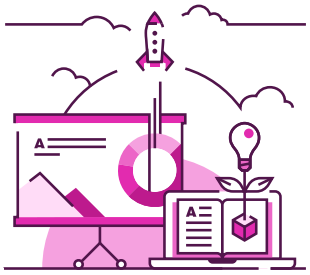
T. +44 161 883 0225
F. +44 161 883 0325
www.brightcarbon.com
info@brightcarbon.com

Digital World Centre
1 Lowry Plaza
The Quays
MediaCity
Manchester
M50 3UB
United Kingdom

Registered in England and Wales.
Company № **7869834**



DATA PROCESSING AGREEMENT (UK GDPR / EU GDPR)

This Data Processing Agreement ("DPA") is entered into between:

Controller: The Customer (as defined in the Agreement)
Processor: BrightCarbon Ltd, Digital World Centre, The Quays, MediaCity, Salford, M50 3UB, United Kingdom

This DPA forms part of and supplements the agreement governing the use of the BrandIn SaaS (the "Agreement"). This DPA includes and incorporates Appendix 1 (BrandIn Data Retention Policy) and Appendix 2 (Sub-processor List), each of which forms part of this DPA. In the event of any conflict between this DPA and the Agreement in relation to the processing of Customer Personal Data, this DPA shall prevail to the extent of that conflict.

1. Definitions

1.1 "Applicable Data Protection Law" means all applicable data protection and privacy legislation in force from time to time, including the UK GDPR, the EU GDPR, the Data Protection Act 2018, and any legislation implementing or supplementing the foregoing, in each case as amended or replaced from time to time.

1.2 "Controller", "Processor", "Data Subject", "Personal Data", and "Processing" shall have the meanings given in Applicable Data Protection Law.

1.3 "Customer Data" shall mean all customer-generated application data, logs, and activity records, unless classified as Compliance & Audit Evidence Data.

1.4 "Customer Personal Data" means any Personal Data processed by the Processor on behalf of the Customer under or in connection with the Agreement.

1.5 "Compliance & Audit Evidence Data" shall mean records required for contractual, legal, or regulatory purposes.

2. Roles of the Parties

2.1 The Customer acts as Controller of Customer Personal Data.

2.2 BrightCarbon acts as Processor and shall process Customer Personal Data only on documented instructions from the Customer, including with regard to transfers of Customer Personal Data to a third country or an international organisation, unless required to do so by applicable law to which the Processor is subject; in such a case, the Processor shall inform the Customer of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest. If the Processor believes that an instruction infringes Applicable Data Protection Law, it shall inform the Customer without undue delay, unless prohibited by law.

T. +44 161 883 0225
F. +44 161 883 0325
www.brightcarbon.com
info@brightcarbon.com

3. Nature, Scope and Purpose of Processing

3.1 Nature of Processing

Processing carried out in connection with the provision of a SaaS add-in. For the avoidance of doubt, the content of Customer Microsoft 365 Office files is processed locally on the User's device and is not transmitted to or stored by the Processor as part of ordinary service operation.

3.2 Purpose of Processing

- Provision and operation of the BrandIn service;
- Account, licensing, and configuration management;
- Logging, security, and incident investigation;
- Support and essential service communications;
- Retention of compliance and audit evidence.

3.3 Duration of Processing

Processing shall continue for the duration of the Agreement and any applicable retention period set out in this DPA, including Appendix 1.

4. Categories of Data and Data Subjects

4.1 Categories of Personal Data

- User identifiers (including names, email addresses, and user IDs)
- Authentication and account metadata
- Usage and telemetry data
- Configuration data (including workspace and library IDs and names, and feature configurations)
- Logs (including IP addresses and system logs)
- Compliance and audit records (e.g. records of Terms & Conditions acceptance)

4.2 Categories of Data Subjects

- Customer employees and authorised users
- Customer administrators, business contacts and support contacts
- Individuals associated with account creation, administration, support, and contractual acceptance records

4.3 Special Category Data

The Customer shall not intentionally submit special category data to the service unless expressly agreed in writing with the Processor and subject to any additional safeguards required by Applicable Data Protection Law.

