BetIndex Limited

Data Protection Policy

Charter Place
23-27 Seaton Place
St Helier
Jersey
JE1 1JY

1 Contents

2 Definitions

Act	Data Protection (Jersey) Law 2005
Board	Board of Directors of BetIndex Limited
Company	BetIndex Limited
Data	Means information which – a) is being processed by means of equipment operating automatically in response to instructions given for that purpose; b) is recorded with the intention that it should be processed by means of such equipment; c) is recorded as part of a Relevant Filing System or with the intention that it should form part of a Relevant Filing System;
Data Controller	The determination of the purposes for which the manner in which any Personal Data are, or are to be, processed
Data Processor	Any person (other than an employee of the Data Controller) who processes the data on behalf of the Data Controller
Data Protection Commissioner	The supervisory authority responsible for enforcing the provisions of the Act in Jersey
Data Subject	The individual who is the subject of Personal Data
Personal Data	Data which relates to a living individual who can be identified- a) from those Data; or b) from those Data and other information which is in the possession of, or is likely to come into the possession of, the Data Controller and includes any expression of opinion about the individual and any indication of the intentions of the Data Controller or any other person in respect of the individual
Policy	This Data Protection Policy
Processing	In relation to information or Data, means obtaining, recording or holding the information or Data or carrying out any operation or set of operations on the information of Data, including- a) organisation, adaption or alteration of the information of Data; b) retrieval, consultation, or use of the information or Data; c) disclosure of the information or Data by transmission, dissemination or otherwise making available, or d) alignment, combination, blocking, erasure or destruction of the information or Data
Relevant Filing System	Any set of information relating to individuals to the extent that, although the information is not processed by electronic means of equipment operating automatically in response to instructions given for

	that purpose, the set is structured, either by way of reference to individuals or by reference to criteria relating to individuals, in such a way that specific information relating to a particular individual is readily accessible.
Sensitive Personal Data	Means Personal Data consisting of information as to- a) the racial or ethnic origin of the Data Subject; b) his political opinions; c) his religious beliefs or other beliefs of a similar nature; d) whether he is a member of a trade union (within the meaning of the Trade Unions Act 1991); e) his physical or mental health or condition; f) his sexual life; g) the commission or alleged commission by him of any offence; or h) any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings

3 Introduction and Policy Statement

The Company is committed to complying with the requirements of the Act and recognises the importance of Personal Data to the business. It is imperative that the Company respects and adheres to the privacy rights of any individual on whom it holds Personal Data.

This Policy outlines the principles upon which the Company will process Personal Data in order to safeguard its business and to respect the rights of individuals when Processing their Personal Data in accordance with the Act.

Furthermore, this Policy also outlines the Company's procedures when engaging with Data Processors to ensure compliance between both parties in accordance with the Act.

It is the responsibility of all employees, contractors, agents, consultants, partners or other parties working on behalf of the Company to ensure compliance with this Policy. Failure to comply with this Policy and the Act may be of detrimental effect to the Company.

4 Data Protection Principles

The Act sets out eight data protection principles which must be adhered to by the Data Controller in relation to the processing of all Personal Data.

The Company also engages Data Processor(s) to process Personal Data on its behalf, such Data Processor(s) must, pursuant to the agreement entered into by both parties, comply with the eight principles in their processing of Personal Data on behalf of the Company.

The eight principles of the Act are as follows:

1. Personal Data shall be processed fairly and lawfully
2. Personal Data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes
3. Personal Data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed
4. Personal Data shall be accurate and, where necessary, kept up to date
5. Personal Data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes
6. Personal Data shall be processed in accordance with the rights of data subjects under the Act
7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of Personal Data and against accidental loss or destruction of, or damage to, Personal Data
8. Personal Data 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 of Data Subjects in relation to the Processing of Personal Data

5 Data Protection Principles Detailed

Principle 1

'Personal Data Shall be processed fairly and lawfully'

This means the Company must:

- Have legitimate reasons for collecting and using, including sharing, Personal Data
- Not use Personal Data in ways that have unjustified adverse effects on the individuals concerned
- Be open and honest about how you intend to use the Personal Data;
- Give appropriate 'privacy policies' or 'fair processing notices' when collecting Personal Data
- Handle individuals Personal Data only in ways they would reasonably expect
- Ensure that individuals are not misled or deceived about the use of their information
- Make sure we do not do anything unlawful with Personal Data

Processing Personal Data will be lawful if it meets one of the following conditions:

