Data Privacy Statement

v2.0_14/05/18

Bluefin Trading Ltd. is committed to being transparent about how it collects and uses personal data and to meeting its data protection obligations. This statement sets out its commitment to data protection. This statement applies to the personal data of clients, suppliers, contacts, third parties or other personal data processed for business purposes. The personal data of job applicants, employees, contractors, interns, apprentices and former employees, referred to as HR-related personal data is covered by our HR Data Protection Policy. The wording in this statement reflects the requirements of the General Data Protection Regulation (GDPR), which comes into effect on 25 May 2018.

Bluefin has appointed the Data Manager as the person with responsibility for data protection compliance. Questions about this statement, or requests for further information, should be directed to the Data Manager, Bluefin Trading Ltd, Keelham Farm, Hebden Bridge, HX7 8TG.

1. Interpretation

Automated Decision-Making (ADM): when a decision is made which is based solely on Automated Processing (including profiling) which produces legal effects or significantly affects an individual. The GDPR prohibits Automated Decision-Making (unless certain conditions are met) but not Automated Processing.

Automated Processing: any form of automated processing of Personal Data consisting of the use of Personal Data to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning that individual's performance at work, health, preferences, interests, reliability, behaviour, location or movements. Profiling is an example of Automated Processing.

Organisation: Bluefin Trading Ltd

Consent: agreement which must be freely given, specific, informed and be an unambiguous indication of the Data Subject's wishes by which they, by a statement or by a clear positive action, signify agreement to the processing of Personal Data relating to them.

Data Controller: the person or organisation that determines when, why and how to process Personal Data. It is responsible for establishing practices and policies in line with the GDPR. We are the Data Controller of all Personal Data used in our business for our own business purposes.

Data Subject: a living, identified or identifiable individual about whom we hold Personal Data. Data Subjects may be nationals or residents of any country and may have legal rights regarding their Personal Data.

Data Privacy Impact Assessment (DPIA): assessments used to identify and reduce risks of a data processing activity. DPIA can be carried out as part of Privacy by Design and should be conducted for all major system or business change programs involving the processing of Personal Data.

EEA: the 28 countries in the EU and Iceland, Liechtenstein and Norway.

Explicit Consent: consent which requires a very clear and specific statement.

General Data Protection Regulation (GDPR): the General Data Protection Regulation. Personal Data is subject to the legal safeguards specified in the GDPR.

Personal Data: any information identifying a Data Subject or information relating to a Data Subject that we can identify (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access. Personal Data includes Sensitive Personal Data and Pseudonymised Personal Data but excludes anonymous data or data that has had the identity of an individual permanently removed. Personal data can be factual (for example, a name, email address, location or date of birth) or an opinion about that person's actions or behaviour.

Personal Data Breach: any act or omission that compromises the security, confidentiality, integrity or availability of Personal Data or the physical, technical, administrative or organisational safeguards that we or our third-party service providers put in place to protect it. The loss, or unauthorised access, disclosure or acquisition, of Personal Data is a Personal Data Breach.

Privacy by Design: implementing appropriate technical and organisational measures in an effective manner to ensure compliance with the GDPR.

Privacy Notices or Statements: separate notices setting out information that may be provided to Data Subjects when the organisation collects information about them.

Processing or process: any activity that involves the use of Personal Data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transmitting or transferring Personal Data to third parties.

Pseudonymisation: replacing information that directly or indirectly identifies an individual with one or more artificial identifiers or pseudonyms so that the person, to whom the data relates, cannot be identified without the use of additional information which is meant to be kept separately and secure.

Related Policies: the organisation's policies, operating procedures or processes related to this Privacy Statement and designed to protect Personal Data.

Sensitive Personal Data: information revealing racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions, sexual life, sexual orientation, biometric or genetic data, and Personal Data relating to criminal offences and convictions.

2. Scope

We recognise that the correct and lawful treatment of Personal Data will maintain confidence in the organisation and will provide for successful business operations. Protecting the confidentiality and integrity of Personal Data is a critical responsibility that we take seriously at all times.

