Data Processing Agreement

Between
University of South Wales

and

# Service provider

Where a contract requires the Service Provider to process Personal Data, as defined under Data Protection legislation, on behalf of the University of South Wales the provisions set out in this addendum will apply.

**PLEASE READ CAREFULLY AND COMPLETE THE PARTS HIGHLIGHTED AND ENSURE THAT APPROPRIATE INFORMATION IS INCLUDED IN SCHEDULE 2.**

**IF A RESTRICTED TRANSFER WILL TAKE PLACE, SCHEDULE 3 MUST ALSO BE COMPLETED**

**IF YOU HAVE ANY QUERIES, PLEASE CONTACT** **DATAPROTECTION@SOUTHWALES.AC.UK**

Contents

[Schedule 1: Definitions and interpretation 10](#_Toc127880667)

[Schedule 2: Data Protection Particulars and Security Requirements: 15](#_Toc127880668)

[Schedule 3 17](#_Toc127880669)

[Part 1: Tables 17](#_Toc127880670)

[Part 2: Mandatory Clauses 19](#_Toc127880671)

[Alternative Part 2 Mandatory Clauses: 24](#_Toc127880672)

|  |  |
| --- | --- |
| Date this Agreement comes into force | DATE- yyyy-mm-dd |
| Date by which this Agreement should be reviewed:  | Six months after coming into force, then annually |
| Agreement owner: | Name |

1. **Parties to this Agreement**
	1. University of South Wales a body corporate established by Royal Charter and Registered Charity (Charity Number 1140312), Llantwit Road, Treforest, Pontypridd. CF37 1DL (The University)
	2. [NAME OF SERVICE PROVIDER] [DESCRIPTION, COMPANY NUMBER AND REGISTERED ADDRESS] (The Service Provider).
2. **Purpose**
	1. The University wishes to engage the Service Provider to provide services as described in the Data Protection Particulars and the Service Provider wishes to carry out those activities.
	2. This Agreement establishes the terms and conditions under which: (a) the University will provide Personal Data to the Service Provider; and (b) the Service Provider shall Process that Personal Data on behalf of the University of South Wales, [in connection with the Main Agreement].
	3. In consideration of their compliance with their respective obligations under this Agreement, the University appoints the Service Provider to process, and the Service Provider agrees to process the Personal Data for the purposes set out in Schedule 2.
3. **Terms of the Agreement**
	1. This Agreement comprises these terms and conditions and the Schedules attached hereto.
	2. For clarity, the Schedules form part of this Agreement and shall have effect as if set out in full in the body of this Agreement. Any reference to this Agreement includes the Schedules.
	3. The University of South Wales shall share the Personal Data with the Service Provider, and the Service Provider shall process that Personal Data, only in accordance with the terms of this Agreement.
4. **Term and termination**
	1. This Agreement shall commence on the date set out at the beginning of it and shall continue: (a) until terminated in accordance with its terms; or (b) until the completion of the processing activities set on in Schedule 2, and thereafter until all Personal Data has been securely deleted or returned to the University in accordance with Clause 5.2 (xv)
	2. Without prejudice to any other right or remedy available to it, the University may terminate this Agreement at any time for any reason with immediate effect by giving 28 days’ written notice.
	3. Clause 4 (Term and termination), Clause 5 (Data protection arrangements) and Clause 7 (indemnity) shall survive the termination or expiry of this Agreement, as shall any other Clause which, by its nature, is intended to survive termination or expiry.
	4. Termination or expiry of this Agreement shall not affect any rights, remedies, obligations or liabilities of the parties that have accrued up to the date of termination or expiry, including the right to claim damages in respect of any breach of the agreement which existed at or before the date of termination or expiry.
5. **Data protection**
	1. The parties agree and acknowledge that University shall be the Controller of all Personal Data Processed by the Service Provider in connection with this Agreement, and the Service Provider shall be the Processor in respect of such Personal Data. Part A of Schedule 2 sets out the scope, nature and purpose of Processing by the Service Provider, the duration of the Processing, the types of Personal Data and categories of Data Subject.

