Data Processing Addendum
(May 2022)

This data processing addendum ("**Addendum**") forms part of the written or electronic agreement between Sage and Customer for the purchase of products and/or solutions identified in the agreement (collectively, the "**Services**") from Sage (the "**Main Agreement**"). Each of Customer and Sage may be referred to herein as a "party" and together the "parties".

How this Addendum applies

This Addendum is to ensure the protection and security of data which is shared with Sage or accessed by Sage for processing on Customer's behalf.

Data protection laws worldwide, including the GDPR (as defined below), place certain obligations upon a data controller to ensure that any data processor it engages provides sufficient guarantees to ensure that the processing of the personal data carried out on its behalf is secure.

This Addendum exists to ensure that there are sufficient security guarantees in place and that the processing conducted by Sage on behalf of Customer complies with obligations equivalent to those in the GDPR.

How to accept this Addendum

This Addendum consists of two parts: the main terms, and Annex 1.

This Addendum has been pre-agreed by Sage.

You are deemed to have accepted this Addendum and its terms if you continue to access or use the Services.

The Customer entity that is deemed to have accepted to this Addendum shall be the same as the Customer entity party to the Main Agreement.

If the Customer entity to this Addendum is not a party to the Main Agreement directly with Sage, this Addendum is not valid and is not legally binding.

Data processing terms

1. Definitions and Interpretation

1.1. All capitalized terms not defined herein shall have the meanings set forth in the Main Agreement.

1.2. In this Addendum, the following terms shall have the meanings set out below:

"**Affiliate**" means any entity that directly or indirectly controls, is controlled by, or is under common control of the subject entity, where "control" is the ownership or control (whether directly or indirectly) of at least 50% of the voting rights in the entity, or otherwise the power to direct the management and policies of the entity. An entity is an Affiliate only so long as such control continues;

"**Customer**" means the customer entity that is party to the Main Agreement;

"**Data Controller**" means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data; where the purposes and means of such Processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;

"**Data Processor**" means a natural or legal person, public authority, agency or other body which Processes Personal Data on behalf of the Data Controller;

"**Data Protection Laws**" means all applicable EU laws and regulations governing the use or processing of Personal Data, including (where applicable) the European Union Directive 95/46/EC (until and including 24 May 2018), the GDPR (from and including 25 May 2018) and any national implementing laws, regulations and secondary legislation, as amended or updated from time to time;

"**EEA**" means the European Economic Area;

"**GDPR**" means EU General Data Protection Regulation 2016/679;

"**Personal Data**" means any information relating to an identified or identifiable natural person ("**Data Subject**") and which is provided by Customer to Sage and Processed by Sage as Sage as Data Processor as part of its provision of the Services to Customer; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

"**Processing**" means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction and "**Process**", "**Processed**" and "**Processes**" shall be construed accordingly;

"**Sage**" shall mean the Sage entity which is party to the Main Agreement;

"**Sage Group**" means Sage and any of its Affiliates; and

"**Supervisory Authority**" means an independent public authority which is established under applicable Member State law and which concerns itself with the Processing of Personal Data.

2. Processing of Personal Data

2.1. The parties acknowledge and confirm that Customer is the Data Controller in respect of the Personal Data and that Customer has sole responsibility for its legality, reliability, integrity, accuracy and quality.

2.2. Sage agrees to comply with the following provisions with respect to any Personal Data Processed for Customer in connection with the provision of the Services under the Main Agreement.

2.3. Customer warrants and represents that:

2.3.1. it will comply with and will ensure that its instructions for the Processing of Personal Data will comply with the Data Protection Laws;

2.3.2. it is authorised pursuant to the Data Protection Laws to disclose any Personal Data which it discloses or otherwise provides to Sage regarding persons other than itself;

2.3.3. it will where necessary, and in accordance with the Data Protection Laws, obtain all necessary consents and rights and provide all necessary information and notices to Data Subjects in order for:

2.3.3.1. it to disclose the Personal Data to Sage;

2.3.3.2. Sage to Process the Personal Data for the purposes set out in the Main Agreement; and

2.3.3.3. Sage to disclose the Personal Data to: (a) its agents, service providers and Affiliates; (b) law enforcement agencies; (c) any other person in order to meet any legal obligations on Sage, including statutory or regulatory reporting; and (d) any other person who has a legal right to require disclosure of the information, including where the recipients of the Personal Data are outside the European Economic Area.

2.4. Sage warrants and represents that it:

2.4.1. shall comply with the Data Protection Laws applicable whilst such Personal Data is in its control;

2.4.2. when acting in the capacity of a Processor, shall only Process the Personal Data:

2.4.2.1. as is necessary for the provision of the Services under the Main Agreement and the performance of its obligations under the Main Agreement; or

2.4.2.2. otherwise on Customer's documented instructions.

3. Sage Obligations

3.1. **Sage shall:**

3.1.1. taking into account the nature of the Processing, assist Customer by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of Customer's obligation to respond to requests from individuals for exercising Data Subjects' rights;

3.1.2. taking into account the nature of the Processing, and the information available to it, provide reasonable assistance to Customer in ensuring compliance with its obligations relating to:

3.1.2.1. notifications to Supervisory Authorities;

3.1.2.2. prior consultations with Supervisory Authorities;

3.1.2.3. communication of any breach to Data Subjects; and

3.1.2.4. privacy impact assessments.

