Book A Movement Ltd
Data Protection Policy

Version 1.0: September 2022

1 This document 'Data Protection Policy'

This data protection policy applies to all operations by Book A Movement Ltd, including their in-house processes, software operations and data storage.

This policy is designed to ensure that Book A Movement Ltd complies with its obligations under the General Data Protection Regulation and how they confirm to the 8 data protection principles:

1. Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless –
    a. at least one of the conditions in Schedule 2 is met, and
    b. in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.
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 this 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 and freedoms of data subjects in relation to the processing of personal data.

This document governs all our operating procedures for our internal processes and platform including servers / hosting.

This is a living document and will be reviewed annually or when required. Updated copies of this document will always be recorded on our website.

2 Document Control

Version	Date	Versions
1.0	13/09/2022	Policy rewritten and replaced any previous versions issued by Book A Movement Ltd. Policy includes all aspects of the business and has been rewritten to comply with GDPR requirements.

3 Our Security Policies

The following small policies apply to all employees for the storing and protection of personal data as outlined in this policy. These security policies are mandatory.

- **Email and Communication –** We use GSuite by Google to manage all of our email, cloud and collaboration tools. All employees will use this system as part of their standard procedure. This includes email, cloud storage, hangouts and other Google related tools.
- **Passwords –** We have a policy of using and forcing complex passwords throughout all of our systems. If there is the slightest doubt that something has been compromised, then a full review of our password policy will be undertaken.
- **Employees –** We ensure that all of our employees are made aware and receive training in our data protection and IT policies.
- **Training –** We will ensure that all our employees are taught the correct procedures and will review training on an annual basis.
- **Permissions –** Staff members are only given access to resources and files as and when required. This includes customer databases.
- **Storage –** Files are to be stored using internal password protected PCs or Cloud Storage. Memory devices will not be used. Where data is printed, this will be destroyed securely using a cross cut shredder. Devices will also be encrypted incase a theft does occur
- **Data Security –** We have many policies relating to the security of our systems which are documented throughout this document
- **Physical Security –** Our office is secured and alarmed. Physical documents are further locked away in secure cabinets. There is also CCTV in use.
- **IT Security –** All of our internal systems utilise the latest software including security patches as required. A firewall blocks our incoming network. Antivirus software is installed on all machines. Please see our further security policies below in relation to our server and system security.
- **Third Party Compliance –** We ensure that all our third party suppliers are GDPR compliant.

4 Data we hold & Backups

The data we hold in our systems belong to our customers and their customers. We control the data format, but ultimately, our customers are the data controllers and should manage their data (in our system) effectively. We provide tools within our systems to make managing this data easier for our customers.

All data (including our code and databases) are stored on our secure cloud servers powered by green energy. All our services are managed by our preferred partner, Krystal Hosting Ltd. They have both been checked for security and GDPR compliance. We have multiple redundancies in place both in terms of backups, but also additional servers to deal with load and redundancy should a server fail.

Payments within The Platforum are managed by GoCardless. We store no information relating to banks or bank account numbers.

5 Data Subject Access Requests

Should a member of the public request a copy of any personal information which Book A Movement Ltd hold about them, they should follow the following policy.

- They should ring or email Book A Movement Ltd customer support
- The request will then be acknowledged by email
- The individual's identity will then be checked to confirm they are the correct individual. This could be by them supplying an address, email address, data of birth or document based evidence
- Data will then be found and analysed to ensure we don't disclose anything unrelated to the individual
- This data will then be provided by email to the individual within 30 days of receiving the original request
- There will be no fee for this, however, if duplicate information is requested at a later date then a small administrative fee may occur.
- If your request is related to a particular company who we host the data for, you should first speak to them as they will most likely hold paper information too which we have no responsibility for.

6 Right to be forgotten

Under Data Protection, should one of customers wish for their personal data to be forgotten (erasure), they should follow the process below:

- We should be contacted by email or phone with the details of the data you are seeking to have removed.
- The director(s) will consider the request and include discussions with all relevant authorities including the ICO. We will ensure that all our statutory obligations are complied with.
- Once we've deemed what data can be deleted, we will confirm the data and timescales involved, before ensuring that the data is deleted from all the correct locations, including the destruction of paper documents if required.

7 Correctly incorrect data

If you believe some data that we hold to be incorrect, you should write to our team by emailing support@bookamovement.co.uk. Once the data has been fixed, we will confirm this back.

8 Reporting a breach

At Book A Movement Ltd we take data breaches very seriously and have a full policy in place should this unfortunate event occur. We have a number of policies in place to protect our systems and sensitive data, as well as our code and backend systems.

Any breach should be reported to the lead developer or company director.

Once a breach has been identified an investigation will be launched to identify what data (if any) has been damaged during the breach. We'll also consider if the data is sensitive or will result in financial loss or discrimination. If it does, the ICO will be informed within 72 hours of the breach occurring.

If the breach results in personal customer information being lost, we will work with our customers to ensure that their customers are contacted and informed about the breach and data loss.