The _____ Policy concerning the processing of personal data and information on effective requirements for protection of personal data.

1. General provisions

1.1. The present Policy determines general principles and the order of personal data processing and measures to ensure their safety at _____ (hereinafter – the Controller).

The purpose of the present policy is to ensure the protection of the human and citizen rights and freedoms during processing of personal data, including protection of rights to inviolability of private life, personal and family secrets, clear and strict observance of requirements of applicable legislation.

1.2. Policy on the processing of personal data is developed in accordance with the provisions of the EU General Data Protection Regulation (GDPR), EU Data Protection Directive (DPD) and applicable legislation that determine the working procedure with personal data and requirements to ensure their safety.

1.3. This Policy shall constitute an integral part of Master Service Agreement #____ (hereinafter - MSA). All the respective terms used in this Policy shall be construed in accordance with the MSA.

1.4. The terms in the present Policy shall be construed as follows:

"Controller" is _____ which in accordance with this Policy either independently or together with other persons organize and (or) carry out processing of personal data, and determine purposes of personal data processing, the scope of personal data to be processed, actions (operations) performed with personal data;

"Automated personal data processing" shall mean the processing of personal data using computer technology;

"Personal data blocking" shall mean the temporary cessation of personal data processing (except if processing is needed for personal data specification);

"Data center" shall mean a specialized organization providing services on placement of server and network equipment, renting servers (including virtual), as well as connection to the Internet;

"Access to personal data" shall mean access of certain persons (including employees) to subjects' personal data processed by the Controller, provided that confidentiality of such information is maintained;

"Controller's Customer or Customer" shall mean a legal entity, individual entrepreneur or natural person who has concluded with the Controller the agreement on

hosting and technical support of information system based on Service according to applicable MSA;

"Confidentiality of personal data" shall mean the obligation of the persons granted with access to personal data, not to disclose it to third parties and not to disseminate personal data without consent of the personal data subject, unless otherwise provided by applicable legislation;

"Personal data pseudonymisation" shall mean 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;

"Personal data processing" shall mean any action (operation) or set of actions (operations) performed with the use of means of automatization or without use of such means on personal data including collection, recording, systematization, accumulation, storage, specification (update, change), extraction, use, transfer (distribution, granting, access), pseudonymisation, blocking, erasure, destruction of personal data;

"Personal data" shall mean any information relating to directly or indirectly identified or identifiable natural person (personal data subject);

"Personal data provision" shall mean actions aimed at revealing personal data to a certain person or persons;

"Sensitive personal data" shall mean personal data concerning race, nationality, political opinions, religious or philosophical beliefs, health, sexual life, sexual orientation, genetic data or biometric data;

"Personal data subject " shall mean natural person to whom the personal data refers.

"Destruction of personal data" shall mean actions resulted in the impossibility to restore the contents of personal data in the personal data information system and (or) resulted in destruction of personal data material carriers;

"CRM system" shall mean a set of software tools created by the Controller on the basis of Mindbox Service, and which is intended for placing and processing the Controller's Customers' data on the basis of agreements with them; the server part of the system is located in a data center not owned by the Controller.

"Controller's website" shall mean a website on _____.

"Applicable legislation" shall mean laws of the _____ and EU legislation concerning the matter, in particular EU General Data Protection Regulation and EU Data Protection Directive.

"EU Data Protection Directive" shall mean Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Official text: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:31995L0046

"EU General Data Protection Regulation" shall mean 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 (General Data Protection Regulation). Official text: http://eur-lex.europa.eu/eli/reg/2016/679/oj

"Data Protection Authority (DPA)" shall mean independent public authority appointed by EU Member State to be responsible for monitoring the application of EU Data Protection Directive and EU General Data Protection Regulation, in order to protect the fundamental rights and freedoms of natural persons in relation to processing and to facilitate the free flow of personal data within the EU.

"Member State" shall mean a member state of the European Union.

"Third country" shall mean a state other than member state of the European Union.

"Cross-border transfer of personal data" shall mean transfer of personal data to state authorities of third country on the territory of such country, natural persons of third country or legal entities of third country (outside of the EU);

1.5. The Policy applies to all subjects' personal data processed by the Controller with the use of automatization means and without the use of such.

1.6. The Controller publishes this Policy on its official website on the Internet at _____ and provides unlimited access to any person who personally applies to the Controller.

