CORPORATE BENCHMARKING SERVICES (SCOTLAND) LIMITED

DATA PROTECTION POLICY

INTRODUCTION

Corporate Benchmarking Services (Scotland) Limited ("the Company") is committed to a policy of protecting the rights and privacy of individuals, including members, in accordance with the General Data Protection Regulation (GDPR) and domestic UK data protection legislation ("the Data Protection Legislation").

The Company processes personal data in order to administer the membership database and generally perform the duties of a membership organisation. This involves the personal data of members but also of a variety of individuals in third party organisations.

In compliance with our stated policy, the Company will ensure that all this information about individuals is collected and used fairly, stored safely and securely, and not disclosed to any third party unlawfully.

All staff, office-bearers and any entity who deals with the Company must comply with the terms of this policy.

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 to Data Protection or other legislation.

KEY CONCEPTS

The Company is a 'Data Controller' in terms of the Data Protection Legislation. The definition of 'Data Controller' together with other key Data Protection Legislation definitions can be found at Annex A.

Data Protection Principles

The Data Protection Legislation requires that anyone processing personal data must comply with Eight Principles of good practice. These Principles are legally enforceable.

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 specified and lawful purposes and shall not be further processed in any manner incompatible with that purpose or those purposes;
3. Shall be adequate, relevant and not excessive in relation to the purpose or purposes for which it is processed;
4. Shall be accurate and where necessary, kept up to date;
5. Shall not be kept for longer than is necessary for that purpose or those purposes;
6. Shall be processed in accordance with the rights of data subjects under the Act;
7. Shall be kept secure i.e. protected by an appropriate degree of security;
8. Shall not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of data protection or an accredited security arrangement is in place.

Rights of Data Subjects

The data subject has rights under the act. These consist of:

- 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;

- The right to correct, rectify, block or erase information regarded as incorrect.

Data Subjects also have the right to take any complaints about how the Company process their personal data to the Information Commissioner:

https://ico.org.uk/concerns/
0303 123 1113.
Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire SK9 5AF

MEMBERSHIP PERSONAL DATA

Personal data of members held by the Company is as provided by members at the point of membership application. These will include Name, Work Address, Mailing Address, work and mobile phone numbers, email address, employing organisation, current job title and/or level and IP address. Where fees are applicable additional details will be held for the purpose of collecting membership fees.

LEGAL BASIS FOR PROCESSING

The Company uses members' personal data in line with the lawful basis of legitimate interest, in order to maintain and manage each individual's employer's membership. This means the Company will use personal data as part of the normal business administration process required to run the membership including engagement with third parties which include but are not limited to:-

- Direct Debit collections with personal data as supplied by the member;
- HMRC; and
- the Company's outsourced Accountants and professional advisers.

In the event that any processing of personal data is contemplated by the Company which requires the consent of the data subject(s), such consent will be obtained prior to any processing.

THIRD PARTIES

There are situations where personal data held by the Company is shared with or is accessible by third party organisations such as our professional advisers, website and IT support providers, payment card processors and the like. In such cases the Company will have arrangements in place with such third parties setting out parties' roles and responsibilities for data protection and with legally binding obligations for the protection of personal data.

SECURITY

The Company is committed to protecting the privacy of personal data and will use appropriate standards of technology and operational security to protect personal data including a secure server and network firewall connection. Operationally, access to personal data is restricted to authorised personnel who are under a duty to maintain the confidentiality and security of such information.

RETENTION OF PERSONAL DATA

Member's data will be held for the term of the member's employer's active membership as requested by the member or their employer and then for any period required in order to comply with HMRC rules or any other regulations or legislation.

In the event of a request for cancellation of a membership, some information will need to continue on file for a period of time in accordance with tax and accounting practices.

DUTIES AND RESPONSIBILITIES

The Company directors are responsible for ensuring compliance with this policy. The directors will meet regularly and address any data protection related issues that arise and generate initiatives or communications as necessary to ensure compliance with this policy.

At an operational level, the Company will ensure that:-

- there is always someone with specific responsibility for and knowledge of data protection who will act as the internal and external point of contact, handle complaints from data subjects and report to the board on data protection operation;
- anybody wanting to make enquiries about handling personal information knows what to do and who to refer enquiries to;
- queries about handling personal information are promptly and courteously dealt with;
- methods of handling personal information are clearly described;
- a regular review and audit is made of the way personal information is held, managed and used, including where new categories of personal data are processed or where processing takes place or if processing is deemed to present a risk to the rights and freedoms of individuals;
- appropriate records of processing records are maintained;
- methods of handling personal information are regularly assessed and evaluated, particularly if new processing takes place or if processing is deemed to present a risk to the rights and freedoms of individuals;
- performance with handling personal information is regularly assessed and evaluated;
- breaches of personal data are promptly assessed, contained and mitigated; and
- breaches of personal data are reported to the ICO and data subjects where necessary.

PROCEDURE FOR REVIEW

This policy will be updated as necessary to reflect best practice or future amendments made to the Data Protection Legislation.

The ICO's website (www.ico.gov.uk) provides further detailed guidance.

For help or advice on any data protection issues, please do not hesitate to contact: the Company's Programme Manager at info@sheiiba.com

Annex A

Key Definitions

1. ‘Personal Data’ means data which relate to a living individual who can be identified from those data or 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. Under the GDPR, the definition of personal data will explicitly extend to IP addresses.

2. Sensitive Personal Data’ means information about an individual’s ethnicity, political opinions, their religious beliefs or other beliefs of a similar nature, membership of a trade union, disability, sexual orientation, the commission or alleged commission by them of any criminal offence, or any proceedings for any offence committed or alleged to have been committed by them, the disposal of such proceedings or of the sentence of any court in such proceedings.

3. Under the GDPR, the term ‘sensitive personal data’ will be replaced by the definition special category data which means any personal data information about an individual’s racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life or sexual orientation and their genetic or biometric data.

4. ‘Processing’ means any operations or set of operations which is performed on personal data whether or not by automated means such as collection, use, disclosure or storage of personal data etc.

5. ‘Data Controller’ means the organisation which, either alone or jointly with another organisation, determines the manner and purpose of the processing of personal data. The Data Controller is primarily responsible for compliance with the Data Protection Legislation.

6. ‘Data Processor’ means an organisation (such as a contractor) which processes personal data on behalf of a Data Controller. Under the GDPR a Data Processor also has responsibilities for compliance with the Data Protection Legislation

7. ‘Personal Data Breach’ means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed