Varalen Capital Markets LLC

Personal Data Processing Policy

Varalen Capital Markets LLC, a foreign company incorporated in USA under Company number 5263705, Registered in New York State (USA) 30 WALL STREET, 8TH FLOOR, NEW YORK, NY 10005-2205, represented by its General Manager Michael Butcher, hereinafter referred to as the **Company**, has developed this Personal Data Processing Policy (hereinafter, the Policy) for the processing and protection of personal data of:

- physical persons, including business persons;
- physical persons who own or control companies;
- physical persons being beneficiaries of other physical persons, except when there are reasons to suppose that another person is the beneficiary.

For the purposes of this Policy, the above-mentioned persons are hereinafter referred to as Contractors and individually Contractor.

The Company and the Contractor, including their respective representatives, are hereinafter referred to as Partners.

1. GENERAL PROVISIONS

1. This Policy regulates the relations between the Company and the Contractors concerning the processing of their personal data contained in paper and (or) electronic databases using automated systems including information telecommunication networks and the Internet, or without such facilities if the personal data processing without them meets the procedures applicable to automated data processing, i.e. allows a preset algorithm of search for personal data recorded on material media and contained in directories or other systemized collections of personal data, and (or) access to such data.

2. This Policy applies to the Contractors of the Company and (or) other contractors and their respective representatives.

3. The Policy is aimed at the protection of rights and discretions of the Partners related to their personal data processing, including the privacy rights and personal and family secrets of each Partner, and confidentiality of such information.

4. This Policy applies when the Contractors' and Partners' personal data processing helps them, under the existing or possible circumstances, raise earnings, avoid unreasonable expenses, maintain market position or gain other commercial profit. In this case confidentiality and commercial secrecy laws shall apply to personal data processing.

5. This Policy applies to the processing of data making part of insider information or when the data Operator is an insider. This Policy applies to the extent consistent with the laws and standards regulating the provision and dissemination of insider information.

2. DEFINITIONS

Personal Data – any information related directly or indirectly to an identified or identifiable individual (Data Subject) or his/her representative, contained in paper and (or) electronic databases.

Personal Data Processing – any action (operation) or a set of actions (operations) performed in the information system using automation tools (computer-aided personal data processing) or without them, in respect of personal data, including collection, recording, systematization, accumulation, storage, clarification (updating, change), extraction, use, transfer (distribution, provision, access) as well as blocking, deletion and destruction.

Cross Border Transfer of Personal Data – data transfer to a foreign country, an authority of a foreign country, a foreign natural or legal person.

Personal Data Operator – the Company, its Contractors, alone or in conjunction with other persons who organize and (or) effect processing of personal data and determine the goals and content of personal data processing and the actions (operations) to be performed therewith.

The Company may appoint any person to act as Personal Data Operator under the respective contract.

A Contractor or its natural persons or third persons gaining unauthorized or accidental access to personal data shall not be considered Personal Data Operators even if they have processed the data.

Partners' Contractors – natural persons, including business persons, having contractual relations with the Company under employment or any other civil law contracts, as well as their respective representatives, and natural persons specified in rubric three and four of the recitals to this Policy.

Immediate Threats to the Personal Data Security – a set of factors and conditions creating immediate threat of unauthorized or accidental access to the personal data as they are processed by the information system using automation tools, that may entail destruction, change, blocking, reproduction, disclosure, dissemination of the personal data and other illegal actions.

3. PERSONAL DATA PROCESSING

1. Personal data should be relevant to the purpose of processing.
2. The content and amount of the personal data under processing shall correspond to the declared purposes of processing. The personal data should not be excessive in relation to the purposes of processing.
3. Personal Data Processing under this Policy is required for the following purposes:
   - protection of life, health and other vital interests of Data Subjects of Partners' Contractors when it is impossible to obtain their consent to the personal data processing;
   - performance of any contract to which the Company is a party or under which the Company or a Contractor is a beneficiary or guarantor, including any agreement for assignment of such contract, and for the purpose of concluding a contract at the initiative of the Company or the Contractor or a contract under which the Company or the Contractor will be a beneficiary or guarantor;
   - publication or statutory disclosure of Partners' Contractors' personal data when required by the applicable laws;
   - promotion of goods, works, services on the market by directly contacting the potential Contractors using any means of communication.
4. Personal Data shall be processed on a legal and fair basis.
5. Personal data processing shall be limited to the achievement of the specified legitimate purposes. Personal data processing inconsistent with the purposes of data collection is not allowed.
6. Prerequisites for personal data processing are: data accuracy, adequacy, sufficiency and, when required, their relevance to the purpose of processing. The Personal Data Operator shall undertake or cause to be undertaken all necessary measures to delete or destruct any incomplete or inaccurate data.
7. Personal data storage shall be effected by the Company and the persons specified in par. 5 and 6 of Article V hereof, in a printed and (or) electronic format, within no less than 5 years. A longer storage term may be fixed by any contract whereto the Contractor is a party, beneficiary or guarantor.
8. Partners' Contractors' personal data should be processed with their prior consent to such processing, except when required by the applicable laws and by this Policy.