The Data Manager is responsible for overseeing this Privacy Statement and, as applicable, developing Related Policies and guidelines. Please contact the Data Manager with any questions about the operation of this Privacy Statement or the GDPR or if you have any concerns that this Privacy Statement is not being or has not been followed.

We adhere to the principles relating to processing of Personal Data set out in the GDPR which require Personal Data to be:

(a) Processed lawfully, fairly and in a transparent manner (Lawfulness, Fairness and Transparency).
(b) Collected only for specified, explicit and legitimate purposes (Purpose Limitation).
(c) Adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed (Data Minimisation).
(d) Accurate and where necessary kept up to date (Accuracy).
(e) Not kept in a form which permits identification of Data Subjects for longer than is necessary for the purposes for which the data is processed (Storage Limitation).
(f) Processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful Processing and against accidental loss, destruction or damage (Security, Integrity and Confidentiality).
(g) Not transferred to another country without appropriate safeguards being in place (Transfer Limitation).
(h) Made available to Data Subjects who are allowed to exercise certain rights in relation to their Personal Data (Data Subject's Rights and Requests).

We will demonstrate compliance with the data protection principles listed above (Accountability).

3. Lawfulness, fairness, transparency

3.1 Lawfulness and fairness

Personal data will be processed lawfully, fairly and in a transparent manner in relation to the Data Subject. We will only collect, process and share Personal Data fairly and lawfully and for specified purposes. The GDPR restricts our actions regarding Personal Data to specified lawful purposes. These restrictions are not intended to prevent processing but to ensure that we process Personal Data fairly and without adversely affecting the Data Subject.

The GDPR allows processing for specific purposes, some of which are set out below:

(a) where the Data Subject has given Consent;
(b) if the processing is necessary for the performance of a contract with the Data Subject;
(c) to meet our legal compliance obligations;
(d) to protect the Data Subject's vital interests;
(e) to pursue our legitimate interests for purposes where they are not overridden because the processing prejudices the interests or fundamental rights and freedoms of Data Subjects. The purposes will be set out in applicable Privacy Notices.

We identify and document the legal ground being relied on for each processing activity.

3.2 Consent

We will only process Personal Data on the basis of one or more of the lawful bases set out in the GDPR, which include Consent. A Data Subject consents to processing of their Personal Data if they indicate agreement clearly either by a statement or positive action. Consent requires affirmative action so silence, pre-ticked boxes or inactivity are unlikely to be sufficient. If Consent is given in a document which deals with other matters, then the Consent will be kept separate from those other matters. Data Subjects can withdraw Consent to processing at any time and withdrawal will be promptly honoured. Consent may need to be refreshed if we intend to process Personal Data for a different and incompatible purpose which was not disclosed when the Data Subject first consented.

Unless we can rely on another legal basis of processing, Explicit Consent will be required for processing Sensitive Personal Data, for Automated Decision-Making and for cross border data transfers. Usually we will be relying on another legal basis (and not require Explicit Consent) to process Sensitive Data. Where Explicit Consent is required, we will issue a notice to the Data Subject.

We will keep records of all Consents so that we can demonstrate compliance with Consent requirements.

3.3 Transparency (notifying data subjects)

The GDPR requires Data Controllers to provide detailed, specific information to Data Subjects. Whenever we collect Personal Data directly from Data Subjects, including for human resources or employment purposes, we will provide the Data Subject with all the information required by the GDPR including the identity of the Data Controller, how and why we will use, process, disclose, protect and retain that Personal Data.

When Personal Data is collected indirectly (for example, from a third party or publicly available source), we will provide the Data Subject with all the information required by the GDPR as soon as possible after collecting/receiving the data. We will check that the Personal Data was collected by the third party in accordance with the GDPR and on a basis which contemplates our proposed processing of that Personal Data.

4. Purpose limitation

Personal Data will be collected only for specified, explicit and legitimate purposes. It will not be further processed in any manner incompatible with those purposes. We will not use Personal Data for new, different or incompatible purposes from that disclosed when it was first obtained unless we have informed the Data Subject of the new purposes and they have Consented where necessary.

