JonesTrading International

Data Protection Policy

Introduction

JonesTrading International Limited (the "**Firm**") needs to collect and use certain types of information about the Data Subjects who come into contact with it in order to carry on its work. This personal information must be collected and dealt with appropriately – whether on paper, in a computer, or recorded on other material – and there are safeguards to ensure this under the Data Protection Act 1998.

The Firm is suitably registered at the Information Commissioner's Office (the "**ICO**") and is able to process data worldwide.

The Firm's Data Protection Policy (the "**Policy**") applies to all its directors, officers, employees, consultants, contractors and secondees (collectively, "**Personnel**").

Definitions

"**Data Controller**"	means the person who (either alone or with others) decides what personal information the Firm will hold and how it will be held or used.
"**Act**"	means the Data Protection Act 1998, the UK legislation that provides a framework for responsible behaviour by those using personal information.
"**Data Protection Officer**"	means the person responsible for ensuring that the Firm adheres to its data protection policy and complies with the Act is **the Firm's Compliance Officer.**
"**Data Subject/Service User**"	means the individual whose personal information is being held or processed by the Firm, for example: a client, an employee, a supporter.
"**Explicit Consent**"	means a freely given, specific and informed agreement by a Data Subject to the processing of personal information about him/ her. Explicit consent is needed for processing sensitive data.
"**Notification**"	means notifying the ICO about the data processing activities of the Firm as certain activities may be exempt from notification.
"**Information Commissioner**"	means the UK's ICO responsible for implementing and overseeing the Act.

"**Processing**"	means collecting, amending, handling, storing or disclosing personal information.
"**Personal Information**"	means information about living individuals that enables them to be identified – e.g. name and address. It does not apply to information about companies and agencies but it does apply to named person(s) or employee(s) within the Firm.
"**Sensitive Data**"	means data about: • racial or ethical origin; • political options; • religious or similar beliefs; • trade union membership; • physical or mental health; • sexual life; • criminal record; and • criminal proceedings relating to a data subject's offences.

Data Controller

The Firm's Compliance Officer is the Data Controller under the Act, which means that s/he is responsible for determining what purposes personal information is held for and how they will be used. It is also his/her responsible for notifying the ICO of the data the Firm holds or is likely to hold, and the general purposes for which this data will be used.

Disclosure

The Data Subject will be made aware in most circumstances how and with whom their information will be shared. There are circumstances where the law allows certain recipients to disclose data, including sensitive data, without the Data Subject's consent. These are:

1. carrying out a legal duty or as authorised by any of the UK's Secretary of State;
2. protecting vital interests of a Data Subject or other person;
3. the Data Subject has already made the information public;
4. conducting any legal proceedings, obtaining legal advice or defending any legal rights;
5. monitoring for equal opportunities purposes – i.e. race, disability or religion;

6. providing a confidential service where the Data Subject's consent cannot be obtained or where it is reasonable to proceed without consent: e.g. where we would wish to avoid forcing stress or illness upon the Data Subjects by providing consent signatures.

The Firm regards the lawful and correct treatment of personal information as very important to successful working, and to maintaining the confidence of those with whom we deal. The Firm intends to ensure that personal information is treated lawfully and correctly.

To this end, the Firm will adhere to the Principles of Data Protection as detailed in the Act.

Specifically, the Principles require that Personal Information:

1. shall be processed fairly and lawfully and, in particular, shall not be processed unless specific conditions are met;
2. shall be obtained only for one or more of the purposes specified in the Act, and shall not be processed in any manner incompatible with that purpose or those purposes;
3. shall be adequate, relevant and not excessive in relation to those purpose(s);
4. shall not be kept for longer than is necessary;
5. shall be processed in accordance with the rights of data subjects under the Act;
6. shall be kept secure by the Data Controller who takes appropriate technical and other measures to prevent unauthorised or unlawful processing or accidental loss or destruction of, or damage to, personal information;
7. shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal information.

The Firm will, through both appropriate management and strict application of criteria and controls:

- observe fully conditions regarding the fair collection and use of information;
- meet its legal obligations to specify the purposes for which information is used;
- collect and process appropriate information, and only to the extent that it is needed to fulfil its operational needs or to comply with any legal requirements;
- ensure the quality of information is used;
- ensure that the rights of people about whom information is held, can be fully exercised under the Act, including:
    - the right to be informed that processing is being undertaken;
    - the right of access to one's personal information;
    - the right to prevent processing in certain circumstances; and
    - the right to correct, rectify, block or erase information which is regarded as wrong information;

- take appropriate technical and organisational security measures to safeguard personal information;
- ensure that personal information is not transferred abroad without suitable safeguards;
- treat people justly and fairly whatever their age, religion, disability, gender, sexual orientation or ethnicity when dealing with requests for information; and
- set out clear procedures for responding to requests for information.