***Obligations applicable to the Service Provider***

* 1. The Service Provider shall, when Processing Personal Data in connection with this Agreement:
1. comply with all applicable provisions of the Data Protection Legislation, including the obligations imposed upon a Data Processor and not act in any way so as to cause the University to breach any of its obligations under the Data Protection Legislation;
2. act only in accordance with the University’s written instructions from time to time regarding the Processing of Personal Data pursuant to this Agreement;
3. notify the University immediately (and in any event within twenty-four (24) hours of becoming aware of the same) if it considers, in its opinion (acting reasonably) that it is required by Applicable Law to act other than in accordance with the instructions of the University, including where it believes that any of the University’s instructions under this Clause infringes any applicable Data Protection Legislation;
4. Process the Personal Data for and on behalf of the University only for the Permitted Purpose in accordance with this Agreement, including the terms of Schedule 2, Part A;
5. keep complete and accurate information and records of any Processing of Personal Data that it carries out on behalf of the University to demonstrate its compliance with this clause 5.2 and make such records available on request to the University;
6. implement and maintain appropriate technical and organisational security measures, including the encryption of personal data in transit and at rest and in accordance with the particulars set out in Schedule 2, which are sufficient to comply with at least the obligations imposed on the University by the Security Requirements and, where requested, provide to the University evidence of its compliance with such requirements;
7. take all reasonable steps, including the provision of appropriate training in data protection, information security to ensure the reliability, competence and integrity of any of the Personnel who shall have access to the Personal Data, ensure that each member of Personnel shall have entered into appropriate contractually-binding confidentiality undertakings, and all times procure compliance by those persons with such obligations of confidentiality;
8. within thirty (30) calendar days of a request from the University, allow its data processing facilities, procedures and documentation to be submitted for scrutiny, inspection or audit by the Data Controller (and/ or its representatives, including its appointed auditors) in order to ascertain compliance with the terms of this Agreement and with the Data Protection Legislation, including the requirements of Article 28 UK GDPR and provide reasonable information, assistance and co-operation to the University, including access to relevant Personnel and/ or, on the request of the University, provide the University with written evidence of its compliance with the requirements of this Agreement and with Data Protection Legislation;
9. not make (nor instruct or permit a third party to make) a Data Transfer unless it: (A) has first obtained the University’s prior written consent; (B) provides, in advance of any such Data Transfer, a Data Transfer Risk Assessment to the University; and (C) has put in place measures to ensure the University’s compliance with the Data Protection Legislation, including entering into, or procuring that such applicable sub-contractors enter into, the relevant Standard Contractual Clauses;
10. not disclose Personal Data to a third party (including a sub-contractor) in any circumstances without the University's prior written consent, save in relation to Third Party Requests where the Service Provider is prohibited by Applicable Law from notifying the University, in which case it shall use reasonable endeavours to advise the University where permitted in advance of such disclosure and in any event as soon as practicable thereafter;
11. not sub-contract the performance of any of its obligations under this Agreement without the prior written consent of the University of South Wales;
12. where in connection with this Agreement, it sub-contracts the processing of any Personal Data to a third party, (A) ensure that the arrangement with the sub-contractor is: (1) governed by a written contract imposing the same terms in relation to the processing of the Personal Data as those set out in this Agreement; and (2) where applicable, meets the requirements of Article 28(3) of the UK GDPR; and (B) be fully liable to the University of South Wales for any breach by that party in respect of its obligations to process Personal Data in accordance with this Agreement and the compliance of that subcontractor with the Data Protection Legislation;
13. notify the University promptly (and in any event within forty-eight (48) hours) following its receipt of any Data Subject Request or Regulator Correspondence and shall: (A) not disclose any Personal Data in response to any Data Subject Request or Regulator Correspondence without the University’s prior written consent; and (B) provide the University with all reasonable co-operation and assistance required by the University in relation to any such Data Subject Request, other rights available to the Data Subject or Regulator correspondence;
14. notify the University promptly (and in any event within twenty-four (24) hours) upon becoming aware of any actual or suspected, threatened or ‘near miss’ Personal Data Breach, with sufficient information to allow the University to meet any obligations under Data Protection Legislation to report or inform Data Subjects of the data breach, and: (A) implement any measures necessary to restore the security of compromised Personal Data; and (B) provide all reasonable assistance to the University to assist the University to make any notifications to the Regulator and affected Data Subjects. Any notification under this clause 5.2 (xiv) must include, (if known by the Service Provider): (a) the nature of the Personal Data Breach; (b) the categories and approximate number of Personal Data Subjects who may be affected by the Personal Data Breach; (c) the categories and approximate number of Person Data records that may be affected; (d) the likely consequences of the Personal Data Breach; and (e) any measures that the Service Provider has taken or proposes to take to address the Personal Data Breach:
15. except to the extent permitted by Applicable Law, upon the University’s request and/or on the earlier of: (A) termination or expiry of this Agreement (as applicable); and/ or (B) the date on which the Personal Data Processed in connection with this Agreement is no longer relevant to, or necessary for, the Permitted Purpose, the Service Provider shall cease Processing all such Personal Data and return and/ or permanently and securely destroy, so that it is no longer retrievable (as directed in writing by the University), all such Personal Data and all copies in its possession or control (including back-up copies); and
16. use all reasonable endeavours, in accordance with Good Industry Practice, to assist the University to comply with the obligations imposed on it by the Data Protection Legislation, including: (A) compliance with the Security Requirements; (B) obligations relating to notifications required by the Data Protection Legislation to the Regulator and/ or any relevant Data Subjects; and (C) undertaking any Data Protection Impact Assessments (and, where required by the Data Protection Legislation, consulting with the Regulator in respect of any such Data Protection Impact Assessments).