4. Personnel

4.1. Sage shall:

4.1.1. take reasonable steps to ensure the reliability of any personnel who may have access to the Personal Data;

4.1.2. ensure that access to the Personal Data is strictly limited to those individuals who need to know and/or access the Personal Data for the purposes of the Main Agreement; and

4.1.3. ensure that persons authorised to Process the Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

4.2. If so required by Data Protection Laws, Sage shall appoint a data protection officer and make details of the same publicly available.

5. Security and Audit

5.1. Sage shall implement and maintain appropriate technical and organisational security measures appropriate to the risks presented by the relevant Processing activity to protect the Personal Data against unauthorised or unlawful Processing and against accidental loss, destruction, damage or disclosure. Such measures include, without limitation, the security measures set out in Annex 1.

5.2. Subject to any existing obligations of confidentiality owed to other parties, Sage shall make available to Customer all information reasonably necessary to demonstrate compliance with the obligations set out in this Addendum, which may include a summary of any available third party security audit report, or shall, at Customer's sole cost and expense (including, for the avoidance of doubt any expenses reasonably incurred by Sage), allow for and contribute to independent audits, including inspections, conducted by a suitably-qualified third party auditor mandated by Customer and approved by Sage.

6. Data Breach

6.1. Sage shall notify Customer if it becomes aware of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to the Personal Data arising from any act or omission of Sage or its sub-processors.

7. Transfer of Personal Data outside the EEA

7.1. Customer expressly agrees that Sage may transfer Customer Data within the Sage Group on the terms of Sage's Master Data Processing and Transfer Agreements, which incorporate the European Commission's standard contractual clauses.

7.2. Customer acknowledges and accepts that the provision of the Services may require the Processing of Personal Data by sub-processors in countries outside the EEA. Sage shall not transfer Personal Data outside the EEA to a sub-processor where such transfer is not

subject to: (a) an adequacy decision (in accordance with Article 45 of the GDPR); or (b) appropriate safeguards (in accordance with Article 46 of the GDPR); or (c) binding corporate rules (in accordance with Article 47 of the GDPR), without Customer's prior written consent.

8. Return and deletion

8.1. At Customer's option, Sage shall delete or return all Personal Data to Customer at the end of the provision of the Services and delete all existing copies of Personal Data unless Sage is under a legal obligation to require storage of that data or Sage has another legitimate business reason for doing so.

9. Use of Sub-Processors

9.1. Customer agrees that Sage has general authority to engage third parties, partners, agents or service providers, including its Affiliates, to Process Personal Data on Customer's behalf in order to provide the applications, products, services and information Customer has requested or which Sage believes is of interest to Customer ("**Approved Sub-Processors**"). Sage shall not engage a sub-processor to carry out specific Processing activities which fall outside the general authority granted above without Customer's prior specific written authorisation and, where such other sub-processor is so engaged, Sage shall ensure that the same obligations set out in this Addendum shall be imposed on that sub-processor.

9.2. Sage shall be liable for the acts and omissions of its Approved Sub-Processors to the same extent Sage would be liable if performing the services of each Approved Sub-Processor directly under the terms of this Addendum.

10. General

10.1. Except as modified by this Addendum, the terms of the Main Agreement shall remain in full force and effect. In the event of any conflict between this Addendum and any privacy-related provisions in the Main Agreement, the terms of this Addendum will prevail.

10.2. Sage and its Affiliates liability under or in connection with this Addendum is subject to the limitation on liability set out in the Main Agreement.

10.3. Sage may modify the terms of this Addendum as provided in the Main Agreement.

ANNEX 1

Security Measures

Category	Measure
Physical Access Control	All of Sage's data processing equipment is hosted in the data centres. Access to these data centres are restricted by well-defined processes and ID Readers. They are also monitored on a 24/7 basis by security staff and surveillance cameras.
Logical access prevention	Sage's data processing systems are accessed by a limited number of authorised users with appropriate access rights. Dual factor authentication is implemented for each role. Such access to transaction data is restricted to a few users from the Operations (Live Services) Team. Within the Live services team different roles are created based on the job requirements. Also, the activity of each user is monitored through monitoring solutions.
Data access control	Only a limited set of users from Sage's Live Services technical team have access to the data processing systems which contain transaction data. Data access privileges are defined by the job role of the user; accordingly only authorised users with appropriate privileges have the access to transaction data. No other user has any kind of access to this data. Sage has also implemented a well-defined approval process to control access to data within its systems. Sage has also implemented monitoring solutions to identify any attempts or actual unauthorised access to its systems and data.
Data transfer control	Sage's processes and systems ensure that all Personal Data is encrypted whilst in transit or in storage. Sage has implemented logging mechanisms to track data flows. Sage users have restricted access to transaction data.
Entry control	Sage has implemented logging and monitoring which enable tracking of changes and any addition/modification/deletion of data and by whom. Additionally, Sage has also implemented role based access mechanisms along with dual factor authentication.
Instruction control	Sage has defined and implemented standard process and policies which require special approval the concerned parties within its business, including: operational, legal and technical teams. Pre-identified individuals from Sage's Live Services team are only involved in the actual processing of transaction data. Pre-defined processes are in place to ensure that the confidentiality and the integrity of such data is maintained.

Availability control	Sage has implemented well defined disaster recovery plans which are tested on a regular basis. Sage has implemented two data centres, which operate in a fail-over mode. Data is replicated between each data centre. Backup procedures and schedules have been defined and implemented.
Separation control	Data is separated both by logical and physical access controls. Network segmentations are in place to ensure that data is stored in the most restrictive zone of the network. Access to the data processing systems and the data itself is restricted by role based privileges and dual factor authentication. All access to the data systems and the data is logged and monitored. The production environment is completely segregated from the test environment.