- With the consent of the individual
- For the performance of a contract with the individual
- To comply with a legal obligation
- To protect the vital interests of the individual
- For the administration of justice, or the exercise of any statutory function
- For the legitimate interests of the organisation, unless the interests of the individual would be prejudiced

Processing Sensitive Personal Data will be lawful if it meets one of the following conditions:

- Explicit consent has been given by the individual;

Or the Processing is necessary for the following reasons:

- Exercising or performing any right or legal obligation conferred or imposed by law in connection with employment
- To protect the vital interests of the individual or another person if consent cannot be given by, or on behalf of, the individual, or the data controller cannot be reasonably expected to obtain the consent of the data subject

- In order to protect the vital interests of another person in the case where consent by, or on behalf or, the individual has been unreasonably withheld
- For the purpose of, or in connection with, any legal proceedings, including prospective legal proceedings
- For obtaining legal advice
- Establishing, exercising or defending legal rights
- Administration of justice
- Exercise of any function of the Crown, a Department of Statutory Board
- For medical purposes and is undertaken by a health professional or a person owing an equivalent duty of confidentiality to a health professional
- Substantial public interest
- For the exercise of any functions conferred on a constable by any rule of law

The Company's privacy policy sets out the purpose of collecting Personal Data from individuals. It is important that all employees, contractors, agents, consultants, partners or other parties working on behalf of the Company are aware of and understand the Company's privacy policy. Personal Data should not be processed unless such Processing meets one of the legitimising conditions set out above.

Principle 2

'Personal Data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with the purpose or those purposes'

There are evident links between the second principle and the other data protection principles. Principle 2 inherently carries an obligation on the Company to make known the purposes for which Personal Data are required, both to the Data Subject and the Data Protection Supervisor.

The principle obliges the Data Controller to identify the purpose(s) for which Personal Data are to be processed, prior to obtaining Data. Personal Data obtained for the purpose(s) must only be processed according to those specified purpose(s).

The Company ensures that:

- It is clear from the outset about why we are collecting Personal Data and what we intend to do with it (as set out in our privacy policy)
- It complies with the Act's fair Processing requirements. This includes the duty to give privacy notices when collecting their Personal Data
- It notifies the Data Protection Commissioner of the purposes of Processing Personal Data
- If we wish to process Personal Data for any purpose that is additional to or different from the originally specified purpose, the new Processing is fair. In this instance the Company would be required to notify the Data Protection Commissioner within 28 days of such a change in Processing

Principle 3

Personal Data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed'

The third principle means that the Company should ensure that:

- We hold Personal Data about an individual that is sufficient for the purpose we are holding it for in relation to that individual
- We do not hold more information than we need for that purpose

This applies to all instances of Data collection.

The Company ensures that it assesses the extent of Personal Data required for each particular purpose.

For example, when obtaining verification on an individual it would be considered excessive to request more than is necessary in order to verify their details, such as a request for a birth certificate or bank statement. However, when enhanced due diligence is required the Company would consider it adequate, proportionate and relevant to request such.

Principle 4

'Personal Data shall be accurate and, where necessary, kept up to date'

In order to comply with the fourth principle the Company should:

- Take reasonable steps to ensure the accuracy of any Personal Data obtained
- Ensure that the source of any Personal Data is clear
- Carefully consider any challenges to the accuracy of information
- Consider whether it is necessary to update the information

Where the Company uses its own resources to compile Personal Data about an individual, the Company must ensure that such information is correct. Particular care should be taken where the information could have serious implications for the individual.

Where the Company obtains Personal Data from the individual or a third party it may be practical to check the accuracy of the Personal Data provided, however, the Act states that if the Company are holding inaccurate Personal Data it will not be considered to have breached the fourth principle as long as:

- The Company has accurately recorded information provided by the individual concerned, or by an organisation
- The Company has taken reasonable steps in the circumstances to ensure accuracy of information

Where an individual challenges the accuracy of their Personal Data the Company should consider whether the information held is accurate. If the Personal Data is inaccurate it should be updated immediately.

Principle 5

'Personal Data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes'

The fifth data protection principle means that the Company should:

- Review the length of time it keeps Personal Data
- Consider the purpose or purposes for which the Company holds Personal Data in deciding whether (and for how long) to retain it
- Securely delete information that is no longer needed for the purpose or purposes
- Update, archive and securely delete information if it goes out of date

Please refer to the Company's data retention and destruction procedure detailed within section 6 of this Policy.