***Obligations applicable to both the University and the Service Provider***

* 1. During the term of this Agreement each party acknowledges that it has obligations under applicable Data Protection Legislation including the following (for clarity, these obligations shall be without prejudice to the obligations applicable to the Service Provider set out at Clause 5.2 above):
		1. to make due notification (where required by applicable Data Protection Legislation) to the Regulator, including in relation to its use and Processing of the Personal Data and comply at all times with the Data Protection Legislation;
		2. to ensure that all Personal Data disclosed or transferred to, or accessed by, the other party is accurate and up-to-date, as well as adequate, relevant and not excessive to enable each party to Process the Personal Data, as envisaged under this Agreement;
		3. to ensure that appropriate operational and technical measures, including encryption implemented to the appropriate Current Standard, are in place to safeguard against any unauthorised or unlawful Processing of Personal Data and against accidental loss or destruction of, or damage to, Personal Data and where requested provide to the other party evidence of its compliance with such requirement;
		4. take reasonable steps to ensure the reliability of any personnel who have access to the Personal Data;
		5. not transfer any Personal Data outside the United Kingdom except in accordance with the requirements of the Data Protection Legislation;
		6. hold the information contained in the Personal Data confidentially; and
		7. not do anything which shall damage the reputation of the other party or that party’s relationship with the Data Subjects.
	2. Each party shall comply with all applicable requirements of the Data Protection Legislation. This Agreement is in addition to, and does not relieve, remove or replace, either party's obligations under the Data Protection Legislation.
	3. Notwithstanding anything in this Agreement to the contrary, this Clause 5 (Data Protection Arrangements) shall continue in full force and effect for so long as the Service Provider Processes any Personal Data in connection with this Agreement.
1. **Freedom of Information**
	1. The Service Provider acknowledges that the University is subject to the requirements of the FOIA and the EIRs. The Service Provider shall:
		1. provide all necessary assistance and cooperation as reasonably requested by the University to enable the University to comply with its obligations under the FOIA and EIRs;
		2. transfer to the University all Requests for Information relating to this Agreement [or to the Main Agreement] that it receives as soon as practicable and in any event within 2 working days of receipt;
		3. provide the University with a copy of all Information belonging to the University requested in the Request For Information which is in its possession or control in the form that the University requires within 5 working days (or such other period as the University may reasonably specify) of the University’s request for such Information; and
		4. not respond directly to a Request For Information unless authorised in writing to do so by the University.
	2. The Service Provider acknowledges that the University may be required under the FOIA and EIRs to disclose Information (including Commercially Sensitive Information) without consulting or obtaining consent from the Service Provider. The University shall take reasonable steps to notify the Service Provider of a Request For Information (in accordance with the Secretary of State’s section 45 Code of Practice on the Discharge of the Functions of Public Authorities under Part 1 of the FOIA) to the extent that it is permissible and reasonably practical for it to do so but (notwithstanding any other provision in this Agreement) the University shall be responsible for determining in its absolute discretion whether any Commercially Sensitive Information and/or any other information is exempt from disclosure in accordance with the FOIA and/or the EIRs.