T. +44 161 883 0225
F. +44 161 883 0325
www.brightcarbon.com
info@brightcarbon.com

5. Processor Obligations

5.1 The Processor shall:

a) Process Customer Personal Data only on documented instructions from the Customer including with regard to international transfers.

b) Ensure that persons authorised to process Personal Data are subject to appropriate confidentiality obligations.

c) Implement appropriate technical and organisational measures proportionate to the risk and consistent with Section 6 and any relevant measures described in the appendices.

d) Assist the Customer, taking into account the nature of the processing and the information available to the Processor, in ensuring compliance with the Customer's obligations under Articles 32 to 36 of the GDPR (or equivalent provisions of Applicable Data Protection Law), including in relation to security, breach notification, data protection impact assessments and prior consultation with supervisory authorities where required.

e) Notify the Customer without undue delay and in any event within 24 hours after becoming aware of a personal data breach.

f) Make available to the Customer all information reasonably necessary to demonstrate compliance with this DPA.

g) At the choice of the Customer, delete or return Customer Personal Data on termination of the Agreement, save to the extent retention is required by applicable law or expressly permitted under Appendix 1.

6. Security Measures

6.1 The Processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including as appropriate: encryption of Customer Personal Data in transit and at rest; access controls and role-based permissions; audit logging and monitoring of system activity; regular security review and testing; and such additional measures as are described in Appendix 1 or otherwise maintained by the Processor, provided such measures do not materially reduce the level of protection for Customer Personal Data during the term of the Agreement.

6.2 Security measures shall be reviewed periodically and updated where appropriate.

7. Sub-processing

7.1 The Customer provides general authorisation for the Processor to appoint sub-processors in connection with the provision of the services.

7.2 The Processor shall:

T. +44 161 883 0225
F. +44 161 883 0325
www.brightcarbon.com
info@brightcarbon.com

a) Maintain an up-to-date list of authorised sub-processors, including the information set out in Appendix 2 as updated from time to time
b) Ensure that each sub-processor is subject to data protection obligations equivalent to those set out in this DPA
c) Remain fully liable for the performance of its sub-processors

7.3 The Processor shall provide at least 30 days' notice of any intended changes to sub-processors.

7.4 The Customer may object to a new sub-processor on reasonable and evidenced data protection grounds within 14 days of receiving notice. If the Customer so objects, the parties shall discuss the objection in good faith. If the Processor cannot reasonably accommodate the objection, either party may terminate the affected services on written notice.

8. International Data Transfers

8.1 Where Personal Data is transferred to a country outside the United Kingdom (UK) or European Economic Area (EEA), the Processor shall ensure that such transfers are made in compliance with Applicable Data Protection Law.

8.2 Where required under Applicable Data Protection Law, transfers shall be subject to an appropriate transfer mechanism, which may include:

- Reliance on Adequacy Decisions issued by the European Commission or the UK Government (as applicable).
- Reliance on the EU-U.S. Data Privacy Framework and the UK Extension thereto, provided the recipient sub-processor is self-certified.
- The use of Standard Contractual Clauses and/or the UK Addendum.

Details of relevant sub-processors, locations and safeguards are set out in Appendix 2.

8.3 To the extent that the Processor transfers Customer Personal Data to a sub-processor in a country not recognised as providing an adequate level of protection under Applicable Data Protection Law, the Processor shall ensure that a valid transfer mechanism is in place as required by Applicable Data Protection Law, which may include the EU SCCs and, where applicable, the UK Addendum.

8.4 Where the EU SCCs and/or the UK Addendum are required:

- the description of the transfer, including the subject matter, duration, nature and purpose of processing, categories of data subjects, and categories of personal data, shall be as set out in this DPA, including Sections 3 and 4 and Appendix 1;
- the technical and organisational measures shall be those set out in Section 6 and Appendix 1, together with any additional measures implemented by the Processor in relation to the relevant transfer;

T. +44 161 883 0225
F. +44 161 883 0325
www.brightcarbon.com
info@brightcarbon.com

- the list of relevant sub-processors, processing locations and applicable transfer mechanisms shall be as set out in Appendix 2; and
- upon reasonable written request, the parties shall provide such further information as is reasonably required to complete the annexes, appendices or tables to the EU SCCs or the UK Addendum in a manner consistent with this DPA.

