BAO

FINANCIAL GROUP

PRIVACY POLICY 2018

1. Introduction

1.1 In order to service our clients BAO Financial Group (hereinafter "BAO" "we" or "us") needs to collect personal data from our clients and /or potential clients and employees.

Considering the above, BAO wants to ensure a high level of data protection as privacy is a cornerstone in gaining and maintaining the trust of our clients, employees and suppliers and thus, ensuring BAO business in the future.

The protection of personal data requires that appropriate technical and organizational measures are taken to demonstrate a high level of data protection. BAO has adopted several internal and external data protection policies, which must be adhered to by employees of BAO.

Additionally, BAO will monitor, audit and document internal compliance with the data protection policies and applicable statutory data protection requirements, including the General Data Protection Regulation ("GDPR").
BAO will also take the necessary steps to enhance data protection compliance within the organization. These steps include the assignment of responsibilities, raising awareness and training of staff involved in processing operations. Please note that this Privacy Policy will be reviewed from time to time to consider any new obligations and that any personal data we hold will be governed by our most recent policy.

This Privacy Policy, along with guidelines for processing of personal data, constitutes the overall framework for processing of personal data within BAO.

1.2 "Personal data" is any information which may be related to an identified or identifiable natural person ("data subject"). An identifiable natural person is one who can be identified, directly or indirectly, by reference to an identifier such as a name, location data, phone number, age, gender, an employee, a job applicant, clients, suppliers and other business partners. This also includes special categories of personal data (sensitive personal data) and confidential information such as health information, account number, identification number, location data, an online identifier or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

1.3 Although, information regarding companies/businesses is not as such, personal data, please note that information relating to contacts within such companies/businesses, e.g. name, title, work email, work phone number, etc. is considered personal data.

1.4 BAO collects and uses personal data for a variety of legitimate business purposes, including establishment and management of customer and supplier relationships, completion of purchase orders, recruitment and management of all

aspects of terms and conditions of employment, communication, fulfilment of legal obligations or requirements, performance of contracts, providing services to clients, etc.

1.5 Personal data shall always be:

- processed lawfully, fairly and in a transparent manner in relation to the data subject;
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- 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;
- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed;
- processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures.

1.6 BAO shall be responsible for and be able to demonstrate compliance with the above as part of BAO's accountability.

2. Legal basis for processing personal data

2.1 Processing of personal data requires a legal basis. The most predominant legal basis for processing personal data within BAO are:

- Consent from the data subject for one or more specific purposes;
- The performance of a contract to which the data subject is party;
- A legal obligation or requirement;
- Legitimate interests pursued by BAO;

2.2 Consent

2.2.1 If the collection, registration and further processing of personal data on clients, suppliers, other business relations and employees are based on such a person's consent to the processing of personal data for one or more specific purposes, BAO shall be able to demonstrate that the data subject has consented to processing of such personal data.

2.2.2 Consent shall be: freely given, specific, informed and unambiguous. The data subject must actively consent to the processing of personal data by a statement or by a clear affirmative action, to him/her.

2.2.3 A request for consent shall be presented in a manner, which is clearly distinguishable from other matters, in an intelligible and easily accessible form, using clear and plain language.

2.2.4 To process special categories of personal data (sensitive personal data) the consent shall also be explicit.

2.2.5 The data subject is entitled to withdraw his/her consent at any time and upon such withdrawal, we will stop collecting or processing personal data about that person unless we are obligated or entitled to do so based on another legal basis.

2.3 Necessary for the performance of a contract:

2.3.1 It will be legitimate to collect and process personal data relevant to the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract. This applies to all contractual obligations and agreements signed with BAO, including the pre-contractual phase irrespective of the success of the contract negotiation or not.

2.4 Comply with a legal obligation

2.4.1 BAO has to comply with various legal obligations and requirements, which have basis in Union or Member State law. Such legal obligation, to which BAO is subject, may be sufficient as a legitimate basis for processing of personal data.