2. **Indemnity**
	1. The Service Provider hereby indemnifies the University against all costs, claims, liabilities, and expenses (including reasonable legal expenses) incurred by the University in connection with or as a result of any breach of this Agreement by the Service Provider, its staff or agents. Liability under this indemnity is unlimited.
	2. For clarity, the parties agree that any limitations on liability set out in the Main Agreement shall not apply to the indemnity set out in this Clause.
3. **Miscellaneous**
	1. No variation of this Agreement shall be effective unless it is in writing and signed by the parties (or their authorised representatives).
	2. A failure or delay by a party to exercise any right or remedy provided under this Agreement or by law shall not constitute a waiver of that or any other right or remedy, nor shall it prevent or restrict any further exercise of that or any other right or remedy. No single or partial exercise of any right or remedy provided under this agreement or by law shall prevent or restrict the further exercise of that or any other right or remedy.
	3. If any provision or part-provision of this Agreement is or becomes invalid, illegal or unenforceable, it shall be deemed modified to the minimum extent necessary to make it valid, legal and enforceable. If such modification is not possible, the relevant provision or part-provision shall be deemed deleted. Any modification to or deletion of a provision or part-provision under this Clause shall not affect the validity and enforceability of the rest of this Agreement.
	4. This Agreement constitutes the entire agreement between the parties and supersedes and extinguishes all previous agreements, promises, assurances, warranties, representations and understandings between them, whether written or oral, relating to its subject matter.
	5. Each party agrees that it shall have no remedies in respect of any statement, representation, assurance or warranty (whether made innocently or negligently) that is not set out in this Agreement.
	6. Nothing in this Agreement is intended to, or shall be deemed to, establish any partnership or joint venture between any of the parties, constitute any party the agent of another party, or authorise any party to make or enter into any commitments for or on behalf of any other party.
	7. This Agreement does not give rise to any rights under the Contracts (Rights of Third Parties) Act 1999 to enforce any term of this Agreement.
	8. This Agreement may be executed in any number of counterparts, each of which when executed shall constitute a duplicate original, but all the counterparts shall together constitute the one agreement.
	9. This agreement and any dispute or claim (including non-contractual disputes or claims) arising out of or in connection with it or its subject matter or formation shall be governed by and construed in accordance with the Laws of England and Wales, as applied in Wales.
	10. Each party irrevocably agrees that the courts of England and Wales shall have exclusive jurisdiction to settle any dispute or claim (including non-contractual disputes or claims) arising out of or in connection with this agreement or its subject matter or formation.

### Signed for and on behalf of University of South Wales

|  |  |  |
| --- | --- | --- |
| Name | Job Title | Date (yyy-mm-dd) |
|  |  |  |
|  |  |  |

### Signed for and on behalf of [INSERT NAME OF SERVICE PROVIDER]

|  |  |  |
| --- | --- | --- |
| Name | Job Title | Date (yyy-mm-dd) |
|  |  |  |
|  |  |  |