Data Collection

Informed Consent

"**Informed Consent**" is when:

- a Data Subject clearly understands why their information is needed, who it will be shared with, the possible consequences of them and agreeing or refusing the proposed use of the data; and
- subsequently, gives their consent.

The Firm will ensure that data is collected within the boundaries defined in this Policy. This applies to data that is collected in person, or by completing a form.

When collecting data, the Firm will ensure that the Data Subject:

- clearly understands why the information is needed;
- understands what it will be used for and what the consequences will be should the Data Subject decide not to give consent to processing;
- as far as reasonably possible, grants explicit consent, either written or verbal for data to be processed;
- as far as reasonably practicable, is competent enough to give consent and has given so freely without any duress; and
- has received sufficient information on why their data is needed and how it will be used.

Data Security

Information and records relating to service users will be stored securely and will only be accessible to authorised Personnel and volunteers.

Personal Information on data subjects/service users is not disclosed either orally or in writing or otherwise to any unauthorised third party.

Information will be stored for only as long as it is needed or as required by statute and will be disposed of appropriately.

It is the Firm's responsibility to ensure all personal and company data is non-recoverable from any computer system previously used within the organisation which has been passed on/sold to a third party.

The FCA has issued a set of good practice guidelines to ensure that firms are adequately protected:-

1. Firms should assess the risk of unauthorised access to the firm's premises and ensure a commensurate level of security to protect the firm's customer data.
2. Firms should have written data security policies and procedures, which are proportionate, accurate and relevant to the firm's day-to-day business;
3. Firms should be applying a risk-based approach to reducing financial crime and enhancing recruitment check where appropriate;
4. Firms should put in place simple and effective methods to raise awareness and periodically test Personnel's understanding of data security;
5. Firms should consider whether the Personnel who changed roles should retain access rights that they no longer need and to conduct regular reviews of individuals' IT access rights;
6. Firms should maintain a clear record of who owns laptops and memory sticks to ensure that the firm would notice if one had been lost or stolen. It is good practice that any laptops or other portable devices are encrypted;
7. Firms should provide internet and email facilities only to Personnel with a genuine business need. The firm should also completely block access to internet facilities, such asocial networking sites, instant messaging, etc., especially if the Personnel have access to customer data;
8. Firms should securely dispose of its data by shredding all confidential waste in-house or by using a specialist secure disposal company;
9. If using third party suppliers, the firm should satisfy itself that it knows its third party suppliers, how they vet their Personnel and have a good understanding of their security arrangements; and
10. The compliance officer of the firm should check whether data security policies or procedures are being followed.

Data Subject access and accuracy

All individuals who are the subject of personal data held by the Firm are entitled to:

• ask what information the Firm holds about them and why;
• ask how to gain access to it;
• be informed how to keep it up to date; and
• be informed what the Firm is doing to comply with its obligations under the Act.

The Firm will also take reasonable steps to ensure that this information is kept up to date by asking data subjects whether there have been any changes.

In addition, the Firm will ensure that:

1. it has a Data Protection Officer with specific responsibility for ensuring compliance with Data Protection;
2. everyone processing personal information understands that they are contractually responsible for following good data protection practice;
3. everyone processing personal information is appropriately trained to do so;
4. everyone processing personal information is appropriately supervised;
5. anybody wanting to make enquires about handling personal information knows what to do;
6. it deals promptly and courteously with any enquires about handling personal information;
7. it describes clearly how it handles personal information;
8. it will regularly review and audit the ways it holds, manages and uses personal information;
9. it regularly assesses and evaluates its methods and performance in relation to handling personal information; and
10. all Personnel are aware that breach of the rules and procedures identify in this Policy may lead to disciplinary action being taken against them.

Breach

If the Firm discovers that any data has been lost or believes there has been a breach of the data protection principle in the way the data is being handled, the Firm's Personnel will notify the Data Controller immediately.

The Firm's priority must always be to close or contain the breach and mitigate the risk to the Data Subjects that may be affected by it.

Future development

This Policy will be updated as necessary to reflect best practice in data management, security and control and to ensure compliance with any changes or amendments made to the Act.

In case of any queries or questions in relation to this Policy, please contact the Data Controller.