5. Data minimisation

Personal Data will be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed. Our personnel will not process Personal Data for any reason unrelated to their job duties. When Personal Data is no longer needed for specified purposes, it will be deleted or anonymised in accordance with our data retention guidelines.

6. Accuracy

Personal Data will be accurate and, where necessary, kept up to date. It will be corrected or deleted without delay when inaccurate. We will ensure that the Personal Data we use and hold is accurate, complete, kept up to date and relevant to the purpose for which we collected it. We will take all reasonable steps to destroy or amend inaccurate or out-of-date Personal Data.

7. Storage limitation

Personal Data will not be kept in an identifiable form for longer than is necessary for the purposes for which the data is processed. We will not keep Personal Data in a form which permits the identification of the Data Subject for longer than needed for the legitimate business purposes for which we originally collected it including for the purpose of satisfying any legal, accounting or reporting requirements. We will take all reasonable steps to destroy or erase from our systems all Personal Data that we no longer require in accordance with our records' retention policies. This includes requiring third parties to delete such data where applicable. We will inform Data Subjects of the period data is stored and how that period is determined.

8. Security integrity and confidentiality

8.1 Protecting Personal Data

Personal Data will be secured by appropriate technical and organisational measures against unauthorised or unlawful processing, and against accidental loss, destruction or damage. We will develop, implement and maintain safeguards appropriate to our size, scope and business, available resources, amount of Personal Data that we own or maintain on behalf of others and identified risks (including use of encryption and Pseudonymisation where applicable). We will regularly evaluate and test the effectiveness of those safeguards to ensure security of our processing of Personal Data.

We will maintain data security by protecting the confidentiality, integrity and availability of the Personal Data, defined as follows:

(a) Confidentiality means that only people who have a need to know and are authorised to use the Personal Data can access it.
(b) Integrity means that Personal Data is accurate and suitable for the purpose for which it is processed.
(c) Availability means that authorised users are only able to access the Personal Data when they need it for authorised purposes.

8.2 Reporting a Personal Data Breach

The GDPR requires Data Controllers to notify any Personal Data Breach to the applicable regulator and, in certain instances, the Data Subject. We have put in place procedures to deal with any suspected Personal Data Breach and will notify Data Subjects or any applicable regulator where we are legally required to do so.

9. Transfer limitation

The GDPR restricts data transfers to countries outside the EEA in order to ensure that the level of data protection afforded to individuals is not undermined. We will only transfer Personal Data outside the EEA if one of the following conditions applies:

(a) the European Commission has issued a decision confirming that the country to which we transfer the Personal Data ensures an adequate level of protection for the Data Subjects' rights and freedoms;
(b) appropriate safeguards are in place;
(c) the Data Subject has provided Explicit Consent to the proposed transfer after being informed of any potential risks, or
(d) the transfer is necessary for one of the other reasons set out in the GDPR including the performance of a contract between us and the Data Subject; public interest; to establish, exercise or defend legal claims, or to protect the vital interests of the Data Subject where the Data Subject is physically or legally incapable of giving Consent, and in some limited cases, for our legitimate interest.

10. Data Subject's rights

Data Subjects have rights when it comes to how we handle their Personal Data. These include rights to:

(a) withdraw Consent to processing at any time;
(b) receive certain information about the Data Controller's processing activities;
(c) request access to their Personal Data that we hold;
(d) prevent our use of their Personal Data for direct marketing purposes;
(e) ask us to erase Personal Data if it is no longer necessary in relation to the purposes for which it was collected or processed or to rectify inaccurate data/complete incomplete data;
(f) restrict processing in specific circumstances;
(g) challenge processing which has been justified on the basis of our legitimate interests or in the public interest;
(h) request a copy of an agreement under which Personal Data is transferred outside of the EEA;
(i) object to decisions based solely on Automated Processing, including profiling (ADM);
(j) prevent processing that is likely to cause damage or distress to the Data Subject or anyone else;
(k) be notified of a Personal Data Breach which is likely to result in high risk to their rights and freedoms;
(l) make a complaint to the supervisory authority, and
(m) in limited circumstances, receive or ask for their Personal Data to be transferred to a third party in a structured, commonly used and machine readable format.