2.4.2 Such legal obligations include obligations to collect, register and/or make available certain types of information relating to employees, clients, etc. Such legal requirements will then form the legal basis for us to process the personal data, however, it is important to note whether the provisions allowing or requiring BAO to process certain personal data also set out requirements in relation to storage, disclosure and deletion.

2.5 Legitimate interests

2.5.1 Data will only be processed where it is necessary for the purposes of the legitimate interests pursued by BAO, and these interests or fundamental rights are not overridden by the interests of the data subject. BAO will, when deciding to process data ensures that the legitimate interests override the rights and freedoms of the individual and that the processing would not cause unwarranted harm. For instance, it is a legitimate interest of BAO to process personal data on potential client in order to expand the business and develop new business relations. The data subject must be given information on the

specific legitimate interest if a processing is based on this provision, cf. section 4.1 below.

3. Processing and transfer of personal data

3.1 BAO as Data Controller

3.1.1 BAO will be considered a data controller to the extent that we decide by which means the data subject's personal data shall be processed e.g. when a data subject signs an agreement with BAO.

3.2 Use of data processors

3.2.1 An external data processor is a company, which processes personal data on behalf of BAO and in accordance with BAO's instructions, e.g. in relation to HR systems, third party IT providers, etc. When BAO outsources the processing of personal data to data processors, BAO ensures that said company as a minimum applies the same degree of data protection as BAO. If this cannot be guaranteed, BAO will choose another data processor.

3.3 Data processing agreements

3.3.1 Prior to transfer of personal data to the data processor, BAO shall enter into a written data processing agreement with the data processor. The data processing agreement ensures that BAO controls the processing of personal data, which takes place outside BAO for which BAO is responsible.

3.3.2 If the data processor/sub-data processor is located outside the EU/EEA, the conditions of clause 3.4.4 below will apply.

3.4 Disclosure of personal data

3.4.1 Before disclosing personal data to others, it is the responsibility of BAO to consider whether the recipient is employed by us or not. Furthermore, we may only share personal data within BAO, if we have a legitimate business purpose in the disclosure.

3.4.2 It is BAO's responsibility to ensure that the recipient has a legitimate purpose for receiving the personal data and to ensure that sharing of personal data is restricted and kept to a minimum.

3.4.3 BAO must show caution before sharing personal data with persons, data subjects or entities outside of BAO. Personal data shall only be disclosed

to third parties acting as individual data controllers if a legitimate purpose for such transfer exists. If the recipient is acting as a data processor, please refer to clause 3.2 above.

3.4.4 If the third-party recipient is located outside the EU/EEA in a country not ensuring an adequate level of data protection, the transfer can only be completed if a transfer agreement has been entered into between BAO and the third party. The transfer agreement shall be based on the EU Standard Contractual Clauses.

4. Rights of the data subjects

4.1 Duty of information

4.1.1 When BAO collects and registers personal data on data subjects BAO is obligated to inform such persons about:

- The purposes of the processing for which the personal data are intended as well as the legal basis for the processing;
- The categories of personal data concerned;
- The legitimate interests pursued by BAO, if the processing is based on a balancing of interests;
- The recipients or categories of recipients of the personal data, if any;
- Where applicable, the fact that BAO intends to transfer personal data to a third country and the legal basis for such transfer;
- The period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;
- The existence of the right to request from BAO access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability;
- Where the processing is based on the data subject's consent, the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;
- The right to lodge a complaint with BAO via the correct procedure or with a supervisory authority;
- Whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data;
- The existence of automated decision-making, including profiling, and meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

This information will in most cases be provided via a privacy notice on BAO's home page.

4.2 Right to access

4.2.1 Any person whose personal data BAO is processing, including, but not limited to, BAO employees, job applicants, external suppliers, clients, potential clients, business partners, etc. has the right to request access to the personal data which BAO processes or stores about him/her.