9. The Company's Contractors herewith consent to the processing of their personal data by the Personal Data Operator, except for the processing by other Contractors or their representatives and third persons as a result of unauthorized or accidental access.

10. The Personal Data Operator processing data on behalf of the Company is not obliged to obtain prior consent of the respective Contractors to the processing.

11. If the Company appoint a third party Operator, the responsibility for such Operator's actions towards Contractors shall be borne by the Company. An Operator processing personal data on behalf of the Company shall be liable directly to the Company.

The Operator organizing the processing of personal data shall, in particular:

- effect internal control of compliance by the Operator and its employees with the applicable personal data laws, including the requirements concerning the protection of personal data;
- make known to the Operator's employees the relevant requirements of the personal data protection laws, international standards, this Policy, the data security requirements;
- organize and (or) control acceptance and processing of the requests and applications submitted by Contractors or their representatives;
- not delegate its functions to any third persons in any way.

12. A Contractor or its representatives or any third persons that may effect processing of personal data through unauthorized or accidental access shall bear legal responsibility towards the Company and (or) the Personal Data Operator.

4. CROSS BORDER TRANSFER OF PERSONAL DATA

1. The Company is the resident of a country which is not a party to the EU Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data and may be included in the list of foreign countries ensuring adequate protection of the Partners' Contractors provided that the laws and personal data protection measures applicable in this country comply with the provisions of the above-stated Convention.

2. For the purposes of this Policy, Cross Border Transfer of Personal Data shall be made if required by a contract whereto the Contractor is a party, or for the protection of life, health and other vital interests of the Contractor or third persons when it is impossible to obtain their respective prior written consent or when required by the applicable laws and the provisions of this Policy.

3. Prior to the Cross Border Transfer of Personal Data and during their further processing the Company guarantees adequate protection of the Contractors' rights by implementing the following procedures:

- identifying data security threats as personal data are processed by the information system;
- implementing administrative and technical procedures ensuring the data protection as they are processed by the information system, as required by the relevant data protection regulations ensuring the data security;
- implementing the relevant procedures of the data protection compliance check;
- assessing the efficiency of the implemented data protection procedures before putting the information system into operation;
- computer data storage media accounting;
- identifying the facts of unauthorized access to personal data and remedial actions;
- restoring personal data that have been modified or destroyed as a result of unauthorized access thereto;
- setting the rules of access to personal data processed by the information system and

ensuring the registration and recording of all actions effected with personal data through the information system;

- controlling personal data protection measures applied and the information system security level.

4. This clause applies to the Partners' Contractors in case of legitimate cross border transfer of personal data by them. The Partners' Contractors represent and warrant that they will undertake all the relevant measures to ensure the data protection and prevention of accidental loss or damage of the personal data or unauthorized access thereto, or change or dissemination thereof, in compliance with the requirements of the national laws and of the EU Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of 28.01.1981 (hereinafter, the Convention), subject to the participation of the respective country in the Convention. If the country of residence is not a party to this Convention, the Partners' Contractors shall comply with the requirements of this Policy.

5. PERSONAL DATA TRANSMISSION

The following prerequisites apply to the Partners' Contractors' personal data transmission, unless otherwise stated in this Policy:

1. Disclosure of personal data to third persons is not allowed except when it is required to prevent a threat to the life and health of Contractors, Partners' Contractors or when required by the applicable laws.

For the purposes of this paragraph, the term 'third persons' shall include any natural and legal persons that may have contractual or other legal relations with the Contractors, Partners' Contractors.

2. Disclosure of the personal data of Contractors, Partners' Contractors for any purposes other than the purposes of this Policy is not allowed.

3. The Personal Data Operator shall warn the Contractors/ Partners' Contractors receiving personal data that such data may be used only for the purposes for which they have been furnished, and require written (or electronic) confirmation of compliance with this rule from any such person. Persons receiving personal data shall keep them confidential.

4. The Personal Data Operator shall appoint an officer (employee) responsible for the personal data security within the information system. Such officer (employee) shall control the transmission of those data only that are necessary for the specific action and for the purposes covered by this Policy.