Principle 6

'Personal Data shall be processed in accordance with the rights of the Data Subjects under the Act'

The sixth data protection principle refers to the rights of individuals, which are:

- A rights of access to information comprising their Personal Data
- A right to object to processing that is likely to cause or is causing unwarranted and substantial damage or distress
- A right to prevent processing for direct marketing
- A right to object to decisions being taken by automated means
- A right in certain circumstances to have inaccurate Personal Data rectified, blocked, erased or destroyed
- A right to claim compensation for damages and distress caused by the Act
- A right to complain to the Data Protection Commissioner

Should the Company receive a request from an individual to access information comprising their Personal Data, also known as a 'subject access request' please refer to section 7 of this Policy.

Principle 7

'Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of Personal Data and against accidental loss or destruction of, or damage to, Personal Data'

The seventh principle means that the Company must have appropriate technical and organisational measures in place to prevent the Personal Data held by the Company being accidently or deliberately compromised. This goes beyond simply ensuring that Personal Data held in paper form is kept in a secure environment and that Personal Data held on computer systems is protected by secure passwords.

Data security is paramount to the Company's compliance with the Act. Examples of technical and organisational measures are as follows:

Technical Measures

- Password protection
- Locking of idle computer terminals
- Appropriate virus checking software and firewalls
- Unique login credentials

Organisational Measures

- Appropriate data protection training
- Staff screening
- Physical access controls

Further details on data security can be found in section 8 of this Policy.

Principle 8

'Personal Data 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 of Data Subjects in relation to the Processing of Personal Data'

Countries in the European Economic Area are deemed to have an adequate level of protection. The European Commission has approved countries outside of the European Economic Area which are deemed to have an adequate level of protection, also known as 'Safe Countries', the list of Safe Countries can be found on the following link:

http://ec.europa.eu/justice/data-protection/document/international-transfers/adequacy/index_en.htm

In respect of all other countries, the European Commission has set down specific rules as to the circumstances in which Personal Data may be transferred. There are three options:

1. Binding Corporate Rules
2. Model Contracts
3. Safe Harbour, for the US

When transferring data outside of the European Economic Area and Safe Countries the Company must ensure that one of the specific rules listed above is in place.

6 Data Retention and Destruction

The Company is committed to complying with the requirements of the Act and recognises the importance of data retention and destruction. The Company therefore ensures adherence to the following:

Data Retention

The Act states that:

'Personal Data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes'

It does not, however, stipulate any retention periods. However, keeping Personal Data for too long may cause issues such as the following:

- Increased risk that the information will go out of date, and that the outdated information will be used in error – to the detriment to all concerned
- As time passes it becomes increasingly difficult to ensure that information is accurate
- Even though the Personal Data may no longer be needed, the Company must still ensure it is held securely
- The Company must be willing to be able to respond to a subject access request for any Personal Data held. This may become more difficult if the Company are holding more data than is necessary

Personal Data held for longer than necessary will, by definition, be excessive and may also be irrelevant. Holding Personal Data for longer than is necessary would mean the Company is likely to breach the third and fourth data protection principles.

The Company has taken the decision to retain all Personal Data securely for a minimum period of 7 years from the date it was securely archived or stored offline.

Destruction

Upon expiration of the 7 year retention period the Company will ensure Personal Data is destroyed securely. The destruction of Personal Data will involve the sanitisation of the media equipment upon which it is held and/or the destruction of offline documentation.

The Company will ensure that all media equipment sanitisation and document destruction is undertaken by a qualified third party. The Company will further ensure that the third party disposing of such Personal Data are appropriately vetted to ensure the highest level of security commensurate with the Personal Data being destroyed.

7 Subject Access Request

The Company is committed to complying with the requirements of the Act and recognises the importance of adhering to subject access requests made by Data Subjects.

A Data Subject has the right to know:

- The purposes for which the Personal Data are processed
- The recipients or classes of recipients of Personal Data to whom the Data may be disclosed
- The information comprising Personal Data, and to receive a copy of such information

- Any information available to the Data Controller on the sources of the Data

A Data Subject may make a subject access request at any time. Under the Act, the Company is required to respond to subject access requests within 40 calendar days from the date upon which the Data Subject has been identified and the relevant subject access request fee has been made. Failure to do so is a breach of the Act and could lead to a complaint being made to the Data Protection Supervisor.

All requests made by the Data Subject must be bought to the attention of senior management of the Company which will subsequently log the request within the subject access request register. Senior management will then ensure the request is dealt with in the appropriate manner.

Prior to the release of any information to a Data Subject senior management will ensure the Company has received the following:

Written Form

The subject access request has been made in writing; this includes e-mails, faxes, written letters and social media.