## Schedule 1: Definitions and interpretation

**Part A- Definitions**

|  |  |
| --- | --- |
| **Definition** | **Interpretation** |
| Addendum to the EU Commission Standard Contractual Clauses | means the Addendum issued under Section 119A of the Data Protection Act 2018 which replaced EU Standard Contractual Clauses for International Transfers in the UK; |
| Applicable Law | means any law, statute, subordinate legislation within the meaning of section 21(1) of the Interpretation Act 1978, bye-law, enforceable right within the meaning of section 2 of the European Communities Act 1972, regulation, order, mandatory guidance or code of practice, judgment of a relevant court of law, or directives or requirements of any regulatory body with which the Service Provider is bound to comply; |
| Commercially Sensitive Information  | means information of a commercially sensitive nature relating to the Service Provider, its intellectual property rights, or its business or which the Service Provider has indicated to the University of South Wales that, if disclosed by the University, would cause the Service Provider significant commercial disadvantage or material financial loss; |
| Confidential Information | any information, however it is conveyed, that relates to the business, affairs, developments, trade secrets, know-how, personnel and suppliers of the Service Provider, including intellectual property rights, together with all information derived from the above, and any other information clearly designated as being confidential (whether or not it is marked as “confidential”) or which ought reasonably to be considered to be confidential, including Commercially Sensitive Information; |
| Current Standard  | means the current standards for encryption recommended by the Information Commissioner’s Office, such as FIPS 140-2 (cryptographic modules, software and hardware) and FIPS 197; |
| Controller | has the meaning set out in the Data Protection Legislation; |
| Processor | has the meaning set out in the Data Protection Legislation; |
| Data Protection Impact Assessment | means an assessment of the impact of the envisaged Processing operations on the protection of Personal Data, as required by Article 35 of the UK GDPR; |
| Data Protection Legislation | means any law, statute, declaration, decree, directive, legislative enactment, order, ordinance, regulation, rule or other binding restriction (as amended, consolidated or re-enacted from time to time) which relates to the protection of individuals with regards to the Processing of Personal Data to which a party to this Agreement is subject, including: (a) the UK GDPR; (b) the EU GDPR (as applicable); (c) the Data Protection Act 2018; and (c) any and all legislation enacted, amended or replaced in the UK in respect of the protection of Personal Data; |
| Data Protection Particulars | means, in relation to the Processing under this Agreement:1. the subject matter and duration of the Processing;
2. the nature and purpose of the Processing;
3. the type of Personal Data being Processed; and
4. the categories of Data Subjects,

