Clear Links

Data Processor Agreement

Contents

PARTIES

(1) Clear Links Support Limited incorporated and registered in England and Wales with company number 05734428 whose registered office is at The Portergate Building, 257 Ecclesall Road, Sheffield, S11 8NX (the **"Company"**); and

(2) You (the **"Worker"**).

BACKGROUND

(A) The Company and the Worker entered into the Terms of Engagement (**Terms of Engagement**) that may require the Worker to process Personal Data on behalf of the Company.

(B) This Personal Data Processing Agreement (**Agreement**) sets out the additional terms, requirements and conditions on which the Worker will process Personal Data when providing services under the Terms of Engagement. This Agreement contains the mandatory clauses required by Article 28(3) of the General Data Protection Regulation *((EU) 2016/679)* for contracts between controllers and processors.

AGREED TERMS

1. Definitions and interpretation

The following definitions and rules of interpretation apply in this Agreement.

1.1 Definitions:

Authorised Persons:	the persons or categories of persons that the Company authorises to give the Worker personal data processing instructions as identified in Annex A.
Business Purposes:	the services described in the Terms of Engagement or any other purpose specifically identified in Annex A.
Business Day:	a day other than a Saturday or Sunday or public holiday in England when banks in London are open for business.
Data Subject:	an individual who is the subject of Personal Data.
Personal Data:	means any information relating to an identified or identifiable natural person that is processed by the Worker as a result of, or in connection with, the provision of the services under the Terms of Engagement; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, 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, processes and process:	either any activity that involves the use of Personal Data or as the Data Protection Legislation may otherwise define processing, processes or process. It includes 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. Processing also includes transferring Personal Data to third parties.

Data Protection Legislation:	all applicable privacy and data protection laws including the General Data Protection Regulation *((EU) 2016/679)* and any applicable national implementing laws, regulations and secondary legislation in England and Wales relating to the processing of Personal Data and the privacy of electronic communications, as amended, replaced or updated from time to time, including the Privacy and Electronic Communications Directive (*2002/58/EC*) and the Privacy and Electronic Communications (EC Directive) Regulations 2003 (*SI 2003/2426*).
Personal Data Breach:	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.
Standard Contractual Clauses (SCC):	the European Commission's Standard Contractual Clauses for the transfer of Personal Data from the European Union to processors established in third countries (controller-to-processor transfers), as set out in the Annex to Commission Decision 2010/87/EU.

1.2 This Agreement is subject to the terms of the Terms of Engagement and is incorporated into the Terms of Engagement. Interpretations and defined terms set forth in the Terms of Engagement apply to the interpretation of this Agreement.

1.3 The Annexes form part of this Agreement and will have effect as if set out in full in the body of this Agreement. Any reference to this Agreement includes the Annexes.

1.4 A reference to writing or written includes faxes and email.

1.5 In the case of conflict or ambiguity between:

1.5.1 any provision contained in the body of this Agreement and any provision contained in the Annexes,

1.5.2 the provision in the body of this Agreement will prevail;

1.5.3 the terms of any accompanying invoice or other documents annexed to this Agreement and any provision contained in the Annexes, the provision contained in the Annexes will prevail;

1.5.4 any of the provisions of this Agreement and the provisions of the Terms of Engagement, the provisions of this Agreement will prevail; and

1.5.5 any of the provisions of this Agreement and any executed SCC, the provisions of the executed SCC will prevail.

2. Personal data types and processing purposes

2.1 The Company and the Worker acknowledge that for the purpose of the Data Protection Legislation, the Company is the controller and the Worker is the processor.

2.2 The Company retains control of the Personal Data and remains responsible for its compliance obligations under the applicable Data Protection Legislation, including providing any required notices and obtaining any required consents, and for the processing instructions it gives to the Worker.

2.3 Annex A describes the subject matter, duration, nature and purpose of processing and the Personal Data categories and Data Subject types in respect of which the Worker may process to fulfil the Business Purposes of the Terms of Engagement.