5. Personal Data shall be stored in the Personal Data Protection and Storage department to be established by the Partners' Contractors. If there is no such department, a Contractor may conclude an agreement with another contractor (a company) having such department, to store personal data there, subject to such contractor's acknowledged awareness of this Policy.

6. Personal Data may be obtained, further processed and stored in a printed or electronic format.

6. ACCESS TO PERSONAL DATA

The following persons shall have the right to access the Partners' Contractors' personal data:

- the Partners' Contractors in respect of their own personal data;
- the Personal Data Operator;
- the company providing the services of the Data Security and Storage department to Partners' Contractors under the respective agreement.

7. PERSONAL DATA SECURITY

1. Besides the procedures specified in par. 3 Article IV of this Policy, persons responsible for personal data processing shall undertake all the relevant measures to counteract immediate threats to data security such as:

- unauthorized access to personal data by Contractors, Partners' Contractors, having access to the information system, including when developing, operating, performing maintenance and (or) repairs, improving, uninstalling the personal data information system;
- external malicious code exposure of the personal data system;
- application of social engineering techniques to Contractors, Partners' Contractors having access to the personal data system;
- unauthorized access to removable data storage media;
- loss of personal data storage media including portable PCs of the system users;
- unauthorized access to the personal data contained in the system using the system security vulnerability;
- unauthorized access to the personal data contained in the system using the system software vulnerability;
- unauthorized access to the personal data contained in the system using the network and data circuit security vulnerability;
- unauthorized access to the personal data contained in the system using computing network security vulnerability;
- unauthorized access to the personal data contained in the system using vulnerabilities arising through improper use of cryptographic protection.

2. There are 3 types of immediate threats to personal data security to be taken into account by those responsible for personal data processing when implementing security procedures:

- the 1st type threats are relevant to systems exposed to threats related to undocumented (undeclared) options contained in the system software used for this data system;
- the 2nd type threats are relevant to systems exposed to threats related to undocumented (undeclared) options contained in the applied software used for this data system;
- the 3rd type threats are relevant to systems exposed to threats related to undocumented (undeclared) options contained in the system and applied software used for this data system.

3. For the purpose of personal data processing 4 security levels are set in the system as follows:

a) The 1st level personal data security is required when at least one of the following conditions applies:

- the information system is exposed to the type 1 threats and either processes special categories of personal data or biometric data or other categories of personal data;
- the information system is exposed to the type 2 threats and processes special categories of personal data of more than 100 000 Data Subjects other than the Personal Data Operator's employees.

b) The 2nd level personal data security is required when at least one of the following conditions applies:

- the information system is exposed to the type 1 threats and processes publicly available personal data;
- the information system is exposed to the type 2 threats and processes special categories of personal data of the Personal Data Operator's employees or special categories of personal data of no more than 100 000 Data Subjects other than the Personal Data

Operator's employees;

- the information system is exposed to the type 2 threats and processes biometric data;
- the information system is exposed to the type 2 threats and processes publicly available personal data of more than 100 000 Data Subjects other than the Personal Data Operator's employees;
- the information system is exposed to the type 2 threats and processes other categories of personal data of more than 100 000 Data Subjects other than the Personal Data Operator's employees;
- the information system is exposed to the type 3 threats and processes special categories of personal data of more than 100 000 Data Subjects other than the Personal Data Operator's employees.

c) The 3rd level personal data security is required when at least one of the following conditions applies:

- the information system is exposed to the type 2 threats and processes publicly available personal data of the Operator's employees or publicly available personal data of no more than 100 000 Data Subjects other than the Personal Data Operator's employees;
- the information system is exposed to the type 2 threats and processes other categories of personal data of the Operator's employees or other categories of personal data of no more than 100 000 Data Subjects other than the Personal Data Operator's employees;
- the information system is exposed to the type 3 threats and processes special categories of personal data of the Operator's employees or special categories of personal data of no more than 100 000 Data Subjects other than the Personal Data Operator's employees;
- the information system is exposed to the type 3 threats and processes biometric personal data;
- the information system is exposed to the type 3 threats and processes other categories of personal data of more than 100 000 Data Subjects other than the Personal Data Operator's employees.

d) The 4th level personal data security is required when at least one of the following conditions applies:

- the information system is exposed to the type 3 threats and processes publicly available personal data;
- the information system is exposed to the type 3 threats and processes other categories of personal data of the Operator's employees or other categories of personal data of no more than 100 000 Data Subjects other than the Personal Data Operator's employees.

