Data Processing Addendum

This Data Processing Addendum (DPA) includes the Data Processing Terms and attached Appendices, and is incorporated into, and forms part of, the agreement between **Bright SG Ltd**, part of the Bright Software Group of Companies (**Bright**), (as **Data Processor**) and the Customer (as **Data Controller** or **Data Processor** on behalf of the Customer's clients), comprising the standard Terms of Service (**Agreement**) governing the Customer's use of the **Bright** Service (**Service**).

This addendum is effective **1st November 2024**.

1. **Instructions**

   This Addendum has been pre-signed on behalf of **Bright**. To enter into this Addendum, Customer must:

   a. Complete the table below by signing and providing Customer's full legal entity name, address and signatory information; and

   b. Submit the completed and signed Addendum to **Bright** via email to privacy@brightsg.com

2. **Effectiveness**

   a. This Addendum will be effective only if it is executed and submitted to **Bright** in accordance with Paragraph 1 above and this Paragraph 2, and all Customer items in the table below are completed accurately and in full.

   b. If the Customer makes any deletions or other revisions to this Addendum, then this Addendum will be null and void.

   c. Customer signatory represents to **Bright** that he or she has the legal authority to bind the Customer and is lawfully able to enter into a contract.

   d. This Addendum will terminate automatically upon termination of the Agreement, or as earlier terminated pursuant to the terms of this Addendum.

3. Signatories

For, and on behalf of:

Bright SG Ltd	Customer
 **By:** **Name:** Richard Grey **Title:** CISO **Contact:** privacy@brightsg.com **Address:** Unit 35, Duleek Business Park, Duleek, Co. Meath, A92 N15E	**By:** **Name:** **Title:** **Breach Notification Email:** **Address:**
Date: 1st November 2024	**Date:**

Data Processing Terms

1. Definitions

Unless otherwise defined in the Agreement, all capitalised terms used in this Addendum will have the meanings given to them below:

Authorised Users	any individual authorised by you to use the Service as set out in your Registration process;
Data Controller	has the meaning given to it in Data Protection Law;
Data Processor	has the meaning given to it in Data Protection Law;
Data Protection Impact Assessment	has the meaning given to it in Data Protection Law;
Data Security Breach	means any known potential or actual breach of the technical and organisational measures or any obligations or duties owed by **Bright** to the Customer relating to the confidentiality, integrity or availability of Personal Data;
Data Subject	has the meaning given to it in Data Protection Law;
Data Transfer Agreement	means the standard contractual clauses for the transfer of Personal Data to third countries approved by the European Commission or such other agreement for the transfer of Personal Data as the Customer may approve;
Data Protection Law	means: (i) the EU Data Protection Directive 95/46/EC and the EU Privacy & Electronic Communications Directive 2002/58/EC, any amendments and replacement legislation including the EU GDPR, European Commission decisions, binding EU and national guidance and all national implementing legislation; and/or (ii) all applicable data protection and privacy legislation in force from time to time in the UK including the UK GDPR; the Data Protection Act 2018 (DPA 2018) (and regulations made thereunder) and the Privacy and Electronic Communications Regulations 2003 (SI 2003/2426) as amended and all other legislation and regulatory requirements in force from time to time which apply to a party relating to the use of Personal Data (including, without limitation, the privacy of electronic communications);

GDPR	means as defined by Data Protection Law: (i) the General Data Protection Regulation (EU) 2016/679 as it applies for Customers based in the EU; or (ii) the UK GDPR and associated regulations as it applies for UK based Customers;
Personal Data	means any personal data (as defined by Data Protection Law) Processed by **Bright** on behalf of the Customer pursuant to or in connection with the Agreement;
Processing	has the meaning given to it in Data Protection Law, and Process will be construed accordingly;
Registration	The process by which you successfully register to use a **Bright** Service and create an account, enabling you to sign up to a Trial Period (if/where applicable) and/or purchase a Subscription to the Service from **Bright**, and the term Register shall be construed accordingly.
Regulator	means any regulator or regulatory body (including the Prudential Regulation Authority, the Financial Conduct Authority, the Information Commissioner's Office and the Bank of England or their successors or equivalent authorities outside of the UK) to which the Customer is subject from time to time or whose consent, approval or authority is required so that the Customer can lawfully carry on its business or other competent data privacy authorities;
Standard Contractual Clauses	means: (i) where the EU GDPR applies, the contractual clauses annexed to the European Commission's Implementing Decision 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council ("EU SCCs"); or (ii) where the UK GDPR applies, standard data protection clauses adopted pursuant to or permitted under Article 46 of the UK GDPR ("UK SCCs").