2. The Controller status and categories of subjects whose personal data are processed by the Controller

2.1. The Controller is the personal data Controller in respect of personal data of the following natural persons:

- employees of the Controller, who have signed labor contracts, as well as persons performing work in favour of the Controller under the concluded civil and commercial contracts (further – Employees);
- close relatives of employees of the Controller, where the processing of their personal data is stipulated in applicable legislation, and performed by the Controller as employer in accordance with the requirements of appropriate state authorities (hereinafter – the Relatives of employees);

- the applicants for vacancies of the Controller, who submitted personally or through specialized organizations for recruitment (recruitment agencies) their CVs, or application forms (hereinafter – Applicants);
- the Controller's clients who are natural persons (including individual entrepreneurs) (hereinafter – Natural Person Clients);
- representatives of counterparties of the Controller with which the Controller has a contractual relations or with which the Controller intends to enter into contractual relations (hereinafter – the Representatives of the counterparties);
- Customer's Clients whose data is stored and processed in Service under the respective MSA.

2.2. Personal data is provided (transmitted) to the Controller to the extent determined by applicable legislation, appropriate state authorities and national extra-budgetary funds within the limits of their powers. In such cases special consent of the subjects for such transfer of personal data is not required.

Customers of the Controller shall independently decide on ordering the Controller to process personal data, determine the composition of data to be transmitted for processing, a list of actions (operations) with personal data that is to be performed by the Controller, and for purposes of such processing.

3. Principles of personal data processing

The processing of personal data by the Controller is carried out in accordance with the following principles:

3.1. Lawful, fair basis and transparent manner for the processing of personal data. The Controller shall take all necessary measures to comply with legal requirements, shall not process the personal data in cases where it is not permitted by applicable legislation, shall not use the personal data to the detriment of the subjects.

3.2. Limitation of the personal data processing by reaching concrete, priorly specified and legitimate purposes. In respect of the Customer's Clients the purpose of personal data processing by the Controller is the due performance of the MSA concluded between the Controller and the Customer.

3.3. Processing of only such personal data which corresponds to the priorly stated purposes of their processing. Compliance of the content and scope of processed personal data with the stated purpose of processing. Preventing the processing of personal data incompatible with the objectives of collecting personal data and excessive regarding the stated purposes of processing. The Controller shall comply with data minimization principle and not collect personal data that is not needed to achieve the purposes specified in the present Policy, shall not use subjects' personal data for any purposes other than those specified above.

3.4. Preventing the unification of databases containing personal data, processing of which is carried out for purposes that are not compatible with each other.

3.5. Providing the accuracy, adequacy and relevance of personal data in relation to the purposes of personal data processing. The Controller takes all reasonable measures to support the relevance of the personal data processed, including but not limited to, the right of every subject to review his or her personal data and to require from the Controller their clarification, rectification, blocking, erasure or destruction, restrict or object data processing in case personal data being incomplete, outdated, inaccurate, illegally obtained, not necessary for the stated purposes of processing or in other way incompatible with the applicable legislation.

3.6. If the storage period of personal data is not set by applicable legislation, the agreement, party to or beneficiary under which the personal data subject is, personal data must be kept in a form that permits identification of data subjects for no longer than it is necessary for the purposes of personal data processing. Personal data may be stored for longer periods insofar as the data will be processed solely for archiving purposes in the public interest, or scientific, historical, or statistical purposes in accordance with applicable legislation and subject to the implementation of appropriate safeguards.

3.7. Destruction or pseudonymisation of personal data after the achievement of the stated purposes of their processing or in case of loss of necessity to achieve such purposes, if it is impossible for the Controller to eliminate committed violations of the order of personal data processing prescribed by law, withdrawal of consent for processing of personal data by the subject, unless otherwise provided by applicable legislation or agreements with other entities.

3.8. Personal data shall be processed in a manner that ensures appropriate security of those data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

3.9. The Controller is responsible for, and shall be able to demonstrate, compliance with the Data Protection Principles under the GDPR.

4. Terms and conditions of personal data processing

4.1. The processing of personal data by the Controller is allowed in the following cases:

4.1.1. Under the consent of the personal data subject for the processing of personal data.

4.1.2. To carry out and fulfill the Controller's functions, powers and obligations under the applicable legislation.

4.1.3. The personal data processing necessary for the exercise of the rights and legitimate interests of the Controller or third parties or to achieve important public purposes, provided that doing so does not violate the rights and freedoms of the personal data subject.