8.5 The Processor shall implement supplementary technical and organisational measures where required by Applicable Data Protection Law to ensure the transferred data is afforded a level of protection essentially equivalent to that guaranteed within the UK/EEA.

9. Data Retention and Deletion

9.1 Customer Personal Data shall be retained only for as long as necessary for the purposes set out in this DPA and in accordance with Appendix 1.

9.2 Unless otherwise agreed in writing, retention and deletion of Customer Personal Data shall be carried out in accordance with Appendix 1. Without limitation:

(a) Standard Customer Data relating to paid subscription accounts shall be retained for 90 days following subscription termination, unless immediate deletion is requested;

(b) Standard Customer Data relating to free plan accounts shall be retained for 90 days of inactivity, as defined in Appendix 1;

(c) server and usage logs may be retained for up to 90 days for operational and security purposes;

(d) backups containing deleted Customer Personal Data may be retained solely for disaster recovery purposes and shall be overwritten or destroyed within a maximum of 30 additional days; and

(e) Compliance & Audit Evidence Data may be retained for the lifetime of the relevant customer account plus 7 years after account termination, unless a longer period is required by law or due to an active dispute.

9.3 Upon the Customer's written request and subject to Appendix 1 and any legal retention requirement, the Processor shall delete or return Customer Personal Data and, where requested, provide written confirmation of deletion. Deletion from backup systems shall occur in accordance with the backup retention cycle described in Appendix 1.

9.4 Nothing in this DPA shall require the Processor to delete Customer Personal Data to the extent retention is required by applicable law, court order, regulatory requirement, legal hold, or active dispute, provided that such data is retained only to the extent and for the duration necessary for that purpose.

T. +44 161 883 0225
F. +44 161 883 0325
www.brightcarbon.com
info@brightcarbon.com

10. Data Subject Rights

10.1 The Processor shall, taking into account the nature of the processing, assist the Customer by appropriate technical and organisational measures, insofar as possible, in responding to requests from Data Subjects.

10.2 The Processor shall not respond directly to Data Subjects except on the documented instructions of the Customer or where required by law.

11. Personal Data Breaches

11.1 The Processor shall notify the Customer without undue delay, and in any event within 24 hours of becoming aware of a Personal Data Breach affecting Customer Personal Data.

11.2 The notification shall include, to the extent available, information reasonably required to meet the Customer's reporting obligations. The Processor shall provide further information in phases as it becomes available.

12. Audit and Compliance

12.1 The Processor shall make available information reasonably necessary to demonstrate compliance with this DPA.

12.2 Any audit:

- Shall be conducted on reasonable notice (normally not less than 30 days, unless required by law or reasonably necessary following a Personal Data Breach or security incident)
- Shall occur no more than once per year unless required by law or following a data breach
- Shall be carried out in a manner that minimises disruption to the Processor's business
- Shall be conducted at the Customer's sole expense, including the reasonable costs of the Processor's time spent assisting with the audit
- May be satisfied through provision of existing audit reports or certifications
- Any audit information disclosed by the Processor shall be treated as confidential information of the Processor

T. +44 161 883 0225
F. +44 161 883 0325
www.brightcarbon.com
info@brightcarbon.com

13. Term and Termination

13.1 This DPA shall remain in force for the duration of the Agreement.

13.2 Upon termination of the Agreement, the Processor shall process, retain, return and delete Customer Personal Data in accordance with Section 9 and Appendix 1.

14. Governing Law

This DPA shall be governed by the laws of England. Any dispute between the Parties relating to this Agreement shall be subject to the exclusive jurisdiction of the courts of England.

