Data Protection Addendum
October 2019

1. DEFINITIONS & INTERPRETATION

1.1. In this Addendum, unless the context otherwise requires:

"**Agreement**" means the agreement between you and us that links to this Addendum. Terms defined in the Agreement and used in this Addendum without further definition have the meaning given to them in the Agreement.

"**Data Protection Laws**" means all applicable European Union and UK laws and regulations governing the use or processing of personal data, including the General Data Protection Regulation (EU) 2016/679 ("**GDPR**") and any national laws implementing or supplementing or superseding the foregoing; "**binding corporate rules**", "**controller**", "**data subject**", "**personal data**", "**personal data breach**", "**processing**", "**processor**", "**pseudonymisation**" and "**supervisory authority**" have the meanings given to them in Data Protection Laws and the term "**supervisory authority**" shall be deemed to include the UK Information Commissioner;

"**European Law**" means European Union law, member state law and/or the law in any part of the UK;

"**International Transfer**" means a transfer of Relevant Data from the European Union or the UK to a third country or international organisation;

"**Relevant Data**" means all Customer Data: (i) which relate to a data subject; and (ii) in respect of which you (the customer) are the controller; and (iii) which will be processed by us on your behalf in connection with the Agreement, as more particularly described in Schedule 1 (Specification of processing);

"**Security Incident**" means a personal data breach in respect of the Relevant Data;

"**Sub-processor**" means another processor of Relevant Data engaged by us; and

"**Your Data Responsibilities**" means your protection responsibilities under or in connection with the Agreement, including:

- your contractual relationships with third parties, other members of your group and your other processors;
- the compliance of your processing (and of other members of your group, if any) under this Addendum and the Agreement as controller;
- the compliance of your business with applicable Data Protection Laws;
- the compliance of your intra-group transfers (if any) of personal data;
- the compliance of your transfers (if any) of personal data to processors and/or other suppliers;
- the compliance of your processing of Relevant Data as controller;
- the compliance of your handling of and response to data subjects' requests under applicable Data Protection Laws, regardless of any assistance we may provide; and
- the compliance of your remote use of our systems from a third country or international organisation (if any)

and otherwise complying with your controller obligations under applicable Data Protection Laws.

1.2. Where there is any express inconsistency between the terms of this Addendum and any other term of the Agreement, the terms of this Addendum shall take precedence.

2. PROCESSING RELEVANT DATA

2.1. The parties acknowledge that, for the purposes of the Agreement, you are the controller and we are the processor of the Relevant Data. Details of the processing of Relevant Data we shall carry out for you are set out in Schedule 1 (Specification of processing), which you agree that you have checked and confirmed as correct or have changed as necessary to reflect the processing of Relevant Data under the Agreement. To change Schedule 1, please download a copy from https://www.sagepeople.com/legal/dpa and send it to globalprivacy@sage.com (marked "Sage People-DPA"). We reserve the right to challenge any changes which we consider to be incorrect. If you have changed Schedule 1 (Specification of processing), it is your responsibility to provide it to us and to agree the changes with us before you enter into the Agreement. The parties may update Schedule 1 (Specification of processing) during the term of the Agreement, in accordance with the Agreement or by mutual written agreement, to reflect changes in processing or for other reasons. Each updated version shall form part of the Addendum.

2.2. You warrant and represent that:

2.2.1. you will comply, and will ensure that your instructions for the processing of Relevant Data will comply, with Data Protection Laws;

2.2.2. you are authorised by the relevant data subjects, or are otherwise permitted pursuant to Data Protection Laws, to disclose the Relevant Data to us;

2.2.3. you will, where necessary, and in accordance with Data Protection Laws, obtain all necessary consents and rights and provide all necessary information and notices to data subjects in order for:
(i) you to disclose the Relevant Data to us; and
(ii) us to process the Relevant Data for the purposes set out in the Agreement and this Addendum and in accordance with Data Protection Laws; and

2.2.4. your instructions to us and/or to any Sub-processor(s) relating to processing of Relevant Data will not put us or any Sub-processor(s) in breach of Data Protection Laws.

2.3. You acknowledge and agree that we may be required or permitted by European Law to disclose certain personal data or other information relating to you, the Services and/or the Agreement to third parties. We may also be required by European Law to process the Relevant Data other than on your documented instructions under paragraph 3.1.1. If that happens, we will inform you of that legal requirement before the processing, unless that legal requirement or law prohibits us from doing so on important grounds of public interest. Where we are prohibited from informing you of the legal requirement, and/or where we are subject to an ongoing legal requirement to process, you give us general authorisation and consent to carry out that processing without your specific authorisation or consent. Just to be clear, that authorisation/consent is from you as a business customer: it is not consent from you as an individual under the GDPR.

