Data Processing And Sharing Agreement

NOTE: WorkInConfidence's standard relationship with its clients is that of Joint Data Controller. Click on the hyperlink to see our Joint Controller Agreement.

This is important for Us and clients so we can guarantee we will not be required to disclose user IDs.

There may be circumstances in which we agree (subject to suitable protections for user identities) to be Processor. In those circumstances this Data Processing and Sharing Agreement shall apply.

Capitalised terms used in this Data Protection Schedule have the meanings given in the Terms and Conditions, unless otherwise defined herein.

1. Additional definitions

1.1 "Data Controller", "Controller", "Data Processor", "Processor", "Data Subject", "Personal Data", "Personal Data Breach" and "processing" shall have the meaning given to those terms in the Data Protection Legislation (providing that "Data Controller" and "Data Processor" shall be deemed to mean, respectively, "Controller" and "Processor" as such terms are defined in the General Data Protection Regulation) and "process" and "processed" shall be construed accordingly.

1.2 "Standard Contractual Clauses" means the European Commission's Standard Contractual Clauses according to the EU Commission decision of 05 February 2010 (2010/87/EU) attached hereto as Annex 3.

1.3 "Data Protection Legislation" means the UK Data Protection Legislation and any other European Union legislation relating to Personal Data 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).

1.4 "UK Data Protection Legislation" means all applicable data protection and privacy legislation in force from time to time in the UK including the General Data Protection Regulation ((EU) 2016/679); the Data Protection Act 2018; the Privacy and Electronic Communications Directive 2002/58/EC (as updated by Directive 2009/136/EC) and the Privacy and Electronic Communications Regulations 2003 (SI 2003/2426) as amended.

2. The parties agree that:

2.1 for the purposes of the Data Protection Legislation, the Customer is the Controller and Work in Confidence Limited (WIC) is the Processor, where Annex 1 sets out the scope, nature and purpose of processing by the Processor, the duration of the processing and the types of Personal Data and categories of Data Subject.

2.2 Where a party is processing Personal Data in their capacity as a separate and independent Controller, each party shall at all times comply with the Data Protection Legislation and shall not, by its act or omission, cause the other party to breach the Data Protection Legislation.

2.3 The Customer will ensure that it has all necessary appropriate consents and notices in place to enable lawful transfer of the Personal Data to the Processor and/or lawful collection of the Personal Data by the Processor on behalf of the Customer for the duration and purposes of this Agreement.

2.4 To the extent any processing of EU Data by the Processor takes place in any country outside the European Economic Area in a country that does not provide an adequate level of protection of personal data (as recognized by the European Commission), then the parties agree that the Standard

Contractual Clauses set out in Annex 3 will apply in respect of that processing of EU Data, and the Processor will comply with the obligations of the 'data importer' in the standard contractual clauses and the Customer will comply with the obligations of the 'data exporter' in the standard contractual clauses.

3. Data Processor terms

3.1 Without prejudice to the foregoing, to the extent that one party is deemed to act as a Data Processor for the other party (as the Data Controller) in respect of Personal Data, the Data Processor shall in respect of such Personal Data:

3.1.1 only process Personal Data on the documented instructions of the Data Controller for the purpose of performing its obligations under this Agreement or as may be agreed in writing between the parties (and on written instructions from the Data Controller to ensure compliance with the Data Protection Legislation and shall not process the Personal Data for its own purposes);

3.1.2 to the extent permitted by law, immediately notify the Data Controller in writing if it believes it has been provided with any instruction to process the Personal Data in breach of the Data Protection Legislation;

3.1.3 use reasonable endeavours to notify the other party if it is obliged to make a disclosure of the Personal Data collected under or in connection with the Agreement under any statutory requirement, such notification to be made in advance of such disclosure or immediately thereafter unless prohibited by law.

3.1.4 take appropriate technical and organisational measures against unauthorised or unlawful processing of Personal Data collected under or in connection with the Agreement and against accidental, unauthorised or unlawful processing of, loss or destruction of, alteration or damage to, disclosure of, or access to, Personal Data and that, having regard to the state of technical development and the cost of implementing any measures, such measures will ensure a level of security appropriate to the harm that might result from such unauthorised or unlawful processing or accidental loss, destruction, alteration, or damage to or disclosure of, or access to the Personal Data and the nature of the Personal Data to be protected, and shall regularly review and update the technical and organisational measures implemented to keep the Personal Data collected under or in connection with the Agreement secure and confidential in order to demonstrate that the processing of the Personal Data is performed in accordance with the Data Protection Legislation;

3.1.5 take reasonable steps to ensure the reliability of all personnel who have access to Personal Data and ensure that only personnel who require access to the Personal Data are given access (and only to the extent necessary) and that such personnel: (i) are informed of the confidential nature of the Personal Data; (ii) have received appropriate training on protecting Personal Data; and (iii) are bound by contractual or statutory confidentiality obligations in relation to the Personal Data, and ensure that any such access is revoked once no longer required;

3.1.6 promptly notify the Data Controller if it receives a request pertaining to the exercise of a Data Subject right pursuant to the Data Protection Legislation, including without limitation, subject access rights, rights to rectification, restriction of processing, data portability, the right to object to processing and automated decision-making. The Data Processor shall not respond to a Data Subject request without the Data Controller's prior written instruction.