15. Signatures

For and on behalf of BrightCarbon Ltd

Name: _____

Title: _____

Signature: _____

Date: _____

For and on behalf of Customer

Name: _____

Title: _____

Signature: _____

Date: _____

T. +44 161 883 0225
F. +44 161 883 0325
www.brightcarbon.com
info@brightcarbon.com

Appendix 1: BrandIn Data Retention and Deletion Schedule

Purpose

This appendix sets out to define the retention and disposal requirements for Customer Personal Data and Customer Data collected and processed by BrandIn. This ensures compliance with contractual obligations, data protection laws (including GDPR), and internal security standards, while minimising risks associated with storing unnecessary or outdated data.

Scope

This appendix applies to:

- All Customer Personal Data and Customer Data processed by BrightCarbon as Processor in connection with the BrandIn service.
- All production, backup, logging, and support systems.
- All users, including paid subscribers and free account users.

Definitions

TERM	DEFINITION
Customer Data	All customer-generated application data, logs, and activity records, unless classified as Compliance & Audit Evidence Data.
Customer Personal Data	Any Personal Data processed by the Processor on behalf of the Customer under or in connection with the Agreement.
Compliance & Audit Evidence Data	Records required for contractual, legal, or regulatory purposes.
Subscription Termination	The date on which a paid subscription ends or is cancelled.
Inactive Free Account	A free account that has had no user login or interactions for 90 consecutive days.

BrightCarbon

T. +44 161 883 0225
F. +44 161 883 0325
www.brightcarbon.com
info@brightcarbon.com

Data Retention Rules

Standard Customer Data

Paid Subscription Accounts

- Customer data will be retained for **90 days after the termination of a paid subscription,** unless immediate deletion has been requested.
- After this period, all associated data will be securely deleted from active BrandIn systems and scheduled for deletion from backups in accordance with this Appendix.

Free Plan Accounts

- For free plans, Customer Data will be retained for **90 days of inactivity**.
- Inactivity is defined as no user logins or interactions with BrandIn during this period.
- After 90 days of inactivity, the account will be closed and associated data will be permanently deleted.

After the applicable retention period expires, all Customer Data is permanently deleted from active systems and scheduled for deletion from backups.

Compliance & Audit Evidence Data

Retained for the lifetime of the customer account plus 7 years after account termination, unless a longer period is required by law or active dispute.

Data Types Covered

This policy distinguishes between Standard Customer Data and Compliance & Audit Records, which are governed by separate retention requirements.

Standard Customer Data

- User Identifiers: User IDs, user names, email addresses.
- Telemetry: Usage metrics.
- Configuration Data: Workspace and library IDs and names. Feature configurations.
- Logs: Server and usage logs retained for 90 days for operational and security purposes.

Compliance & Audit Evidence Data

Certain categories of data are classified as Compliance & Audit Evidence Data and are subject to extended retention requirements beyond standard Customer Data deletion periods.

These include:

- **Record of acceptance of Terms & Conditions:** user name, role, email, timestamp.

T. +44 161 883 0225
F. +44 161 883 0325
www.brightcarbon.com
info@brightcarbon.com

- **Tenant Identifier linked to acceptance and termination events:** Tenant ID, Tenant Name, account lifecycle events with timestamps (such as creation, modification, closure, and Customer Data deletion events).

These records are retained to:

- Establish legal proof of contract formation.
- Support dispute resolution.
- Meet regulatory, audit, and security obligations.

Secure Disposal

Standard Customer Data

1 | At the end of the 90-day retention period:
    - Customer Data is flagged for deletion.
2 | Data is permanently removed from:
    - Primary production databases
3 | Backup systems:
    - Backups containing deleted data are retained only for disaster recovery and are automatically overwritten or destroyed within a maximum of **30 additional days**.

After deletion, recovery of Customer Data is not possible.

A deletion certificate will be provided upon request for paid subscriptions.

Compliance & Audit Evidence Data

Compliance & Audit Evidence Data are excluded from the standard deletion process and are securely retained for the defined legal retention period. Upon expiration of this extended period, these records are permanently deleted or anonymised.

Legal Holds & Exceptions

If data must be retained due to:

- Legal obligations
- Court orders
- Regulatory requirements

the data will be placed under a **legal hold** and retained only for the minimum period required by law.