2.4. Where we assist you with your compliance with data protection requirements or where we otherwise assist you under or pursuant to this Addendum, we reserve the right to charge you on the basis of our standard applicable pricing. In addition you will be responsible for the cost of engaging any third-party auditor you wish to commission to conduct an audit pursuant to this Addendum. You will reimburse us for all additional costs and liabilities incurred by us resulting from any failure or delay(s) by you to comply with your obligations under this Addendum. Nothing in this paragraph 2.4 shall affect our rights to charge you under the Agreement.

3. **OUR OBLIGATIONS**

3.1. We shall:

3.1.1. ***Lawful Instructions****:* except as indicated in paragraph 2.3 and paragraph 5.1.5, only process the Relevant Data in accordance with your documented instructions including with regard to International Transfers; you hereby instruct us to process the Relevant Data in order to provide the Services and in accordance with any other instructions set out in the Agreement; nothing in this paragraph 3.1.1 will permit you to vary our obligations and/or any instructions under the Agreement other than with our prior written agreement; if we reasonably consider that any of your instructions may put us and/or any Sub-processor(s) in breach of Data Protection Laws and/or any provision of the Agreement, we shall be entitled not to carry out that processing and will not be in breach of the Agreement or otherwise liable to you as a result of our failure to carry out or delays in carrying out that processing;

3.1.2. ***Security of Processing****:* implement appropriate technical and organisational measures to ensure a level of security appropriate to the risks that are presented by processing (in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to the Relevant Data), taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of the processing of Relevant Data, as well as the risk of varying likelihood and severity for the rights and freedoms of the data subjects, and including, as and where appropriate, measures to ensure:

(a) the pseudonymisation and/or encryption of the Relevant Data;
(b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
(c) the ability to restore the availability of and access to the Relevant Data in a timely manner in the event of physical or technical incident; and
(d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing;

3.1.3. take steps to ensure that any natural person acting under our authority who has access to Relevant Data does not process them except on your instructions, unless he or she is required to do so by European Law; and

3.1.4. operate, maintain and enforce an information security management programme ("Security Programme") which is consistent with recognised industry practice; the Security Programme contains appropriate administrative, physical, technical and organisational safeguards, policies and controls in the following areas:
• Information security policies
• Organisation of information security
• Human resources security
• Asset management

• Access control
• Cryptography
• Physical and environmental security
• Operations security
• Communications security
• System acquisition, development and maintenance
• Supplier relationships
• Information security incident management
• Information security aspects of business continuity management
• Legislative, regulatory and contractual compliance;

3.1.5. ***Assistance in Compliance****:* taking into account the nature of the processing, assist you by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of your obligation to respond to requests by data subjects exercising their rights under Data Protection Laws; **please note** that if we assist you in responding to requests, including the provision of tools or reports within the Services to support your searches, we give no warranty and make no representation as to the compliance of the nature and scope of the search with applicable Data Protection Laws, nor do we warrant or represent the accuracy or completeness of the output of our assistance: it is your responsibility, and not our responsibility, to determine the nature and scope of the search, validate the output and ensure that your response to the data subject is compliant in all respects with applicable Data Protection Laws, as further referred to in paragraph 7;

3.1.6. assist you, by providing you with necessary information in our possession, in ensuring compliance with the obligations in Data Protection Laws in respect of security of processing, notification of a Security Incident to a supervisory authority, communication of a Security Incident to the data subject, data protection impact assessments and prior consultation, taking into account the nature of processing and the information available to us;

3.1.7. notify you without undue delay after we become aware of a Security Incident;

3.1.8. ***Staff Confidentiality Obligations***: ensure that our staff who are authorised to process the Relevant Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality; and

3.1.9. ***Return or Deletion of Relevant Data****:* at your option (to be exercised by written notice from you) delete or return to you (as provided in the Agreement), all the Relevant Data after the end of the provision of the Services relating to the processing, and (in the case of return), delete existing copies of the Relevant Data unless any European Law requires us to store the Relevant Data; however we will be entitled to retain any Relevant Data which: (a) we have to keep to comply with any applicable laws; (b) we are required to keep for insurance, accounting, taxation, legal, regulatory or record keeping purposes; or (c) is necessary to investigate and resolve performance or security issues, and this Addendum will continue to apply to retained Relevant Data; notwithstanding any provision to the contrary in the Agreement, we shall be entitled to delete the Relevant Data in accordance with our normal data cleansing policies; in respect of Relevant Data which are archived/backed up, you instruct us to retain those archived/backed up Relevant Data in accordance with the typical period for which those Relevant Data are archived/backed up by us for the Services in question.

