

DATA PROCESSING CONTRACT

(A) University of Salford (UoS) acts as a Data Controller.

(B) UoS wishes to contract certain Services, which imply the processing of personal data, to the Data Processor.

(C) The Parties seek to implement a data processing agreement that complies with the requirements of the current legal framework in relation to data processing and with the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

(D) The Parties wish to lay down their rights and obligations.

IT IS AGREED AS FOLLOWS:

1. DEFINITIONS, INTERPRETATION AND CONSIDERATION

1.1 The following words and phrases used in this Agreement and the Schedules shall have the following meanings except where the context otherwise requires:

“Applicable Law”	means the laws of England (and any EU regulations from time-to-time applicable (i) whilst the United Kingdom remains a member of the European Union or (ii) subsequently under the terms of the European Union (Withdrawal Bill));
“Business Day(s)”	means a day other than a Saturday, Sunday or English bank holiday;
“Controller”	has the meaning of ‘controller’ set out in Article 4 of GDPR for the purpose of this Agreement is UoS;
“Data Loss Event”	means any event that results, or may result, in unauthorised access to Personal Data held by UoS hereunder, and/or actual or potential loss and/or destruction of Personal Data, including any Personal Data Breach;
“Data Protection Legislation”	means all applicable privacy or data protection laws and regulations (as amended, consolidated or re-enacted from time-to-time) which relate to the protection of individuals with regards to the processing of personal data to which a party is subject, including the Data Protection Act 2018 and GDPR and the Privacy and Electronic Communications (EC Directive) Regulations 2003, for as long as any of the above are incorporated into Applicable Law together with any guidance and/or codes of practice issued from time-to-time by the ICO;
"Data Subject"	means an individual who is the subject of the Personal Data;
“Data Subject Access Request”	means a request made by, or on behalf of, a Data Subject in accordance with rights granted pursuant to the Data Protection Legislation to access their Personal Data;
“Deletion”	means to remove or obliterate Personal Data such that it

cannot be recovered or reconstructed and this meaning applies to “Destruction;”

“GDPR”	means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and repealing Directive 95/46/EC (General Data Protection Regulation) OJ L 119/1, 4.5.2016;
“ICO”	means the Information Commissioner’s Office;
“Original Agreement”	the terms and conditions currently in force between the parties for the Services;
“Personal Data”	has the meaning set out in Article 4 of GDPR and means any personal data and sensitive personal data, (as defined by the Data Protection Act 2018), and includes (but is not limited to) special categories of personal data which reveal racial or ethnic origin, political opinions, religious or philosophical beliefs, sex, sexual orientation, trade union membership or the processing of genetic or biometric data, for the purpose of uniquely identifying a natural person or which the Processor might encounter whilst conducting the Services and the Data specified in Schedule 1;
“Processing and Process”	have the meaning set out in Article 4 of GDPR and means any operation or set of operations which is performed upon Personal Data, whether or not by automatic means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction or data or as set out in Part 1, section 3(4) of the Data Protection Act 2018;
“Processor”	means any person (other than an employee of UoS) who processes the data on behalf of UoS;
“Services”	means the outline services above and more particularised in the Original Agreement entered into by UoS;
“Technical and Organisational Security Measures”	<u>means those</u> measures including but not limited to those specified in Schedule 1 aimed at protecting the Personal Data against accidental or unlawful destruction, theft 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.

1.2 The headings in this Agreement are inserted for convenience only and shall not affect its construction or interpretation. References in this Agreement to clauses, schedules and appendices are, unless otherwise stated, references to the clauses of and schedules to this Agreement.

1.3 The Processor accepts the obligations in this Agreement in consideration of UoS continuing to use its Services.

1.4 Notwithstanding anything to the contrary set out in the Original Agreement, to the extent that there is any duplication or conflict between definitions or clauses used in the Original Agreement and this Agreement, the definitions and clauses set out in this Agreement will vary the Original Agreement, apply and take precedence in respect of Personal Data and liability for breaches for Data Protection Legislation. In all other respects the Original Agreement as amended by this Agreement shall continue in full force and effect.

2. Processing of Company Personal Data

2.1 Processor shall:

2.1.1 comply with all applicable Data Protection Legislation in the Processing of UoS Personal Data; and

2.1.2 not Process UoS Personal Data other than on the UoS's documented instructions.

2.2 The Company instructs Processor to process Company Personal Data.

3. Processor Personnel

Processor shall take reasonable steps to ensure the reliability of any employee, agent or contractor who may have access to UoS Personal Data, ensuring in each case that access is strictly limited to those individuals who need to know / access the relevant UoS Personal Data, as strictly necessary for the purposes of the Principal Agreement, and to comply with Applicable Laws in the context of that individual's duties to the Contracted Processor, ensuring that all such individuals are subject to confidentiality undertakings or professional or statutory obligations of confidentiality.