3. Worker's obligations

3.1 The Worker will only process the Personal Data to the extent, and in such a manner, as is necessary for the Business Purposes in accordance with the Company's written instructions from the Data Protection Officer. The Worker will not process the Personal Data for any other purpose or in a way that does not comply with this Agreement or the Data Protection Legislation. The Worker must promptly notify the Company if, in its opinion, the Company's instruction would not comply with the Data Protection Legislation.

3.2 The Worker must promptly comply with any Company request or instruction from the Data Protection Officer requiring the Worker to amend, transfer, delete or otherwise process the Personal Data, or to stop, mitigate or remedy any unauthorised processing.

3.3 The Worker will maintain the confidentiality of all Personal Data and will not disclose Personal Data to third parties unless the Company or this Agreement specifically authorises the disclosure, or as required by law. If a law, court, regulator or supervisory authority requires the Worker to process or disclose Personal Data, the Worker must first inform the Company of the legal or regulatory requirement and give the Company an opportunity to object or challenge the requirement, unless the law prohibits such notice.

3.4 The Worker will reasonably assist the Company with meeting the Company's compliance obligations under the Data Protection Legislation, taking into account the nature of the Worker's processing and the information available to the Worker, including in relation to Data Subject rights, data protection impact assessments and reporting to and consulting with supervisory authorities under the Data Protection Legislation.

3.5 The Worker must promptly notify the Company of any changes to Data Protection Legislation that may adversely affect the Worker's performance of the Terms of Engagement.

4. Security

4.1 The Worker must at all times implement appropriate technical and organisational measures against unauthorised or unlawful processing, access, disclosure, copying, modification, storage, reproduction, display or distribution of Personal Data, and against accidental or unlawful loss, destruction, alteration, disclosure or damage of Personal Data including, but not limited to, the security measures set out in Annex B. The Worker must document those measures in writing and periodically review them to ensure they remain current and complete, at least annually.

4.2 The Worker must implement such measures to ensure a level of security appropriate to the risk involved, including as appropriate:

4.2.1 the pseudonymisation and encryption of personal data;

4.2.2 the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

4.2.3 the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; and

4.2.4 a process for regularly testing, assessing and evaluating the effectiveness of security measures.

5. Personal Data Breach

5.1 The Worker will promptly and without undue delay notify the Company if any Personal Data is lost or destroyed or becomes damaged, corrupted, or unusable. The Worker will restore such Personal Data at its own expense.

5.2 The Worker will immediately and without undue delay notify the Company if it becomes aware of:

5.2.1 any accidental, unauthorised or unlawful processing of the Personal Data; or

5.2.2 any Personal Data Breach.

5.3 Where the Worker becomes aware of 5.2.1 and/or 5.2.2 above, it shall, without undue delay, also provide the Company with the following information:

5.3.1 description of the nature of 5.2.1 and/or 5.2.2, including the categories and approximate number of both Data Subjects and Personal Data records concerned;

5.3.2 the likely consequences; and

5.3.3 description of the measures taken, or proposed to be taken to address 5.2.1 and/or 5.2.2, including measures to mitigate its possible adverse effects.

5.4 Immediately following any unauthorised or unlawful Personal Data processing or Personal Data Breach, the parties will co-ordinate with each other to investigate the matter. The Worker will reasonably co-operate with the Company in the Company's handling of the matter, including:

5.4.1 assisting with any investigation;

5.4.2 providing the Company with physical access to any facilities and operations affected;

5.4.3 making available all relevant records, logs, files, data reporting and other materials required to comply with all Data Protection Legislation or as otherwise reasonably required by the Company; and

5.4.4 taking reasonable and prompt steps to mitigate the effects and to minimise any damage resulting from the Personal Data Breach or unlawful Personal Data processing.

5.5 The Worker will not inform any third party of any Personal Data Breach without first obtaining the Company's prior written consent, except when required to do so by law.

5.6 The Worker agrees that the Company has the sole right to determine:

5.6.1 whether to provide notice of the Personal Data Breach to any Data Subjects, supervisory authorities, regulators, law enforcement agencies or others, as required by law or regulation or in the Company's discretion, including the contents and delivery method of the notice; and

5.6.2 whether to offer any type of remedy to affected Data Subjects, including the nature and extent of such remedy.