4. **USE OF SUB-PROCESSORS**

4.1. Without prejudice to any provisions in the Agreement relating to sub-contracting, you hereby give your general written authorisation to us engaging Sub-processors to process the Relevant Data. Where the Sub-processor is in a third country, you hereby instruct us to make an International Transfer under paragraph 5.

4.2. We shall respect the conditions referred to in Article 28(2) GDPR for engaging a Sub-processor.

4.3. If we appoint a Sub-processor, we will put a written contract in place between us and the Sub-processor that specifies the Sub-processor's processing activities and imposes on the Sub-processor substantially similar terms, appropriate to the sub-processing they will undertake. If that Sub-processor fails to fulfil its data protection obligations, we shall remain liable to you for the performance of that Sub-processor's obligations.

5. **TRANSFERS OF PERSONAL DATA TO A THIRD COUNTRY OR INTERNATIONAL ORGANISATION**

5.1. We shall only make an International Transfer to a recipient:

5.1.1. on the basis of an adequacy decision made under Data Protection Laws;

5.1.2. on the basis of appropriate safeguards that are in place, and you agree to execute any documents (including data transfer agreements) relating to that International Transfer which we request that you to execute from time to time for that purpose;

5.1.3. on the basis of binding corporate rules approved by a competent supervisory authority; or

5.1.4. on the basis of an applicable derogation in Data Protection Laws

which in each case applies to the International Transfer in question; or

5.1.5. if we are required to make the International Transfer to comply with European Law, in which case we will notify you of the legal requirement prior to that International Transfer unless the European Law prohibits us from notifying you on public interest grounds. Where we are prohibited from informing you of the legal requirement, and/or where we are subject to an ongoing legal requirement to transfer, you (a business customer) give us general authorisation and consent to carry out that transfer without your specific authorisation or consent.

5.2. You acknowledge and agree that you shall be responsible, and we shall not be responsible, for the compliance of any International Transfers that occur when Users access the Services through a browser from a third country or international organisation, as further referred to in paragraph 7.

6. RIGHTS OF AUDIT

6.1. At your reasonable request and subject to you (and any third-party auditor) entering into an appropriate confidentiality agreement, we shall:

6.1.1. make available to you such information as may reasonably be necessary to demonstrate compliance with the obligations for processor agreements laid down in Data Protection Laws; and

6.1.2. subject to paragraphs 6.3 and 6.4 below, allow you (or an independent, third-party professional auditor mandated by you and acceptable to us, both of us acting reasonably) to conduct an audit, including inspection, of our processing of Relevant Data pursuant to the Agreement, and contribute to that audit,

except that you agree that nothing in this paragraph 6.1 shall require us to act in breach of an obligation of confidentiality owed to a third party.

6.2. With respect to paragraph 6.1, we shall immediately inform you in writing, but without any obligation to monitor or enquire as to the legality of your instructions or to give legal advice if, in our opinion, to follow an instruction given by you would give rise to a breach of applicable Data Protection Laws.

6.3. Where we have commissioned audit report(s) which we offer to make available to you, you agree that you may only proceed with your own audit/inspection if, acting in good faith, you are reasonably dissatisfied with the audit report(s), and that your own audit/inspection is subject to our rights in paragraph 2.4. You must coordinate with us on the timing and scope of any such audit/inspection and refrain from any act or omission that could lead to the degradation, overload or unavailability of the Services. The scope of your audit must exclude other customers' data. Any testing, probing or scanning tools used on our infrastructure must be pre-approved by us. You must not and must instruct any third-party auditor not to) include in your audit report any sensitive information that could be used by a third party to the detriment of the security of the Services (including, but not only, details of vulnerabilities). You must instruct any third-party auditor to give us the reasonable opportunity to review the report before it is provided to you in final form and to communicate with the auditor to resolve any questions or issues of fact. You and the auditor must keep the results and findings of any audits confidential and disclose them to third parties only to the extent required by law.

6.4. In relation to any Sub-processors that are engaged pursuant to paragraph 4 and/or any data centre facilities used by us, you acknowledge and agree that it is sufficient, for the purposes of satisfying the requirements of paragraph 6.1, that we shall have a right to audit or inspect those Sub-processors and/or those data centre facilities or their available audit reports on your behalf, subject to reasonable restrictions.