Fees

The Company's fee of £10.00 to action the subject access request has been settled. Note that an inspection of records only must be provided free of charge.

Additional Information

Sufficient information has been provided by the Data Subject in order for the Company to identify the person making the request and to locate the information which that person seeks.

In certain circumstances a subject access request can be made on behalf of the Data Subject. Sufficient documentation has been provided to ensure the Data Subject has authorised a third party to request such information on their behalf.

Once the Company is in receipt of the above senior management will comply with the subject access request and in any event within 40 calendar days. If the Company does not hold any information the Data Subject will be advised accordingly.

When collating the requested information for the Data Subject the Company ensures that the following areas are searched for Personal Data:

- All computer systems – Networked and non-networked computers together with computer systems used by any of the Company's Data Processors
- Manual files where staff have ready access to specific information about a particular individual, or such information can be found applying a standard search procedure

- Electronically and non-electronically archived files

As a result of the above searches the Company will review the information and will:

- Decide if there is any information which is not Personal Data and therefore does not need to be provided
- Decide what information may not need to be provided because it may reveal the identity of another person
- Decide what information it does not need to provide because an exemption can be applied. Exemptions include but are not limited to legal professional privilege, confidential references, management forecasts and planning, negotiations, regulatory functions and unstructured manual data held by public authorities

Once all Personal Data requested by the Data Subject has been collated and reviewed by the Company, the Company will provide the Data Subject with the information in written intelligible form. This means that it should be provided in a form which can be understood by the average person, and where complex/technical terms or codes are used these should be explained so that the information can be understood.

In some instances where a subject access request raises complex issues the Company may use external legal advisors to assist. When relying upon external advisors the Company will ensure that the response is dealt with within the statutory timeframe.

8 Data Security

The seventh principal requires Data Controllers to consider appropriate measures to ensure the integrity of Data and that appropriate care is taken with Personal Data. The Act does not set out what security measures will be appropriate, nor does it specify acceptable types of security measures. The Company assesses the Personal Data it holds and makes judgement as to the degree of protection that is necessary.

The Company takes into account the following when ensuring adequate protection of Personal Data:

Physical Security Measures

- Location and storage of Personal Data
- Sophistication of the Company's access controls relevant to the sensitivity of the Personal Data
- Process for destruction of physical documents containing Personal Data
- Process for sanitisation of hardware containing Personal Data
- Procedures to protect Personal Data against burglary, fire or natural disaster
- Procedures to cover temporary removal of Personal Data from the Data Controller's premises or systems

Organisational Security Measures

- Appointment of a director to take responsibility for data protection
- Availability of resources to ensure the director responsible for data protection can perform their role successfully
- Continual review of security measures to protect Personal Data
- Continual monitoring to ensure compliance with this Policy
- Staff who have access to Personal Data are vetted prior to access being granted
- Staff training on an annual basis

Technical Measures

- Use of anti-virus software to protect Personal Data
- Ensuring the security and regular change of user passwords
- Security of back-up data
- Continual monitoring of user access rights
- Encryption of sensitive Personal Data files
- Security of mobile devices
- Prevention of downloads
- Safe destruction of Personal Data

The Company may from time to time outsource certain functions which involve third parties Processing Personal Data on its behalf. In order to comply with the Act the Company ensures, where possible, that contractual arrangements clearly define the following:

- The nature of the Personal Data being processed and how the Data Processor should be processing such data
- A right for the Company to audit the Data Processor against its obligations under the Act
- Ensuring that the Data Processor can't sub-process without the Company's prior approval

Furthermore the Company ensures consideration to the following prior to outsourcing any Processing:

- Whether the outsourcing company is reputable and able to offer sufficient guarantees in relation to how they will process Data on the Company's behalf
- If the outsourcing is cross border, whether the contract is enforceable in the other jurisdiction
- Whether the organisation has adequate procedures in place to vet its staff
- Whether to oblige the organisation to report any breaches or other issues immediately on discovery

9 Notification

As a data controller, the Company is required to notify the Data Protection Commissioner that it is processing personal data. The Company is registered in the register of data controllers.

Data controllers must renew their notification with the Data Protection Commissioner on an annual basis. Failure to notify constitutes a criminal offence.

Any changes to the register or breaches of the Act must be notified to the Information Commissioner's Office within 28 days of taking place.

Senior management shall be responsible for notifying and updating the Data Protection Commissioner.

10 Implementation

This Policy shall be deemed effective as of 08/07/2015. No part of this Policy shall have retroactive effect and shall thus apply only to matters occurring on or after this date.