5.7 The Worker will cover all reasonable expenses associated with the performance of the obligations under clause 5.2 and clause 5.4 unless the matter arose from the Company's specific instructions, negligence, wilful default or breach of this Agreement, in which case the Company will cover all reasonable expenses.

5.8 The Worker will also reimburse the Company for actual reasonable expenses that the Company incurs when responding to a Personal Data Breach to the extent that the Worker caused such a Personal Data Breach, including all costs of notice and any remedy as set out in clause 5.6.

6. Cross-border transfers of personal data

6.1 The Worker must not transfer or otherwise process Personal Data outside the European Economic Area (**EEA**) without obtaining the Company's prior written consent.

6.2 Where such consent is granted, that consent will be subject to the Worker agreeing in writing to only process, or permit the processing, of Personal Data outside the EEA under specific conditions that will be notified to the Worker at the time of consent in order to ensure that all requirements of the Data Protection Legislation are complied with.

6.3 If any Personal Data transfer between the Company and the Worker requires execution of SCC in order to comply with the Data Protection Legislation (where the Company is the entity exporting Personal Data to the Worker outside the EEA), the parties will complete all relevant details in, and execute, an SCC, and take all other actions required to legitimise the transfer.

7. Subcontractors

The Worker may not authorise any third party or subcontractor to process the Personal Data.

8. Complaints, data subject requests and third party rights

8.1 The Worker must, at no additional cost, take such technical and organisational measures as may be appropriate, and promptly provide such information to the Company as the Company may reasonably require, to enable the Company to comply with:

8.1.1 the rights of Data Subjects under the Data Protection Legislation, including subject access rights, the rights to rectify and erase personal data, object to the processing and automated processing of personal data, and restrict the processing of personal data; and

8.1.2 information or assessment notices served on the Company by any supervisory authority under the Data Protection Legislation.

8.2 The Worker must notify the Company immediately if it receives any complaint, notice or communication that relates directly or indirectly to the processing of the Personal Data or to either party's compliance with the Data Protection Legislation.

8.3 The Worker must notify the Company within 3 Business Days if it receives a request from a Data Subject for access to their Personal Data or to exercise any of their related rights under the Data Protection Legislation.

8.4 The Worker will give the Company its full co-operation and assistance in responding to any complaint, notice, communication or Data Subject request.

8.5 The Worker must not disclose the Personal Data to any Data Subject or to a third party other than at the Company's request or instruction, as provided for in this Agreement or as required by law.

9. Term and terminations

9.1 This Agreement will remain in full force and effect so long as:

9.1.1 the Terms of Engagement remains in effect, or

9.1.2 the Worker retains any Personal Data related to the Terms of Engagement in its possession or control (**Term**).

9.2 Any provision of this Agreement that expressly or by implication should come into or continue in force on or after termination of the Terms of Engagement in order to protect Personal Data will remain in full force and effect.

9.3 The Worker's failure to comply with the terms of this Agreement is a material breach of the Terms of Engagement. In such event, the Company may terminate the Terms of Engagement effective immediately on written notice to the Worker without further liability or obligation.

9.4 If a change in any Data Protection Legislation prevents either party from fulfilling all or part of its Terms of Engagement obligations, the parties will suspend the processing of Personal Data until that processing complies with the new requirements. If the parties are unable to bring the Personal Data processing into compliance with the Data Protection Legislation within 20 Business Days, they may terminate the Terms of Engagement on written notice to the other party.

10. Data return and destruction

10.1 At the Company's request, the Worker will give the Company a copy of or access to all or part of the Company's Personal Data in its possession or control in the format and on the media reasonably specified by the Company.

10.2 Within 7 Business Days of the termination of Terms of Engagement for any reason or expiry of its term, the Worker will securely delete or destroy or, if directed in writing by the Company, return and not retain, all or any Personal Data related to this Agreement in its possession or control.

10.3 If any law, regulation, or government or regulatory body requires the Worker to retain any documents or materials that the Worker would otherwise be required to return or destroy, it will notify the Company in writing of that retention requirement, giving details of the documents or materials that it must retain, the legal basis for retention, and establishing a specific timeline for destruction once the retention requirement ends.