4.2.2 If BAO processes or stores personal data about the data subject, the data subject shall have the right to access the personal data and the reasons for the data to be processed in relation to the criteria set out in 4.1.1.

4.3 The data subject shall have the right to obtain from BAO without undue delay the rectification of inaccurate personal data concerning him or her.

4.4 The data subject shall have the right to obtain from BAO the erasure of personal data concerning him or her and BAO shall have the obligation to erase personal data without undue delay, unless required by law to retain any information for a prescribed period of time, for example, by financial regulators or tax authorities.

4.5 The data subject shall have the right to obtain from BAO restriction of processing, if applicable.

4.6 The data subject shall have the right to receive the personal data registered in a structured and commonly used and machine-readable format, if applicable.

4.7 The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her which is based on a balancing of interests, including profiling.

4.8 Any requests received from a data subject to exercise the rights in this clause will be answered as soon as reasonably possible, and no later than 30 days from receipt. Requests shall be forwarded without delay to BAO's Support Team (bao@baofinancial.com).

5. Data Protection by Design and Data Protection by Default

5.1 New products, services, technical solutions, etc. must be developed so that they meet the principles of data protection by design and data protection by default.

5.1.1 Data protection by design means that when designing new products or services due consideration to data protection is taken.

- BAO will consider the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing.
- BAO shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymization, which are designed to implement data protection principles, such as data minimization, in an effective manner and to integrate the necessary safeguards into the processing in order to meet data protection requirements and protect the rights of data subjects.

5.1.2 Data protection by default requires that relevant data minimization techniques are implemented.

- BAO shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which is necessary for each specific purpose of the processing is processed.
- This minimisation requirement applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility.
- Such measures shall ensure that by default personal data is not made accessible without careful consideration.

6. Records of processing activities

6.1 BAO shall as data controller maintain records of processing activities under BAO's responsibility. The records shall contain the following information:

- the name and contact details of;
- the purposes of the processing;
- a description of the categories of data subjects and of the categories of personal data;
- the recipients to whom the personal data have been or will be disclosed, including recipients in third countries or international organizations;
- where applicable, transfers of personal data to a third country, including the identification of that third country and, if relevant, the documentation of suitable safeguards;
- where possible, the envisaged time limits for erasure of the various categories of data;
- where possible, a general description of the applied technical and organisational security measures.

6.1.1 BAO shall make the records available to relevant data protection authorities upon request.

7. Deletion of personal data

7.1 Personal data shall be deleted when BAO no longer has a legitimate purpose for the continuous processing or storage of the personal data, or when it is no longer required to store the personal data in accordance with applicable legal requirements.

7.2 Detailed retention periods with respect to various categories of personal data are specified in BAO's Data Retention and Information Sharing policy.

8. Assessment of risk

8.1 If BAO processes personal data that is likely to result in a high risk for the persons whose personal data is being processed, a Data Protection Impact Assessment ("DPIA") shall be carried out.

> 8.1.1 A DPIA implies that BAO will, taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with data protection requirements.

8.2 The technical and organisational measures shall be reviewed and updated where necessary and no later than every 6 months.

8.2.1 Adherence to approved codes of conduct or approved certification mechanisms may be used as an element by which to demonstrate compliance with the appropriate technical and organisational measures pursuant to this clause.

9. National requirements

9.1 BAO shall comply with both the GDPR and national data protection legislation.

9.2 If applicable national legislation requires a higher level of protection for personal data than such policies/guidelines, such stricter requirements are to be complied with. If BAO's policies/guidelines are stricter than the local legislation, our policies/guidelines must be complied with.

10. Contact and complaints

10.1 If you have any questions regarding the content of this policy, please contact BAO's Data Protection officer at bao@baofinancial.com.
10.2 If you would like to file a complaint about BAO's processing of personal data, please contact the Cyprus Data Protection Agency.