Data and Analytics

Definitions

"**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.

"**Customer Data**" shall mean the data, information or material provided, inputted or submitted by you or on your behalf into the Services, which may include data relating to your customers and/or employees.

"**Customer Personal Data**" has the meaning set out in clause 1.

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

"**Personal Data**" means any information relating to an identified or identifiable natural person ("**Data Subject**"); 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.

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

"**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.

"**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.

Sage as Data Processor

1. For the purposes of this Agreement, the parties agree that you are the Data Controller in respect of Personal Data contained within Customer Data ("**Customer Personal Data**") and as Data Controller, you have sole responsibility for its legality, reliability, integrity, accuracy and quality.

2. You warrant and represent that:
   2.1. you will comply with and will ensure that your instructions for the Processing of Customer Personal Data will comply the Data Protection Laws;
   2.2. you are authorised pursuant to the Data Protection Laws to disclose any Customer Personal Data which you disclose or otherwise provide to us regarding persons other than yourself;
   2.3. you 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:
      2.3.1. you to disclose the Customer Personal Data to us;
      2.3.2. us to Process the Customer Personal Data for the purposes set out in this Agreement; and
      2.3.3. us to disclose the Customer Personal Data to: (a) our agents, service providers and other companies within the Sage group of companies; (b) law enforcement agencies; (c) any other person in order to meet any legal obligations on us, 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 Customer Personal Data are outside the European Economic Area.

3. To the extent that Sage Processes any Customer Personal Data, the terms of Exhibit A shall apply and the parties agree to comply with such terms.

Sage as Data Controller

4. Where, and to the extent we Process your Personal Data as a Data Controller in accordance with our Privacy Notice http://www.sage.com/au/footer/privacy-policy, we shall comply with all Data Protection Laws applicable to us as Data Controller.

Analytics

5. You agree that we may record, retain and use Customer Data generated and stored during your use of the Service (including Customer Personal Data, which we shall Process as Data Controller as set out in our Privacy Notice http://www.sage.com/au/footer/privacy-policy on the basis of our legitimate business interests), in order to:
   5.1. deliver advertising, marketing (including in-product messaging) or information to you which may be useful to you, based on your use of Services;
   5.2. carry out research and development to improve our, and our Affiliates', services, products and applications;
   5.3. develop and provide new and existing functionality and services (including statistical analysis, benchmarking and forecasting services) to you and other Sage customers;
   5.4. provide you with location based services (for example location relevant content) where we collect geo-location data to provide a relevant experience,

   provided that Sage shall only record, retain and use the Customer Data and/or Process Customer Personal Data on a pseudonymised basis, displayed at aggregated levels, which will not be linked back to you or to any living individual. If at any time you do not want us to use Customer Data in the manner described in this clause 5, please contact us at the email address set out in the Privacy Notice http://www.sage.com/au/footer/privacy-policy

Exhibit A
Data Processing Addendum

1. Interpretation

1.1. Where there is any inconsistency between the terms of this Exhibit A and any other terms of this Agreement, the terms of this Exhibit A shall take precedence.

2. **Processing of Customer Data**

2.1. During the term of this agreement we warrant and represent that we:

2.1.1. shall comply with the Data Protection Laws applicable to us whilst such Customer Data is in our control;

2.1.2. when acting in the capacity of a Processor, shall only Process the Customer Data:

2.1.2.1. as is necessary for the provision of the Services under this Agreement and the performance of our obligations under this Agreement; or
2.1.2.2. otherwise on your documented instructions.

2.2. We agree to comply with the following provisions with respect to any Personal Data Processed for you in connection with the provision of the Service under this Agreement.

3. Obligations of Sage

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; and

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 Customer Data;
4.1.2. ensure that access to the Customer Data is strictly limited to those individuals who need to know and/or access the Customer Data for the purposes of this Agreement; and
4.1.3. ensure that persons authorised to Process the Customer 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 Customer 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, we shall make available to you all information reasonably necessary to demonstrate compliance with the obligations set out in this Exhibit A, which may include a summary of any available third party security audit report, or shall, at your sole cost and expense (including, for the avoidance of doubt any expenses reasonably incurred by us), allow for and contribute to independent audits, including inspections, conducted by a suitably-qualified third party auditor mandated by you and approved by us.

6. Data Breach

6.1. Sage shall notify you if we become 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. You expressly agree that we may transfer Customer Data within the Sage group of companies on the terms of Sage's Master Data Processing and Transfer Agreements, which incorporate the European Commission's standard contractual clauses.

7.2. You acknowledge that the provision of the Service may require the Processing of Personal Data by sub-processors in countries outside the EEA. We 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 your prior written consent.

8. Return and deletion

8.1. At your option, Sage shall delete or return all Customer Data to you at the end of the provision of the Services and delete all existing copies of Customer Data unless we are under a legal obligation to require storage of that data or we have another legitimate business reason for doing so.

9. Use of Sub-Processors

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

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 Exhibit A.

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.*