4. To ensure the protection of all the data security levels, the following requirements shall be met in addition to the prerequisites stipulated in Article V par. 5 and 6:

- automatic recording in the electronic security log of any new, changed or terminated powers of the persons stated in Article VI in respect of access to personal data contained in the information system;
- access to the electronic security log to be granted exclusively to the persons specified in Article VI and strictly for the purposes covered by this Policy;
- safekeeping of personal data media;
- ensuring the security of the premises where the information system is installed to prevent uncontrolled access to or presence in such premises of any unauthorized persons.

5. If, upon submission of any personal data by a Contractor or a Partners' Contractor, any unauthorized data processing is identified, the Operator shall block such personal data being processed illegally or ensure blocking thereof immediately after the submission. If, upon submission of any personal data by a Contractor or a Partners' Contractor or their respective

representative, any inadequate or incorrect personal data are identified, the Operator shall block such personal data immediately, unless such blocking infringes upon the rights and legal interests of any Contractors, Partners' Contractors or third persons.

6. If the inadequacy or inaccuracy of the personal data is confirmed, the Operator shall check the data through the documents submitted by Contractors, Partners' Contractors or their respective representatives or other relevant documents or cause such check to be done within seven days after the submission of the data and then unblock them.

7. If any unauthorized personal data processing by the Operator, Contractors, partners' Contractors or third persons is identified, such persons shall, within three business days, stop the unauthorized processing or cause it to be stopped. If it is impossible to ensure authorized processing, the said persons shall, within no more than ten business days after the detection of unauthorized processing, destroy such personal data or ensure their destruction. The said persons shall inform the Company, Contractors, Partners' Contractors or their representatives of the remedial actions or the destruction of the personal data in question.

8. If it is impossible to destroy the personal data as mentioned above and within the term specified in par.4 of this Article, the Operator shall block such personal data and ensure their destruction within no more than six months unless otherwise required by the applicable laws.

9. As soon as the purpose of personal data processing is achieved, the Operator shall stop the processing and destroy the personal data or cause authorized persons to do so, no earlier than specified in Article III par. 7 hereof or if the Operator has no right to process the data without prior consent of the Contractors /Partners' Contractors in conformity with this Policy and (or) with the applicable laws.

10. If the Contractors /Partners' Contractors revoke their consent to personal data processing, the Operator shall stop or cause to stop the processing and, if the storage of such data is no longer required for the purposes of their processing, destroy them, but no earlier than as specified in Article III par. 7 hereof or if the Operator has no right to process the data without prior consent of the Contractors /Partners' Contractors in conformity with this Policy and (or) with the applicable laws.

Contractors /Partners' Contractors may send revocation of the consent in writing to the Operator personally or through their representative or via e-mail.

8. CONFIDENTIALITY OF PERSONAL DATA

1. The Personal Data Operator shall ensure the safekeeping and confidentiality of the material data storage media, preventing unauthorized access from the moment of creation of such documents till the expiry of their storage and destruction term.

2. The obligation stipulated in par.1 above shall arise with any other persons directly or indirectly gaining access to personal data, including the information specified in Article I par.4.

3. For the purposes of the personal data confidentiality, the Company will render all the required legal assistance and help to Contractors / Partners' Contractors, including appeals to the relevant authorities and organizations of the respective countries of residence, international organizations and officials in the sphere of financial markets, and to self-regulating members of the civil community.

9. RESPONSIBILITY FOR NON-COMPLIANCE WITH THIS POLICY

The Personal Data Operator, the Contractors, Partners, Partners' Contractors and third persons having gained unauthorized or accidental access to personal data, bear responsibility under the applicable laws.

10. ADMISSIBLE EXCEPTIONS

This Policy admits exceptions unless inconsistent with the applicable laws, as follows:

- as stipulated in Article 3 par. 10;
- the Personal Data Operator shall be released of the obligation to provide Contractors/ Partners' Contractors with the information such as: full name and address of the Operator or its representative; purpose and legal basis of the personal data processing; expected users of personal data; rights of the Contractors / Partners' Contractors hereunder; source of the personal data if received by law or under a contract to which the Contractor/ Partners' Contractor is a party/ beneficiary/ guarantor;
- other exceptions provided for by the laws.

11. CONTRACTOR'S ACCEPTANCE OF THIS POLICY. CONTRACTOR'S CONSENT TO THE PERSONAL DATA PROCESSING

1. The Contractor has thoroughly read and understood the contents of this Policy including special terms and definitions and hereby agrees to and accepts this Policy.

2. The Contractor undertakes to comply with this Policy to the fullest extent and shall bear responsibility for any non-compliance or partial non-compliance, and for the action of any third persons in the events stipulated in this Policy.

3. The Contractor hereby gives consent to his/her personal data processing, of his/her own free will and in his/her interests, strictly for the purposes of such processing and for no other purposes.