2. Data Protection

2.1. **Bright** acts as a Processor in respect of the Personal Data. Appendix 1 to this Addendum sets out certain information regarding **Bright**'s Processing of the Personal Data as required by article 28(3) of the GDPR.

2.2. The Customer is a Controller or, where acting on behalf of their Customer, is a Processor, in respect of the Personal Data and shall comply with its obligations under Data Protection Law.

2.3. **Bright** shall comply with its obligations as a Processor under Data Protection Law. If **Bright** is or becomes aware of any reason that would prevent its compliance with Data Protection Law or any incident of non-compliance with Data Protection Law in connection with the Processing of Personal Data under this Agreement, it shall notify the Customer in the most expedient time possible.

2.4. **Bright** agrees that it will acquire no rights or interest in the Personal Data, will only Process the Personal Data in accordance with this Agreement and any other written instructions of the Customer, unless Processing of the Personal Data is required by applicable law to which **Bright** is subject, in which case **Bright** shall inform the Customer of that legal requirement before Processing, unless such applicable law prohibits the provision of such information on important grounds of public interest.

2.5. To the extent possible for **Bright** to do so, taking into account the nature of the Processing of Personal Data, and without requiring **Bright** to incur any additional costs, **Bright** agrees to assist the Customer within such reasonable timescale as may be specified by the Customer with the fulfilment of the Customer's obligations to respond to Data Subject rights requests received from the Data Subjects of the Personal Data Processed in connection with this Agreement. Should **Bright** receive any such requests directly, **Bright** will immediately inform the Customer that it has received the request and forthwith forward the request to the Customer. **Bright** will not respond in any way to such a request, except on the instructions of the Customer.

2.6. **Bright** agrees to assist the Customer within such reasonable timescale as may be specified by the Customer with the conduct of Data Protection Impact Assessments and prior consultation requests to Regulators in relation to Personal Data Processing under this Agreement which the Customer reasonably considers to be required of the Customer under article 35 or 36 of the GDPR.

2.7. **Bright** will ensure that its personnel who Process Personal Data under this Agreement are subject to obligations of confidentiality in relation to such Personal Data.

2.8. The Customer hereby generally authorises **Bright** to engage third parties to carryout Processing of the Personal Data (Third-Party Service Providers) provided **Bright** shall ensure that the Processing is carried out under a written contract imposing on the Third-Party Service Provider equivalent obligations as are imposed on **Bright** under this Agreement in respect of the Processing and protection of Personal Data.

Prior to implementing any changes concerning the addition or replacement of Third-Party Service Providers engaged by **Bright** pursuant to the Customer's general authorisation, **Bright** will notify the Customer of such proposed engagement through **Bright**'s published list of Third-Party Service Providers. The Customer may, within fourteen working days of publication of such notice, give notice in writing, objecting to **Bright** disclosing Personal Data to such Third-Party Service Provider and the Customer's objection will be deemed to be the Customer's waiver of **Bright**'s obligation to perform its obligations under the Agreement that **Bright** would ordinarily perform using that Third Party Service Provider. The Customer hereby provides specific authorisation for **Bright** to engage as Third-Party Service Providers those parties listed at:

https://brightsg.com/subprocessors

2.9. **Bright** will also make available to the Customer, any Regulator or their representatives all information necessary to demonstrate compliance with its obligations under this Addendum and allow for and contribute to audits conducted by the Customer or another auditor mandated by the Customer, at the Customer's cost.