10.4 If requested to do so by the Company, the Worker will certify in writing that it has destroyed the Personal Data within the time scales specified in clause 10.2 above.

11. Records

11.1 The Worker will keep detailed, accurate and up-to-date written records regarding any processing of Personal Data it carries out for the Company, including but not limited to, the access, control and security of the Personal Data, approved subcontractors and affiliates, the processing purposes, categories of processing, any transfers of personal data to a third country and related safeguards, and a general description of the technical and organisational security measures referred to in clause 4.1 (**Records**).

11.2 The Worker will ensure that the Records are sufficient to enable the Company to verify the Worker's compliance with its obligations under this Agreement and the Worker will provide the Company with copies of the Records upon request.

11.3 The Company and the Worker must review the information listed in the Annexes to this Agreement once a year to confirm its current accuracy and update it when required to reflect current practices.

12. Audit

12.1 The Worker will permit the Company and its third-party representatives to audit the Worker's compliance with its Agreement obligations, on at least 5 Business Days' notice, during the Term. The Worker will give the Company and its third-party representatives all necessary assistance to conduct such audits. The assistance may include, but is not limited to:

12.1.1 physical access to, remote electronic access to, and copies of the Records and any other information held at the Worker's premises or on systems storing Personal Data;

12.1.2 access to and meetings with any of the Worker's personnel reasonably necessary to provide all explanations and perform the audit effectively; and

12.1.3 inspection of all Records and the infrastructure, electronic data or systems, facilities, equipment or application software used to store, process or transport Personal Data.

12.2 The notice requirements in clause 12.1 will not apply if the Company reasonably believes that a Personal Data Breach occurred or is occurring, or the Worker is in breach of any of its obligations under this Agreement or any Data Protection Legislation.

12.3 If a Personal Data Breach occurs or is occurring, or the Worker becomes aware of a breach of any of its obligations under this Agreement or any Data Protection Legislation, the Worker will:

12.3.1 within 1 Business Day of the triggering event, conduct its own audit to determine the cause;

12.3.2 produce a written report that includes detailed plans to remedy any deficiencies identified by the audit;

12.3.3 provide the Company with a copy of the written audit report; and

12.3.4 remedy any deficiencies identified by the audit within 5 Business Days.

12.4 At the Company's written request, the Worker will:

12.4.1 conduct an information security audit before it first begins processing any Personal Data and repeat that audit on an annual basis;

12.4.2 produce a written report that includes detailed plans to remedy any security deficiencies identified by the audit;

12.4.3 provide the Company with a copy of the written audit report; and

12.4.4 remedy any deficiencies identified by the audit within 5 Business Days.

13. Warranties

13.1 The Worker warrants and represents that:

13.1.1 it and any other person or persons accessing Personal Data on its behalf is informed of the confidential nature of the Personal Data and is bound by confidentiality obligations and use restrictions in respect of the Personal Data;

13.1.2 it and any other person or persons accessing Personal Data on its behalf are reliable and trustworthy and have received the required training on the Data Protection Legislation relating to the Personal Data;

13.1.3 it and anyone operating on its behalf will process the Personal Data in compliance with this Agreement, the Data Protection Legislation and other laws, enactments, regulations, orders, standards and other similar instruments;

13.1.4 it has no reason to believe that the Data Protection Legislation prevents it from providing any of the Terms of Engagement's contracted services; and

13.1.5 considering the current technology environment and implementation costs, it will take appropriate technical and organisational measures to prevent the unauthorised or unlawful processing of Personal Data and the accidental loss or destruction of, or damage to, Personal Data, and ensure a level of security appropriate to:

13.1.5.1 the harm that might result from such unauthorised or unlawful processing or accidental loss, destruction or damage;

13.1.5.2 the nature of the Personal Data protected; and

13.1.5.3 comply with all applicable Data Protection Legislation and its information and security policies, including the security measures required in clause 4.1.

13.2 The Company warrants and represents that the Worker's expected use of the Personal Data for the Business Purposes and as specifically instructed by the Company will comply with the Data Protection Legislation.