as set out in Schedule 2; |
| Data Subject Request | means an actual or purported subject access request or notice or complaint from (or on behalf of) a Data Subject exercising its rights under the Data Protection Legislation; |
| Data Subject | has the meaning given to it in the Data Protection Legislation; |
| Data Transfer Risk Assessment | means a risk assessment which set out details of the following:1. the Personal Data that will be transferred;
2. the Restricted Country or Countries to which the Personal Data will be transferred;
3. the means by which the Data Processor will ensure an appropriate level of protection and appropriate safeguards in respect of the Personal Data that will be transferred to a Restricted Country so as to ensure the Data Processor’s compliance with Data Protection Legislation; and
4. in providing and evaluating the risk assessment, the Data Processor shall ensure that it has regard to the Data Protection Legislation in connection with transfers of Personal Data to any Restricted Country;
 |
| Data Transfer | means transferring the Personal Data to, and/ or accessing the Personal Data from and/ or Processing the Personal Data within, a jurisdiction or territory that is a Restricted Country; |
| ElRs  | means the Environmental Information Regulations 2004 together with any guidance and/or codes of practice issued by the Information Commissioner or relevant government department in relation to such regulations;  |
| FOIA  | means the Freedom of Information Act 2000, and any subordinate legislation made under the Act from time to time, together with any guidance and/or codes of practice issued by the Regulator or relevant government department in relation to such legislation; |
| EU 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; |
| Good Industry Practice | means, at any time, the exercise of that degree of care, skill, diligence, prudence, efficiency, foresight and timeliness which would be reasonably expected at such time from a leading and expert supplier of similar services to those being carried out under this Agreement, such supplier seeking to comply with its contractual obligations in full and complying with all applicable laws (including the Data Protection Legislation); |
| Information:  | has the meaning given under section 84 of FOIA; |
| International Data Transfer Agreement | means the International Data Transfer Agreement issued under Section 119A of the Data Protection Act 2018 which replaced EU Standard Contractual Clauses for International Transfers in the UK.  |
| Permitted Purpose | means the purpose of the Processing as set out in more detail in the Data Protection Particulars; |
| Personal Data Breach | has the meaning set out in the Data Protection Legislation; |
| Personal Data | means any Personal Data (as defined in the Data Protection Legislation) processed by either Party in connection with this Agreement; |
| Personnel | means all persons engaged or employed from time to time by the Data Processor in connection with this Agreement, including employees, consultants, contractors and permitted agents; |
| Process or Processing | has the meaning set out in the Data Protection Legislation; |
| Regulator | means the UK Information Commissioner (including any successor or replacement); |
| Restricted Country | means a country, territory or jurisdiction outside of the UK which neither the EU Commission nor the UK Secretary of State has deemed to provide adequate protection in accordance with EC Directive 95/46/EC and/or Article 45(1) of the GDPR (as applicable); or the UK Adequacy Regulations made by the UK Secretary of State under Section 17A of The Data Protection Act 2018; |
| Request for Information | means a request for information or an apparent request under the Code of Practice on Access to Government Information, FOIA or the Environmental Information Regulations; |
| Security Requirements | means the requirements regarding the security of the Personal Data, as set out in the Data Protection Legislation (including, in particular, Article 5(f) of the UK GDPR and/ or the measures set out in Article 32(1) of the UK GDPR (taking due account of the matters described in Article 32(2) of the UK GDPR)) as applicable; |
| Sensitive Personal Data | which in the UK GDPR is referred to as “special categories of personal data” has the meaning set out in the Data Protection Legislation; |
| Standard Contractual Clauses | means the ICO's International Data Transfer Agreement for the transfer of personal data from the UK and/or the ICO's International Data Transfer Addendum to EU Commission Standard Contractual Clauses and/or the European Commission's Standard Contractual Clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 as set out in the Annex to Commission Implementing Decision (EU) 2021/914 and/or 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 as adapted for the UK, a completed copy of which comprises Part 1 of Schedule 3. or such alternative clauses as may be approved by the European Commission or by the UK from time to time;  |
| Third Party Request | means a written request from any third party for disclosure of Personal Data where compliance with such request is required or purported to be required by law or regulation. |
| UK GDPR | has the meaning given in Section3(10) of the Data Protection Act 2018. |

**Part B - Interpretation**

1. Clause and Schedule headings are inserted for convenience only and shall not affect the interpretation of this Agreement.
2. References to Clauses and Schedules are to the Clauses and Schedules of this Agreement.
3. A reference to a statute or statutory provision is a reference to it as amended, extended or re-enacted from time to time.
4. A reference to a statute or statutory provision shall include all subordinate legislation made under that statute or statutory provision.
5. Any words following the terms including, include, in particular or any similar expression shall be construed as illustrative and shall not limit the sense of the words, description, definition, phrase or term preceding those terms.
6. Words in the singular shall include the plural and in the plural include the singular.

## Schedule 2: Data Protection Particulars and Security Requirements:

### Part A - Data Protection Particulars

|  |  |
| --- | --- |
| **Subject Matter of the Processing:** | [This should be a high level, short description of what the processing is about i.e., its subject matter of the contract. Example: The processing is needed in order to ensure that the Processor can effectively deliver the contract to provide a service to members of the public. ] |
| **Duration of the Processing:** | [Clearly set out the duration of the processing including dates] |
| **Nature and Purpose of the Processing:** | [Please be as specific as possible and make sure that you cover all intended purposes] The nature of the processing means any operation 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 of data (whether or not by automated means) etc. The purpose might include: employment processing, statutory obligation, recruitment assessment etc] |
| **Type of Personal Data:** | [Examples here include: name, address, date of birth, NI number, telephone number, pay, images, biometric data etc] |
| **Categories of Data Subject:** | [Examples include: Staff (including volunteers, agents, and temporary workers), customers/ clients, suppliers, patients, students / pupils, members of the public, users of a particular website etc] |