3.1.7 without undue delay upon discovery, notify the Data Controller of any actual or suspected Breach of this Schedule including a Breach of security leading to the accidental or unlawful

destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise processed ("Personal Data Breach").

3.1.8 immediately provide such cooperation, assistance and information to the Data Controller, at the Data Controller's reasonable costs, as may be required to allow the Data Controller to comply with: (a) the completion of any data protection impact assessment as reasonably required from time to time pursuant to the Data Protection Legislation; (b) the data protection by design and data protection by default principles under the Data Protection Legislation; (c) the rights of Data Subjects pursuant to the Data Protection Legislation, including without limitation, subject access rights, rights to rectification, restriction of processing, data portability, the right to object to processing and automated decision-making; (d) notices served by any supervisory authority for data protection purposes, such as the Information Commissioner's Office in the UK; and (e) any other notification and the Data Controller's or the Controller's (as applicable) other obligations set out in the Data Protection Legislation;

3.1.9 at the Data Controller's reasonable costs, allow representatives of the Data Controller to audit its compliance with the requirements of this Schedule on reasonable notice, and/or on request, to provide evidence of its compliance with such requirements;

3.1.10 transfer Personal Data from the European Economic Area (EEA) to outside the EEA, the European Union (EU) or the UK (to the extent that the UK is no longer in the EEA or the EU) only on the basis that the Data Processor shall, and where applicable shall procure that its subcontractor shall, prior to any such transfer: (i) ensure there are in place appropriate safeguards to protect the Personal Data including (without limitation), ensuring there is in place with the Data Controller such further documentation as may be necessary for the transfers to be lawful; (ii) ensure there are in place enforceable Data Subject rights and effective legal remedies for Data Subjects as required by the Data Protection Legislation; and (iii) comply with any reasonable written instructions relating to the same from Data Controller from time to time

3.1.11 for users in the EU, not engage a sub-processor without prior specific or general authorisation of the Data Controller. In the case of general written authorisation, the Data Processor shall inform the Data Controller of any intended changes concerning the addition or replacement of other Data Processors, thereby giving the relevant Data Controller the opportunity to object to such changes. If no objection is received within 10 working days of the Data Controller being notified of any potential change then the sub processor is considered authorised. If the Data Controller rejects any reasonable change proposed by WIC, then WIC shall be entitled to terminate this Agreement and provision of its' services. Existing sub-processors are deemed to be authorized and listed in Annex 2. The Data Controller shall use only sub-processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of the Data Protection Legislation and ensure the protection of the rights of the Data Subjects. Processing by a Data Processor shall be governed by a contract or other legal instrument governed by English law or the law of an EU Member State, that is binding on the Data Processor with regard to the Controller and that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of Personal Data and categories of Data Subjects and the obligations and rights of the Controller and shall contain terms not less protective that those in this Agreement, and

3.1.12 not later than 180 after the end of the Agreement, or if instructed earlier upon the request of the Controller as soon as reasonably practicable, permanently delete from its information technology systems all copies of Personal Data in its possession.

ANNEX 1: DETAILS OF DATA PROCESSING

(a) Subject matter: The subject matter of the data processing under this Data Protection Agreement is the provision of an online system (pc, mobile and tablet) to engage and understand staff better to deliver healthier organisations

(b) Duration of processing: WIC will process data only for the duration of the Agreement, unless instructed otherwise by UK law or otherwise agreed in writing.

(c) Nature and Purpose of processing: Onboarding of employees, hosting surveys, responses, feedback responses; management reporting

(d) Categories of data being processed:

(i) Emails, user names and passwords, job roles, mobile phone numbers

(ii) User created content (feedback, conversations, survey responses)

(e) Categories of data subjects:

(i) Employees and representatives of the Data Controller

(ii) Other stakeholders, persons or entities the Data Controller may choose from time to time to seek feedback, views or input from using the WIC platform.

