measures, to inform the controllers/co-controllers which are processing the personal data of the data subject's request.

18. As a personal data controller, **MUHARSKI OOD** has also developed technological measures concerning the limitation of the processing of personal data which include a temporary move of the selected personal data to another handling system, terminating user access to them and/or temporary removal of published data from the company's website.

19. In order to maintain security and prevent processing that is in violation of the LPDP or the General Regulation, **MUHARSKI OOD** shall constantly and in real time perform software assessment of the risks associated with the processing, and undertake technological measures to

limit those risks, consisting of encryption. Those measures shall ensure an appropriate level of security, including confidentiality, taking into account the state of the art and the costs of implementation in relation to the risks and the nature of the personal data to be protected. In assessing data security risk, **MUHARSKI OOD** gives consideration to all risks that are presented by personal data processing, such as accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed which may in particular lead to physical, material or non-material damage.

20. A personal data breach may, if not addressed in an appropriate and timely manner, result in physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, damaging of reputation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned. Therefore, immediately after it becomes aware of a violation of the security of personal data, **MUHARSKI OOD** shall bear its obligation and the responsibility, without undue delay, to notify the Commission of the protection of personal data about the breach of personal data security no later than 72 hours after becoming aware, unless **MUHARSKI OOD** is unable to prove, in compliance with the accountability principle, that it is unlikely for the security breach to lead to risks to the individuals' rights and freedoms. Where such notification cannot be submitted within 72 hours, the reasons for the delay shall be stated by **MUHARSKI OOD** and it shall provide the information to the Commission on the protection of personal data in phases without undue further delay.

Date: 17.05.2018

MUHARSKI OOD