We will verify the identity of an individual requesting data under any of the rights listed above.

11. Accountability

11.1 We will implement appropriate technical and organisational measures in an effective manner, to ensure compliance with data protection principles. We have adequate resources and controls in place to ensure and to document GDPR compliance including:

(a) appointing a suitably qualified manager accountable for data privacy;
(b) implementing Privacy by Design when processing Personal Data and completing DPIAs where processing presents a high risk to rights and freedoms of Data Subjects;
(c) integrating data protection into internal documents;
(d) regularly training our personnel on the GDPR and data protection matters including Data Subject's rights, Consent, legal bases, DPIA and Personal Data Breaches, and
(e) regularly testing privacy measures and conducting reviews to assess compliance.

11.2 Record keeping

The GDPR requires us to keep full and accurate records of our data processing activities. These records include the name and contact details of the Data Controller, clear descriptions of the Personal Data types, Data Subject types, processing activities, processing purposes, third-party recipients of the Personal Data, storage locations, transfers, retention periods and a description of security measures in place.

11.3 Training

We will ensure all personnel have undergone adequate training to enable them to comply with data privacy laws.

11.4 Privacy By Design and Data Protection Impact Assessment (DPIA)

We are required to implement Privacy by Design measures when processing Personal Data by implementing appropriate technical and organisational measures (like Pseudonymisation) in an effective manner, to ensure compliance with data privacy principles. We will take into account the following:

(a) the state of the art;
(b) the cost of implementation;
(c) the nature, scope, context and purposes of processing, and
(d) the risks, likelihood and severity for rights and freedoms of Data Subjects posed by the processing.

We will also conduct DPIAs in respect to high risk processing.

11.5 Automated Processing (including profiling) and Automated Decision-Making

Generally, ADM is prohibited when a decision has a legal or similar significant effect on an individual unless:

(a) a Data Subject has Explicitly Consented;
(b) the processing is authorised by law, or
(c) the processing is necessary for the performance of or entering into a contract.

If certain types of Sensitive Data are being processed, then grounds (b) or (c) will not be allowed but such Sensitive Data can be processed where it is necessary for substantial public interest like fraud prevention. If a decision is to be based solely on Automated Processing (including profiling), then Data Subjects will be informed of their right to object. Suitable measures will be put in place to safeguard the Data Subject's rights, freedoms and legitimate interests. We will inform the Data Subject of the logic involved in the decision making or profiling, the significance and envisaged consequences and give the Data Subject the right to request human intervention, express their point of view or challenge the decision. A DPIA will be carried out before any Automated Processing (including profiling) or ADM activities are undertaken.

11.6 Direct marketing

We will specifically offer the right to object to direct marketing. A Data Subject's objection to direct marketing will be promptly honoured. If a client opts out at any time, their details will be suppressed as soon as possible. Suppression involves retaining just enough information to ensure that marketing preferences are respected in the future.

11.7 Sharing Personal Data

Generally we are not allowed to share Personal Data with third parties unless certain safeguards and contractual arrangements have been put in place. We will only share the Personal Data we hold if the recipient has a job-related need to know the information and the transfer complies with any applicable cross-border transfer restrictions. We will only share the Personal Data we hold with third parties, such as our service providers, if:

(a) they have a need to know the information for the purposes of providing the contracted services;
(b) sharing the Personal Data complies with a Privacy Notice provided to the Data Subject and, if required, the Data Subject's Consent has been obtained;
(c) the third party has agreed to comply with required data security;
(d) the transfer complies with any applicable cross border transfer restrictions, and
(e) a fully executed written contract that contains GDPR approved third party clauses has been obtained.

12. Changes to this Privacy Statement

We reserve the right to change this Privacy Statement at any time so please check back regularly to obtain the latest copy of this Statement. This Privacy Statement does not override any applicable data privacy laws and regulations.