ANNEX 2: LIST OF CURRENT SUB-PROCESSORS

Amazon Web Services (AWS): Security, hosting, data storage and email delivery

CloudFlare

ANNEX 3: STANDARD CONTRACTUAL CLAUSES

STANDARD CONTRACTUAL CLAUSES (PROCESSORS)

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection both parties have agreed on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

Clause 1: Definitions

For the purposes of the Clauses:

(a) 'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject' and 'supervisory authority' shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (1);

(b) 'the data exporter' means the WorkInConfidence client (controller) who transfers the personal data;

(c) 'the data importer' means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and

the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

(d) 'the sub-processor' means any processor engaged by the data importer or by any other sub-processor of the data importer who agrees to receive from the data importer or from any other sub-processor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

(e) 'the applicable data protection law' means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

(f) 'technical and organisational security measures' means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2: Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

Clause 3: Third-party beneficiary clause

The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

The data subject can enforce against the sub-processor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the sub-processor shall be limited to its own processing operations under the Clauses.

The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4: Obligations of the data exporter

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law

(and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b) that it has instructed and throughout the duration of the personal data-processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

(g) to forward any notification received from the data importer or any sub-processor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for sub-processing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of sub-processing, the processing activity is carried out in accordance with Clause 11 by a sub-processor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

(j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5: Obligations of the data importer

The data importer agrees and warrants:

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data

exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;

(d) that it will promptly notify the data exporter about:

(i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation;

(ii) any accidental or unauthorised access; and

(iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f) at the request of the data exporter to submit its data-processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for sub-processing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(h) that, in the event of sub-processing, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing services by the sub-processor will be carried out in accordance with Clause 11;

(j) To send promptly a copy of any sub-processor agreement it concludes under the Clauses to the data exporter.

Clause 6: Liability

The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or sub-processor is entitled to receive compensation from the data exporter for the damage suffered.

If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his sub-processor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity.

The data importer may not rely on a breach by a sub-processor of its obligations in order to avoid its own liabilities.

If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the sub-processor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the sub-processor agrees that the data subject may issue a claim against the data sub-processor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the sub-processor shall be limited to its own processing operations under the Clauses.

Clause 7: Mediation and jurisdiction

The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

(a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

(b) to refer the dispute to the courts in the Member State in which the data exporter is established.

The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8: Cooperation with supervisory authorities

The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any sub-processor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any sub-processor preventing the conduct of an audit of the data importer, or any sub-processor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5(b).

Clause 9: Governing law

The Clauses shall be governed by the law of the Member State in which the data exporter is established.

Clause 10: Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11: Sub-processing

The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the sub-processor which imposes the same obligations on the sub-processor as are imposed on the data importer under the Clauses. Where the sub-processor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the sub-processor's obligations under such agreement.

The prior written contract between the data importer and the sub-processor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the sub-processor shall be limited to its own processing operations under the Clauses.

The provisions relating to data protection aspects for sub-processing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established namely

The data exporter shall keep a list of sub-processing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5(j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12: Obligation after the termination of personal data-processing services

The parties agree that on the termination of the provision of data-processing services, the data importer shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

The data importer warrants that upon request of the data exporter and/or of the supervisory authority, it will submit its data-processing facilities for an audit of the measures referred to in paragraph 1.

A signed copy is available for the Data Exporter on request to WorkInConfidence.

Appendix 1 to the Standard Contractual Clauses

The Member States of any Data Controller may specify, according to their national procedures, any additional necessary information to be contained in this Appendix

Data exporter: The relevant client of WorkInConfidence Limited.

The data exporter is (please specify briefly your activities relevant to the transfer):

See Annex 1 of the Data Processing Agreement

Data importer: The data importer is See Annex 1 of the Data Processing Agreement

Data subjects

The personal data transferred concern the following categories of data subjects: See Annex 1 of the Data Processing Agreement

Categories of data

The personal data transferred concern the following categories of data (please specify): See Annex 1 of the Data Processing Agreement

Special categories of data (if appropriate)

Special category data is not expected to be uploaded to the system but may be contained in feedback response, communications etc.

Processing operations

The personal data transferred will be subject to the following basic processing activities (please specify):

See Annex 1 of the Data Processing Agreement A signed copy is available for the Data Exporter on request to WorkInConfidence.

DATA EXPORTER: WorkInConfidence Client

DATA IMPORTER: Name: WorkInConfidence Limited

Appendix 2

to the Standard Contractual Clauses

This Appendix forms part of the Clauses and where possible should be completed and signed by the parties.

Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c).

All aspects of data security are included in both employee and contractor contracts

Data transferred between the client and server is encrypted using SSL

All companies have their information and conversations held in separate databases

All passwords are salted and hashed

The system insists that users select strong passwords

Databases are regularly backed up

Systems are in place to prevent intrusion and logs are automatically scanned for anomalies.