4.1.4. The personal data processing is necessary in order to protect the vital interests of the data subject or of another natural person.

4.1.5. The personal data processing carried out for statistical or other research purposes provided the obligatory personal data pseudonymisation so that personal data does not require identification.

4.1.6. Unlimited access of individuals to personal data provided by the personal data subject or, at his request.

4.1.7. Personal data shall be subject to publication or mandatory disclosure in cases prescribed by applicable legislation.

4.2. The Controller shall not disclose personal data to third parties or distribute it without the consent of the personal data subject, unless otherwise stipulated by applicable legislation.

4.3. The Controller shall not process sensitive personal data regarding racial and ethnic origin, political opinions, religious or philosophical beliefs, health, sexual life of the subjects, sexual orientation, genetic data or biometric data, unless processing of such data is permitted by applicable legislation or personal data subject gives an appropriate consent.

4.4. The processing of personal data concerning criminal convictions may be carried out by the Controller solely in the cases and manner established by applicable legislation.

4.5. Biometric personal data, including photographic images, used by the Controller to identify the subject can be processed by the Controller only with the consent of the subject or in the case where such processing is required by the applicable legislation.

4.6. The Controller shall not conduct the cross-border transfer of personal data, with the exception of cases stipulated by the agreement with the Controller's Customer provided the compliance with applicable legislation.

4.7. Cross-border data transfers to a recipient in a third country may take place if the third country receives an Adequacy Decision from the European Commission in accordance with the EU applicable legislation.

4.8. The Controller shall not make decisions that induce legal consequences in respect of the personal data subject or otherwise affect the rights and legitimate interests of subjects solely on the basis of automated processing of personal data. Data that has legal

consequences or affecting the rights and legitimate interests of the subject shall be verified by the authorized employees of the Controller before their use.

5. Personal data processing methods

5.1. The Controller shall process the personal data with use of automatization means, and without the use of such means.

5.2. This Policy applies in full scale to personal data processing with use of automatization means and processing without the use of automatization means – in cases where such processing is consistent with the nature of actions (operations) performed over personal data with use of automatization, thus enables in accordance with a specified algorithm to search personal data recorded in tangible medium, and contained in files or other systematic collections of personal data and (or) access to such personal data.

6. Confidentiality of personal data

6.1. The Controller shall ensure the confidentiality of the processed personal data, under the procedure provided by applicable legislation.

6.2. Confidentiality is not required with respect to:

- personal data after its pseudonymisation;
- personal data, to which an access of an unlimited amount of persons is provided by the personal data subject or on the request of the subject (hereinafter – the personal data made publicly available by the personal data subject);
- personal data which is subject to publication or mandatory disclosure under applicable legislation.

7. The consent of the personal data subject for personal data processing

7.1. The personal data subject makes the decision on provision of its personal data to the Controller and gives consent for the processing freely on his or her own will and in his or her interest. Consent for personal data processing must be specific, informed, unambiguous and conscious and may be given by subject by a statement or a clear affirmative action. The form of consent shall provide the possibility to confirm its receipt.

7.2. In the case of consent for the personal data processing received from representative of personal data subject, the powers of the representative to give consent on behalf of the subject data shall be examined by the Controller.

When requesting personal data, the processing of which is not prescribed by the applicable legislation or not required for the performance of the agreement, party to which the personal data subject is, obtaining the consent of the subject is required only for the processing of additionally requested by the Controller of data.

7.3. Personal data of persons signing the agreement with the Controller contained in the state registers of companies, individual entrepreneurs, legal entities, commercial registers and others are publicly available, except information on the number, date of issuance and the authority issuing the natural person identity document. Privacy protection and consent of the subjects for processing is not required. In all other cases the consent of personal data subjects who are Representatives of counterparties of the Controller is required, with the exception of the persons who signed the agreement with the Controller, as well as provided power of attorney to act in the name and on behalf of the personal data subject or counterparties of the Controller and thereby committed a clear affirmative action, confirming their consent to the personal data processing referred to in the text of the contract and/or power of attorney. Consent for transfer of personal data of its representatives (employees) to the Controller can be obtained by the Controller's counterparty. In this case, the Controller is not required to obtain consent for the personal data processing.