2.10. **Bright** will notify the Customer within 24 hours of a known Data Security Breach following the procedure set out in Appendix 3 (and follow-up with a detailed description in writing, including the cause of the breach, remedial action taken and the potential consequences of the breach) and support the Customer in any notification of the breach to Regulators and/or Data Subjects.

2.11. Other than as expressly permitted under this Agreement, on expiry or termination of this Agreement for whatever reason **Bright** shall return, destroy or permanently erase, at the Customer's election, all copies of Customer Personal Data in its possession or control, where technically feasible.

2.12. The provisions of this Clause 2 shall survive the term of this Agreement until **Bright** has returned or destroyed all Personal Data in accordance with Clause 2.11.

2.13. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing of the Personal Data as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, **Bright** shall in relation to the Personal Data implement appropriate technical and organisational measures to ensure a level of security appropriate to that risk, including, as appropriate, the measures referred to in Article 32(1) of the GDPR. In assessing the appropriate level of security, **Bright** shall take account the risks that are presented by Processing of the Personal Data, in particular with respect to a Data Security Breach.

3. Data Exports

3.1. **Bright** may only Process, or permit the Processing, of Personal Data outside the European Economic Area (EEA) or UK under the following conditions:

3.1.1. **Bright** is Processing, or permitting the Processing, of Personal Data in a territory which is subject to a current finding by the European Commission under the Data Protection Laws that the territory provides adequate protection for the privacy rights of individuals; or

3.1.2. **Bright** participates in a valid cross-border transfer mechanism under the Data Protection Laws, so that **Bright** (and, where appropriate, the Customer) can ensure that appropriate safeguards are in place to ensure an adequate level of protection with respect to the privacy rights of individuals as required by article 46 of the GDPR.

3.2. To the extent that any Personal Data transfer from Customer to **Bright** outside the EEA/UK requires execution of Standard Contractual Clauses in order to comply with the Data Protection Laws, the Customer (as Data Exporter) and **Bright** (as Data Importer) hereby enter into the Standard Contractual Clauses in respect of such transfer.

To the extent that any Personal Data transfer from the Customer to a Third-Party Service Provider outside the EEA/UK requires execution of Standard Contractual Clauses in order to comply with the Data Protection Laws, the Customer hereby appoints **Bright** as its agent to enter into the Standard Contractual Clauses between Customer (as Data Exporter) and such Third-Party Service Provider (as Data Importer).

3.3. In the event that the transfer mechanism entered into under Clause 3.1 or 3.2 ceases to be valid, **Bright** shall at the Customer's discretion:

3.3.1. enter into and/or procure that any relevant Third-Party Service Provider enters into an appropriate alternative data transfer mechanism;

3.3.2. destroy any Personal Data in its and/or its Third-Party Service Provider's possession; or

3.3.3. return any Personal Data in its and/or its Third-Party Service Provider's possession to the Customer.

3.4. In the event that there ceases to exist any valid data transfer mechanism which would enable the Personal Data to be lawfully transferred by the Customer to **Bright**, the Customer shall be entitled to terminate this Agreement by giving a minimum of three (3) months' prior written notice to **Bright**.

Appendix 1

Description of the Processing of Personal Data

1. **Nature of Processing**

   Bright provides cloud-based HR, Payroll, Accounting, Practice Management and/or Tax software services to Customers.

   Personal Data is Processed, stored and retrieved automatically for the provision of the Service by **Bright** (as a Data Processor) to the Customer (as a Data Controller) and/or by the Customer (as a Data Processor) to their clients where the Customer itself is a Payroll Bureau, Accounting or Bookkeeping Practice.

   Bright will process Personal Data in order to perform its obligations under the Service Agreement and this Data Processing Addendum.

