Bring It On Limited

GDRP Compliance Policy and Procedures

1. INTRODUCTION

This document covers the policies and procedures required to comply with UK General Data Protection Regulation (UK GDPR), tailored by the Data Protection Act 2018.

2. DATA COMPLIANCE ADMINISTRATOR

Bring It On Limited (the Company) is not a public authority or body, its core activities do not require regular and systematic monitoring of individuals on a large scale and do not involve processing, on a large scale, 'special categories' of personal data, criminal convictions or offences data.

The Company has therefore decided that there is no legal requirement to appoint a Data Compliance Officer.

The Company has appointed a Data Compliance Administrator to administer these procedures and act as the contact for GDPR queries.

The appointed Administrator is currently Carol Harrison, who can be contacted at the following email: info@bringitonne.co.uk.

3. DATA PROTECTION IMPACT ASSESSMENT

Having reviewed the nine relevant criteria the Company has concluded that the data we process is not “likely to result in a high risk”. We therefore conclude that a DPIA is not required.

4. TYPES OF DATA

The types of data stored and processed by the Company are listed in Appendix 1. Some of this data may constitute Personal Data.

The Company has no employees and therefore it holds no Personal Data relating to employees.

The Company does not hold any Personal Data relating to young people or vulnerable adults.

Some data is collected via our website. This is limited to contact details from Schools and Companies wishing to take part in Bring It On events and is specifically provided by them.

5. POLICIES ON THE USE OF DATA

Data held and processed by the Company will only be used for purposes associated with the delivery of its charitable objectives and in particular the delivery of the Bring It On Exhibition and any associated events, including ‘online’ activities.

Data will never be passed to third parties for commercial gain.

Data will only be passed to third parties where this is necessary to fulfil the Company’s legal obligations, for the delivery of the Company’s Charitable Objectives or to permit suppliers or contractors to deliver their contractual obligations to the Company. Third parties are required to use this data only for the purposes for which it is provided.

Data will be passed to Trustees to enable them to carry out their legal obligations. They are required to use such data only for the purpose for which it was provided and to delete it when no longer required for that purpose or when they cease to be a Trustee.

Personal Data relating to Trustees, including training records, will be kept by the Company for the reasons given in Section 9. below.

6. USERS OF DATA

The following individuals and organisations process and make use of the Company's Data:

- The Company Secretary
- The Founders (Bowman Bradley, Thomas Chacko, Carol Harrison and Moira Shaftoe)
- The Trustees
- Members of the Steering Committee
- Suppliers and Contractors

7. SECURITY OF DATA

Data is kept in electronic and paper form. Most data exchanged with third parties is exchanged electronically. Paper records are kept only by the company secretary.

The Company hard disk is kept by the Company Secretary in a secure environment. It is password protected and not normally connected to the internet. It is used primarily as a back-up drive.

The Company Secretary keeps data on a personal computer which is password protected and kept in a secure environment. Paper records are kept in a secure environment.

The Founders keep limited data on their personal computers which are password protected and kept in a secure environment.

Trustees keep contact data for each other and have given their permission for this to be exchanged between them.

Members of the Steering Committee keep contact data for each other and have given their permission for this to be exchanged between them.

Suppliers and contractors keep Company data under their own GDPR procedures and are required to use it only for the purposes for which it has been provided and not to pass it to third parties for commercial gain.

8. DATA BREACHES

Any data breach will be taken seriously by BIO the Company in line with the procedures laid out in this document.

The Company will maintain a Data Breach Log which will be held by the Data Compliance Administrator, see section 2 above.

Data breaches will include but not be limited to:

- Electronic hacking of the Company's systems by third parties
- Mis-sent emails or other communications containing confidential information.
- Confidential data left in the home or in external locations for others to see.

In the event of any data breach being discovered the following procedures will be followed:

1. The subject of the data breach will be identified, and the data affected established.
2. Any parties affected by the breach will be identified.
3. If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, affected parties will be informed immediately and the Information Commissioner's Office will be advised of the breach.

4. An internal investigation, led by the Data Compliance Administrator, will be set up to understand how and why the breach has occurred and what needs to be undertaken to prevent a similar occurrence happening again and corrective action taken.
5. Details will be recorded in the Data Breach Log.

9. RETENTION SCHEDULE

Except as specifically required by this procedure, it is the decision of the business that all data described in Appendix 1 needs to be retained for the purposes of:

- Defending the Company and its insurers against any legal claims brought against it.
- Any future tax investigation by HMRC into the Company's accounts
- Any future professional indemnity claims with respect to the activities of the Company.

10. VERIFICATION AND UPDATING OF DATA

The Company will attempt to verify and update data regularly to ensure that it is accurate.

11. SUBJECT ACCESS REQUESTS

The Company will comply with Subject Access Requests (SAR's) in line with the regulatory requirements. A Subject Access Request Log will be maintained by the Data Compliance Administrator and the following procedure followed:

1. Confirm the subject of the SAR and record the date of the request and required reply date in the Subject Access Request Log.
2. Review the nature of the data subject and the requested information.
3. Identify all data which is held on the subject.
4. Confirm with subject what form they would like the information submitted in
5. Submit information to the subject.
6. Complete Subject Access Request Log with the actual reply date

Date	Issue	By	Comments
1/5/21	0	Bowman Bradley	First Issue
25/11/21	1	Thomas Chacko	Reviewed with no changes

Bring It On Limited

GDRP Compliance Policy and Procedures

Appendix 1 – Data Schedule

What Data We Hold	Data Held BY		
Contact Details for:			
Schools	Suppliers and Contractors	Some data collected via our website	Company Hard Drive
Companies/Exhibitors	Suppliers and Contractors	Some data collected via our website	Company Hard Drive
Suppliers	The Founders		Company Hard Drive
Trustees	Company Secretary	Trustees	Company Hard Drive
Supporters	The Founders		Company Hard Drive
Steering Team Members	The Founders	Members of the Steering Team	Company Hard Drive
Other Interested Parties	The Founders		Company Hard Drive
Bank Account Details for:			
Suppliers	The Company Secretary		Company Hard Drive
Personal Details for			
Trustees	The Company Secretary		Company Hard Drive