7.4. The Customer shall provide that all its Clients have given appropriate and lawfully obtained consent for the personal data processing. The Controller deems that the Customer acts in good faith and fulfils its obligations concerning the consent obtaining from the personal data subjects. The Controller shall not be liable for obtaining of such consent.

If the Controller processes personal data by order of Customer, it is not obliged to obtain the consent of personal data subject for the processing of personal data.

7.5. The consent of the subjects for providing their personal data is not required when the Controller receives, within the framework of its competence, motivated request from Data Protection Authorities (DPAs), the prosecution bodies, law enforcement bodies, security agencies, state labour inspection bodies while carrying out state supervision and control over observance of labor legislation and other bodies authorised to request information on the employees in accordance with the competence stipulated by applicable legislation.

A motivated request should include the purpose of the request, the reference to the legal grounds of the request, including confirming powers of the authority making the request and the list of requested information.

7.6. In case where receipt of requests from organizations that do not possess the appropriate authorization, the Controller is obliged to obtain the consent of the subject to provide his or her personal data and to warn the persons receiving the personal data that these data can be used only for the purposes for which they are communicated, and to require from such persons confirmation that this rule will be (was) followed.

7.7. Silence, pre-ticked boxes, inactivity, failure to opt-out, or passive acquiescence do not constitute valid consent.

7.8. The data subject shall have the right to withdraw his or her consent at any time without detriment. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent.

7.9. In all cases the Controller shall have the obligation to provide evidence of obtaining the consent of personal data subject for the personal data processing or evidence of the grounds specified by applicable legislation.

8. Rights of personal data subjects

8.1. The personal data subject has the right to receive information regarding the processing of his or her personal data. The subject shall have the right to require from the Controller to clarify his/her personal data, to rectify, to block or to erase it, to restrict or object its processing in case personal data being incomplete, outdated, inaccurate, illegally obtained, not necessary for the stated purpose of the processing or the erasure is necessary for compliance with applicable legislation, and also to use legal remedies to protect the rights.

8.2. Personal data subjects have the right to object, on grounds relating to their particular situation, to the processing of personal data, where the basis for that processing is either:

- public interest; or
- legitimate interests of the Controller

The Controller shall cease such processing unless the Controller:

- demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject; or
- requires the data in order to establish, exercise or defend legal claims.

8.3. Personal data subjects have the right to object to the processing of personal data for the purpose of direct marketing, including profiling.

8.4. Where personal data being processed for statistical purposes, the data subject has the right to object, unless the processing is necessary for the performance of a task carried out for reasons of public interest.

8.5. If the personal data subject considers that the Controller processes personal data in violation of applicable legislation or otherwise violates his rights and freedoms, the personal data subject may complain the actions or omission of the Controller to the relevant DPA or seek judicial remedy.

8.6. The personal data subject has the right to protect his or her rights and legitimate interests in court, including right to damages and (or) compensation of moral damage.

8.7. Personal data subjects have the right not to be subject to a decision based solely on automated processing which significantly affect them (including profiling). Such processing is permitted where:

- it is necessary for entering into or performing a agreement with the data subject provided that appropriate safeguards are in place;
- it is authorised by law; or
- the data subject has explicitly consented and appropriate safeguards are in place.

8.8. Data subjects have a right to receive a copy of their personal data in a commonly used machine-readable format.

8.9. The Controller shall, within one month of receiving a request made under those rights, provide any requested information in relation to any of the rights of data subjects. If the Controller fails to meet this deadline, the data subject may complain to the relevant DPA and may seek a judicial remedy. Where the Controller receives large numbers of requests, or especially complex requests, the time limit may be extended by a maximum of two further months.

8.10. The Controller shall give effect to the rights of access, rectification, erasure and the right to object, free of charge. The Controller may charge a reasonable fee for repetitive requests, manifestly unfounded or excessive requests or further copies.

8.11. The Controller shall not refuse to give effect to the rights of a data subject unless the Controller cannot identify the data subject. The Controller shall use all reasonable efforts to verify the identity of data subjects. Where the Controller has reasonable doubts as to the identity of the data subject, the Controller may request the provision of additional information necessary to confirm the identity of the data subject, but is not required to do so.

8.12. To the extent that the Controller can demonstrate that it is not in a position to identify the data subject, the Controller is exempt from the application of the rights of data subjects prescribed by the applicable legislation. The Controller is also not obliged to obtain further personal data in order to link data in its possession to a data subject.

8.13. Where Controller has disclosed personal data to any third parties, and the data subject has subsequently exercised any of the rights of rectification, erasure or blocking, the Controller shall notify those third parties of the data subject's exercising of those rights. The Controller is exempt from this obligation if it is impossible or would require disproportionate effort. The data subject is also entitled to request information about the identities of those third parties. Where the Controller has made the data public, and the data subject exercises these rights, the Controller shall take reasonable steps to inform third parties that the data subject has exercised those rights.

9. Information on ongoing requirements for protection of personal data

9.1. Protection of personal data processed by the Controller is supported by the realization of legal, organisational and technical measures necessary and sufficient to ensure that the requirements of the applicable legislation in the field of personal data protection are met.

9.2. Legal measures shall include:

- the development of the Controller's local acts fulfilling the requirements of applicable legislation, including the present Policy concerning the personal data processing and its publication on the website of the Controller;
- refusal of any means of personal data processing not complying with the purposes predetermined by the Controller.

9.3. Organizational measures shall include:

- the appointment of a person responsible for personal data processing organization;
- the appointment of a person responsible for ensuring the security of personal data in information systems;
- limitation of Controller's employees number who have access to personal data and the organization of the permission system of access to it;
- informing the employees on applicable legislation on personal data, including requirements for the protection of personal data, local acts of the Controller for the personal data processing, training of the specified employees;
- determination in the employment obligations and job descriptions for Controller's employees obligations to ensure the security of personal data processing and liability for violation of the established procedure;
- regulation of the personal data processing;
- organization of personal data material carriers accounting and their storage to ensure the prevention of theft, spoofing, unauthorized copying and destruction;
- identification of threats to the personal data security at the processing in information systems, formation of threats models on their basis;
- placement of personal data processing technical means within a secured territory;
- restriction of unauthorized persons' access to the Controller's premises, prevention of their presence in the premises where the work with personal data is performed and technical means of their processing are placed, without supervision by the Controller's employees.

9.4. Technical measures shall include:

- the identification of personal data type security threats on an assessment of possible damage to personal data subjects, which may be caused in the event of a security breach, determination of the personal data protection level and implementation of requirements for the personal data protection at their processing in information

systems, the fulfilment of which provides established levels of personal data protection;

- development of the personal data protection system on the basis of model threats in accordance with the Member States standards of protection of personal data at the processing in information systems as may be established by respective Member State authority;
- the use of information security means which passed the conformity assessment procedure to eliminate the relevant threats;
- evaluation of the effectiveness of the measures taken to ensure the security of personal data;
- realization of the permission system of employees' access to personal data processed in information systems, to software-hardware and to software means of information protection;
- registration and accounting of actions with personal data of users of information systems where personal data is processed;
- detection of malicious software (use of antivirus software) on all nodes of the information network of the Controller providing the respective technical capability;
- safe internetwork connection (application of firewalling);
- detection of intrusions in the information system of the Controller, violating or creating prerequisites for violation of the established requirements for the security of personal data;
- recovery of personal data, modified or destroyed as a result of unauthorized access (backup system and restoration of personal data system);
- periodic monitoring of user activities, investigations of the personal data security requirements violations;
- control over compliance with these requirements (independently or by engaging on a contractual basis legal entities and individual entrepreneurs having the license for performing activity on technical protection of confidential information) not less than 1 time in 3 years.

10. Information about ongoing requirements for protection of personal data

10.1. Other rights and obligations of the Controller as controller of personal data and the person organizing personal data processing by order of other controllers are determined by applicable legislation on personal data.

10.2. The Controller's officials and employees responsible for violation of rules regulating the processing and protection of personal data, shall bear material, disciplinary, administrative, civil or criminal liability in accordance with applicable legislation.

10.3. The provisions of the present Policy shall be reviewed where required. Mandatory Policy review shall be conducted in case of significant changes in applicable legislation on personal data.

10.4. When amending Policies the following issues shall be considered:

- changes in the information infrastructure and (or) in information technologies used by the Controller;
- the prevailing in the European Union practice of legislation enforcement in the sphere of personal data;
- change of the personal data processing conditions and characteristics by the Controller due to the introduction to its activity of new information systems, processes and technologies.