2. **Purpose of Processing**

   Personal Data is processed during the provision of the Service to the Customer, Customer employees and Customer clients, that may from time-to-time include the following:

   - Individual company payroll services
   - Bureau payroll services
   - Business accounting book-keeping services
   - Accounts production services
   - Practice management services
   - Compliance, Revenue and Tax authority submissions, filings and returns

3. **Categories of Personal Data**

   Bright may from time-to-time Process Personal Data about the following categories of Data Subjects on behalf of the Data Controller:

   HR & Payroll Data

   - Employee Full name (including preferred name)
   - Postal address, email address(es) and phone number(s)
   - Personal Public Service (PPS) / National Insurance (NI) number
   - Revenue information (Revenue Commissioners in Ireland; HMRC in the UK)
   - Bank account name, sort-code, account number
   - Pension details
   - Absence records
   - Contract of employment and other HR details
   - Next of kin
   - Payslip information
   - Date of birth
   - Marital status
   - Nationality, preferred language

Tax & Accounting Data

- Full name (including preferred name)
- Postal address, email address(es) and phone number(s)
- Customer / Supplier name, postal address, email address(es) and phone number(s)
- VAT number
- Financial transaction and bank feed information related to the Customer's business
- Results of checks, including credit checks and anti-money laundering checks
- Business details (including all data resulting from checks with Companies House as provided by the account holder including shareholding and appointments)

And any additional Personal Data provided by you or any Authorised User in the course of the provision of the Services by **Bright**.

4. Special Categories of Personal Data

Bright has no requirement to collect or process any special categories of Personal Data, as defined under Data Protection Law, in order to provide the Service.

5. Children

Bright does not knowingly collect or solicit any Personal Data from anyone under the age of 16 or knowingly allow such persons to register for **Bright**. **Bright** Services are not directed at children under the age of 16. If we learn that we have collected personal data from a child under age 16 without verification of parental consent, we will delete that information as quickly as possible.

6. Categories of Data Subjects

Bright may from time-to-time Process Personal Data about the following categories of Data Subjects on behalf of the Data Controller / Data Processor:

- Company details of the Data Controller and/or Processor
- Employees of the Data Controller
- Clients of the Data Controller
- Customer / Supplier details of the Data Controller (Accounting customers only)

7. Recipients of Personal Data

On request, initiated by the Customer, **Bright** may send revenue and tax return filings for the Customer, to and as required by the relevant tax authorities, and which may include necessary Personal Data of the Customer and their employees, customers and suppliers as applicable.

8. Duration of Processing

Bright will process Personal Data for the term of the Service Agreement (and any exit period) and thereafter as long as **Bright** is required to process any Personal Data pursuant to the Data Protection Legislation.

9. Data Protection Officer

Under Data Protection Law, **Bright** are not required to appoint a dedicated DPO, because:

- we are not a public authority or body;
- we do not perform large scale, regular, systematic monitoring of individuals;
- we do not perform large scale processing of special categories of data or data relating to criminal convictions and offences

All queries regarding Data Protection Law and the processing of Personal Data should be addressed to the Chief Information Security Officer (CISO) via privacy@brightsg.com, or in writing to:

Chief Information Security Officer,
Bright Software Group,

Unit 35,
Duleek Business Park,
Duleek,
Co. Meath,
A92 N15E,
Rep. Of Ireland.

Appendix 2

Security Measures

Information regarding the technical and organisational measures **Bright** has implemented to protect Personal Data in accordance with clause 2.13 of this Addendum is available on our website at:

https://brightsg.com/security

Appendix 3

Template Breach Notification Form

Data Security Breach notifications in accordance with Clause 2.10 above must be made electronically and shall contain at least the following minimum details regarding the Data Security Breach:

1. **Timing of the Breach**

   [**Bright** to insert both the discovery and start time (which may be earlier) of the breach.]

2. **Nature of the Breach**

   [**Bright** to insert a description of the breach, including the categories and approximate number of affected data subjects.]

3. **Likely Consequences**

   [**Bright** to insert a description of the likely consequences of the breach, e.g., risk of identity theft, media coverage, etc.]

4. **Mitigating Measures**

   [**Bright** to insert description of the measures taken/to be taken to address the breach and mitigate its effects.]