Compliance & Audit Evidence Data

Record of acceptance of Terms & Conditions (including, where applicable, user name, role, email and timestamp) and tenant audit records may be preserved beyond standard retention periods where required to fulfill contractual obligations, respond to legal claims, or comply with regulatory requirements.

T. +44 161 883 0225
F. +44 161 883 0325
www.brightcarbon.com
info@brightcarbon.com

Security During Retention

All retained data is protected by:

- Encryption at rest and in transit (AES-256, TLS 1.2 or higher)
- Access controls and role-based permissions
- Audit logging
- Regular security reviews

Customer Responsibilities

Customers are responsible for exporting or retrieving any data they wish to retain before the end of the retention period.

Key Notes

BrightCarbon acts as Processor in relation to Customer Personal Data processed on behalf of customers in connection with the BrandIn service.

Customers may request early deletion of data by contacting the Data Privacy Officer at **dpo@brightcarbon.com**.

T. +44 161 883 0225
F. +44 161 883 0325
www.brightcarbon.com
info@brightcarbon.com

Appendix 2: Sub-processor List

Authorized Sub-processors

To provide and maintain the **BrandIn** SaaS platform, **BrightCarbon** engages certain third-party service providers ("Sub-processors") that may process Customer Personal Data on our behalf.

A *Sub-processor* is any third party engaged by **BrightCarbon** that may process Customer Personal Data on BrightCarbon's behalf in connection with the operation, security, support or improvement of the BrandIn service.

We conduct due diligence on all Sub-processors prior to engagement and require each Sub-processor to enter into a written agreement imposing appropriate data protection obligations, including confidentiality, security controls, and restrictions on further subcontracting. Sub-processors may process Customer Personal Data only for the purposes of providing services to **BrightCarbon** in connection with the **BrandIn** platform.

International Data Transfers

International transfers involving sub-processors listed in this Appendix are subject to the safeguards described in Section 8 of this DPA.

Updates to this Sub-processor List

We may update this list from time to time as our business needs evolve. Any such update shall be reflected in this Appendix 2. Customers will be notified of any new Sub-processors at least **30 days in advance** via email. Customers may raise objections to the engagement of a new Sub-processor by contacting us as described below.

Contact

If you have any questions about our use of Sub-processors, please contact us at **dpo@brightcarbon.com**.

BrightCarbon

T. +44 161 883 0225
F. +44 161 883 0325
www.brightcarbon.com
info@brightcarbon.com

List of Sub-processors (Last updated 19/05/2026)

Name	Service provided	Data categories processed	Processing purpose	Sub-processor location	Transfer mechanism	DPA
Microsoft Corporation (Azure)	Cloud hosting and infrastructure	User identifiers (including user IDs, user names and email addresses); telemetry and usage metrics; server and usage logs; and compliance/audit evidence data including Terms & Conditions acceptance records and tenant lifecycle records	Hosting and operation of the BrandIn SaaS platform, storage of service-side account, configuration, telemetry, logging, and audit data, and support for system availability, resilience, and disaster recovery	UK	Not a restricted transfer to the sub-processor; processing occurs in the EEA and is covered by UK adequacy regulations	Yes
SendGrid (Twilio)	Email delivery.	Contact info (name, email).	Delivery of essential operational, account and service-related email notifications	United States	EU-U.S. Data Privacy Framework and UK Extension where applicable.	Yes
Freshworks (Freshdesk)	Customer support ticketing.	Contact details (name, email) and any personal data included in support requests, including attachments such as screenshots	Handling customer-initiated support tickets and related service support communications	EU	EEA processing; UK adequacy regulations apply where relevant.	Yes
Sentry.io	Server error logging.	IP addresses, logs.	Error logging	EU	EEA processing; UK adequacy regulations apply where relevant.	Yes

T. +44 161 883 0225
F. +44 161 883 0325
www.brightcarbon.com
info@brightcarbon.com

Active Campaign	Backup email delivery for critical service communications	Contact info (name, email).	Fallback delivery of critical operational notifications relating to service disruption, account administration, or other essential (non-marketing) BrandIn communications where the primary delivery channel is unavailable or unsuitable	EU	EEA processing; UK adequacy regulations apply where relevant.	Yes