Processor shall ensure that all employees, agents or contractors have undertaken training on Data Protection Laws relating to handling Personal Data and how it applies to their particular duties at the commencement of their employment and prior to being given access to files or databases containing personal data; and

(c) are aware both of Processor's duties and their personal duties and obligations under Data Protection Laws and this Agreement;

(d) participate in regular refresher training particularly when there are legislative changes and otherwise, at least annually.

4. Security

4.1 Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Processor shall in relation to UoS Personal Data implement appropriate technical and organizational measures to ensure a level of security appropriate to that risk, including, as appropriate, the measures referred to in Article 32(1) of the GDPR.

4.2 In assessing the appropriate level of security, Processor shall take account in particular of the risks that are presented by Processing, in particular from a Personal Data Breach.

5. Subprocessing

5.1 Processor shall not appoint (or disclose any UoS Personal Data to) any Subprocessor unless required or authorized by the Company.

6. Data Subject Rights

6.1 Taking into account the nature of the Processing, Processor shall assist UoS by implementing appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Company obligations, as reasonably understood by Company, to respond to requests to exercise Data Subject rights under the Data Protection Laws.

6.2 Processor shall:

6.2.1 promptly notify UoS if it receives a request from a Data Subject under any Data Protection Law in respect of UoS Personal Data; and

6.2.2 ensure that it does not respond to that request except on the documented instructions of UoS or as required by Applicable Laws to which the Processor is subject, in which case Processor shall to the extent permitted by Applicable Laws inform UoS of that legal requirement before the Processor responds to the request.

7. Personal Data Breach

7.1 Processor shall notify UoS without undue delay upon Processor becoming aware of a Personal Data Breach affecting UoS Personal Data, providing UoS with sufficient information to allow UoS to meet any obligations to report or inform Data Subjects of the Personal Data Breach under the Data Protection Laws.

7.2 Processor shall co-operate with UoS and take reasonable commercial steps as are directed by UoS to assist in the investigation, mitigation and remediation of each such Personal Data Breach.

8. Data Protection Impact Assessment and Prior Consultation

Processor shall provide reasonable assistance to UoS with any data protection impact assessments, and prior consultations with Supervising Authorities or other competent data privacy authorities, which UoS reasonably considers to be required by article 35 or 36 of the GDPR or equivalent provisions of any other Data Protection Law, in each case solely in relation to Processing of UoS Personal Data by, and taking into account the nature of the Processing and information available to, the Processor.

9. Deletion or return of Company Personal Data

9.1 Subject to this section 9 Processor shall promptly and in any event within

10 business days of the date of cessation of any Services involving the Processing of UoS Personal Data (the "Cessation Date"), delete and procure the deletion of all copies of those UoS Personal Data.

10. Audit rights

10.1 Subject to this section 10, Processor shall make available to UoS on request all information necessary to demonstrate compliance with this Agreement, and shall allow for and contribute to

audits, including inspections, by UoS or an auditor mandated by UoS in relation to the Processing of UoS Personal Data by the Contracted Processors.

10.2 Information and audit rights of UoS only arise under section 10.1 to the extent that the Agreement does not otherwise give them information and audit rights meeting the relevant requirements of Data Protection Law.

11. Data Transfer

11.1 The Processor may not transfer or authorize the transfer of Data to countries outside the EU and/or the European Economic Area (EEA) without the prior written consent of UoS. If personal data processed under this Agreement is transferred from a country within the European Economic Area to a country outside the European Economic Area, the Parties shall ensure that the personal data are adequately protected. To achieve this, the Parties shall, unless agreed otherwise, rely on EU approved standard contractual clauses for the transfer of personal data.

12. General Terms

12.1 Confidentiality.

Each Party must keep this Agreement and information it receives about the other Party and its business in connection with this Agreement (“Confidential Information”) confidential and must not use or disclose that Confidential Information without the prior written consent of the other Party except to the extent that:

- (a) disclosure is required by law;
- (b) the relevant information is already in the public domain.

12.2 Notices.

All notices and communications given under this Agreement must be in writing and will be delivered personally, sent by post or sent by email to the address or email address set out in the heading of this Agreement at such other address as notified from time to time by the Parties changing address.

13. Governing Law and Jurisdiction

13.1 This Agreement is governed by the laws of England.

13.2 Any dispute arising in connection with this Agreement, which the Parties will not be able to resolve amicably, will be submitted to the exclusive jurisdiction of the courts of England.