14. Indemnification

14.1 The Worker agrees to indemnify, keep indemnified and defend at its own expense the Company against all costs, claims, damages or expenses incurred by the Company or for which the Company may become liable due to any failure by the Worker or any other person or persons accessing Personal Data on its behalf, to comply with any of its obligations under this Agreement or the Data Protection Legislation.

14.2 Any limitation of liability set forth in the Terms of Engagement will not apply to this Agreement's indemnity or reimbursement obligations.

15. Notices

15.1 Any notice or other communication given to a party under or in connection with this agreement shall be in writing and shall be:

15.1.1 delivered by hand or by pre-paid first-class post or other next working day delivery service at its registered office (if a company) or its principal place of business (in any other case); or

15.1.2 sent by email by the Worker to the address specified by Clear Links in Annex A: Authorised Persons or by the Company to the address specificed by the Worker in their Support Worker Application Form or subsequent updates.

15.2 Any notice or communication shall be deemed to have been received:

15.2.1 if delivered by hand, on signature of a delivery receipt;

15.2.2 if sent by pre-paid first-class post or other next working day delivery service, at 9.00 am on the second Business Day after posting or at the time recorded by the delivery service; and

15.2.3 if sent by email, at the time of transmission, or, if this time falls outside business hours in the place of receipt, when business hours resume. In this clause, business hours means 9.00am to 5.00pm Monday to Friday on a day that is not a public holiday in the place of receipt.

15.3 This clause does not apply to the service of any proceedings or other documents in any legal action or, where applicable, any arbitration or other method of dispute resolution.

ANNEX A

Personal Data Processing Purposes and Details

Subject matter of processing: The subject matter of the processing is the provision of non-medical help support to students.

Duration of Processing: The duration of the processing is the duration of the assignment - the period during which you render services to the Student as specified in an Assignment Confirmation.

Nature and purpose of Processing: The nature and purpose of the data processing is to arrange, deliver and monitor the provision of non-medical help support to the student that you have been matched with.

Personal Data Categories: The categories of personal data you will process are the name, contact details (phone number and email address), information about the university course and information about the support delivered to the student you are matched with. The special category personal data you may process is information about the student's disability.

Data Subject Types: The data subject is a student requiring the services of you during an Assignment.

Authorised Persons: Clear Links Support Data Protection Officer (DPO). Currently Dexter Johnstone, dexter.johnstone@clear-links.co.uk, 0114 278 6866.

ANNEX B

Security measures. A general description of the security measures required of the Worker.

- The Worker must ensure that any electronic device which is used to store personal data is passworded/passcoded.
- The Worker must not store personal data on publicly accessible computers. Personal data must only be accessible to the Worker.
- The Worker must keep any records of support which contain personal data which could be used to identify the student securely.
- The Worker must keep any hard copy records (e.g. hand-written notes, printed electronic data) in a safe and secure place.
- The Worker must consider ways of anonymising the records and record as little personal data as possible within the record.
- The Worker must ensure that personal data in any format is not left in any public place.
- The Worker must not use a shared email account for correspondence about their support work.
- The Worker must be the only person who has access to the email account used for correspondence about their support work.
- The Worker must include only the minimum personal data required within the email.
- The Worker must not email a message to more than one student at a time or copy in other people to emails about students.
- The Worker must not forward emails that contain any personal data about students to 3rd parties.
- The Worker must only include information about one student in an email.
- The Worker must ensure that when making and receiving calls no one can overhear personal information.
- The Worker must not mention the student's personal data or circumstances in phone messages. The Worker must be aware that messages left on landline numbers may be accessed by other people.
- The Worker must ensure that personal data is kept up to date.
- The Worker must not share personal data with any other party, other than Clear Links. Any such requests must be referred to requests to our Clear Links Support Data Protection Officer.
- The Worker must permanently delete or destroy personal data once their assignment with a student has ended.
- The Worker must ensure that destruction is carried out in a secure manner. Hard copy documents must be shredded. Data stored electronically must be deleted and data emptied from the 'recycle bin' or 'deleted items' folder.
- The Worker must ensure that personal data is deleted within 7 working days from the end date of the assignment.
- The Worker must not transfer personal data outside the European Economic Area.