7. YOUR OBLIGATIONS

7.1. You shall comply with Your Data Responsibilities. We are not in any way responsible for Your Data Responsibilities.

8. SAGE AS CONTROLLER

8.1. We will process personal data as a controller under the Agreement and/or this Addendum, for example but not exhaustively, in the management of our relationship with you, or in our use of Usage Data under paragraph 9. Please see our website privacy notice for further details. Paragraphs 2.1 (and Schedule 1) and paragraphs 3 to 6 inclusive of this Addendum shall not apply to personal data of which we are a controller.

9. JOINT CONTROLLERS

9.1. As at the date of the Agreement, the parties do not consider themselves to be joint controllers (that is, where two or more controllers jointly determine the purposes and means of processing of the Relevant Data) for the purpose of the processing activities referred to in this Addendum.

9.2. If and to the extent that the parties later determine that their arrangement has become one of joint controllers of the Relevant Data, they shall comply with the requirements set out in article 26 GDPR.

Schedule 1
Specification of processing

Subject matter and duration of the processing of Relevant Data:
Subject matter: the provision of the Services and any professional services under the Agreement
Duration: the term of the Agreement including any transitional periods on entrance or exit from the Agreement and any archival/backup period references in clause 3.1.9 of this Addendum.

Nature and purpose of the processing of Relevant Data:
*Any or all of the following processing operations for the purpose of providing the Services for which you subscribe; your use of and requirements for the Services; any professional services under the Agreement; the requirements in the Agreement; and third party requests and other extraneous events (the "**Purposes**"):*
- ✓ Collection
- ✓ Recording
- ✓ Organisation
- ✓ Structuring
- ✓ Storage
- ✓ Adaptation/alteration
- ✓ Retrieval
- ✓ Consultation
- ✓ Use
- ✓ Disclosure by transmission / dissemination or otherwise making available
- ✓ Alignment / combination
- ✓ Restriction
- ✓ Erasure / destruction
- ✓ Others: .....

Type of Relevant Data (including any special categories of Relevant Data or other sensitive data):
Any or all of the following depending on the Purposes:
- ✓ **Personal details** (any information that identifies the data subject and their personal characteristics e.g. name, address, contact details, age, sex, date of birth, physical description and any identifier issued by a public body, e.g. National Insurance number or social security number)
- ✓ **Education and training details** (any information which relates to the education and any professional training of the data subject e.g. academic records, qualifications, skills, training records, professional expertise, and student and pupil records)
- ✓ **Family, lifestyle and social circumstances** (any information relating to the family of the Data subject and the data subject's lifestyle and social circumstances e.g. current marriage and partnerships and marital history, details of family and other household members, habits, housing, travel details, leisure activities and membership of charitable or voluntary organisations)
- ✓ **Employment details** (any information relating to the employment of the data subject e.g. employment and career history, recruitment and termination details, attendance records, health and safety records, performance appraisals, training records and security records) and pension information)
- ✓ **Financial details** (any information relating to the financial affairs of the data subject e.g. income, salary, assets and investments, payments, creditworthiness, loans, benefits, grants, insurance details and pension information)
- ✓ **Goods and services provided** (any information relating to goods and services that have been provided e.g. goods or services supplied, licences issued, agreements and contracts)
- ✓ **Special categories of personal data** (racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a data subject, data concerning health or data concerning a data subject's sex life or sexual orientation)
- ✓ **Criminal data** (criminal convictions and offences or related security measures, including personal data relating to: (a) the alleged commission of offences by the individual (b) proceedings for an offence committed or alleged to have been committed by the individual or the disposal of such proceedings, including sentencing)
- ✓ Others: .....

Categories of data subjects:
Any or all of the following depending on the Purposes:
- ✓ Staff including volunteers, agents, temporary and casual workers of yours
- ✓ Customers/clients (who are individuals or sole traders) of yours
- ✓ Suppliers (sole traders) of yours
- ✓ Contact persons of corporate entities (e.g. at suppliers or customers, where supplier is not a sole trader or customer is not an individual) of yours
- ✓ Members or supporters (e.g. shareholders) of yours
- ✓ Complainants, correspondents and enquirers of yours
- ✓ Relatives, guardians and associates (of data subjects) of your staff
- ✓ Advisers, consultants and other professional experts or legal representatives (individuals/sole traders) of yours
- ✓ Partners, resellers (individuals/sole traders) of yours
- ✓ Donors, supporters (individuals/sole traders) of yours
- ✓ Students if input by you
- ✓ Offenders and suspected offenders if input by you
- ✓ Landlords/tenants of yours
- ✓ Users of the Services not included in the above
- ✓ Others: .....

Controller's obligations and rights:
The obligations in paragraph 2.2 and paragraph 7.
The rights to enforce the data processing terms in paragraphs 3, 4, 5 and 6 against us as your processor.