### Part B - Security Requirements

|  |  |
| --- | --- |
| **Methods and standards of encryption used:***Use Strong Encryption for the electronic transfer of Personal Information and Confidential Information outside of USW-controlled networks, within externally-controlled networks or when transmitting Personal Information and Confidential Information over any untrusted network.* *Use Strong Encryption to protect Personal Information and Confidential Information when stored.**“Strong Encryption” means the use of encryption technologies with minimum key lengths of 256-bits for symmetric encryption and 1024-bits for asymmetric encryption. Strong Encryption includes, but is not limited to: TLS v1.3, Point to Point Tunnelling Protocol (PPTP), AES 256, RSA 1024 bit, SHA3, Internet Protocol Security (IPSEC), SFTP, and SSH.* | [***Note: This Part schedule should include any specific restrictions/security requirements.***] |

## Schedule 3

International Data Transfer Addendum to the EU Commission Standard Contractual Clauses

This Schedule may be deleted where no restricted transfer will be made

 If a restricted transfer will be made, please complete the sections highlighted in grey.

Standard Data Protection Clauses to be issued by the Commissioner under S119A(1) Data Protection Act 2018

International Data Transfer Addendum to the EU Commission Standard Contractual Clauses

VERSION B1.0, in force 21 March 2022

This Addendum has been issued by the Information Commissioner for Parties making Restricted Transfers. The Information Commissioner considers that it provides Appropriate Safeguards for Restricted Transfers when it is entered into as a legally binding contract.

## Part 1: Tables

### Table 1: Parties

Start date

|  |  |  |
| --- | --- | --- |
| 1. **The Parties**
 | 1. **Exporter (who sends the Restricted Transfer)**
 | 1. **Importer (who receives the Restricted Transfer)**
 |
| 1. **Parties’ details**
 | 1. Full legal name:
2. Trading name (if different):
3. Main address (if a company registered address):
4. Official registration number (if any) (company number or similar identifier):
 | 1. Full legal name:
2. Trading name (if different):
3. Main address (if a company registered address):
4. Official registration number (if any) (company number or similar identifier):
 |
| 1. **Key Contact**
 | 1. Full Name (optional):
2. Job Title:
3. Contact details including email:
 | 1. Full Name (optional):
2. Job Title:
3. Contact details including email:
 |
| 1. **Signature (if required for the purposes of Section ‎2)**
 |  |  |

### Table 2: Selected SCCs, Modules and Selected Clauses

|  |  |
| --- | --- |
| 1. **Addendum EU SCCs**
 | Yes/No The version of the Approved EU SCCs which this Addendum is appended to, detailed below, including the Appendix Information:1. Date:
2. Reference (if any):
3. Other identifier (if any):
4. **Or**

 Yes/No the Approved EU SCCs, including the Appendix Information and with only the following modules, clauses or optional provisions of the Approved EU SCCs brought into effect for the purposes of this Addendum:  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 1. Module
 | 1. Module in operation
 | 1. Clause 7 (Docking Clause)
 | 1. Clause 11 (Option)
 | 1. Clause 9a (Prior Authorisation or General Authorisation)
 | 1. Clause 9a (Time period)
 | 1. Is personal data received from the Importer combined with personal data collected by the Exporter?
 |
| 1. 1
 |  |  |  |  |  |  |
| 1. 2
 |  |  |  |  |  |  |
| 1. 3
 |  |  |  |  |  |  |
| 1. 4
 |  |  |  |  |  |  |

### Appendix Information

“**Appendix Information**” means the information which must be provided for the selected modules as set out in the Appendix of the Approved EU SCCs (other than the Parties), and which for this Addendum is set out in:

**Table 3: Appendix Information**

“**Appendix Information**” means the information which must be provided for the selected modules as set out in the Appendix of the Approved EU SCCs (other than the Parties), and which for this Addendum is set out in:

|  |
| --- |
| Annex 1A: List of Parties:       |
| Annex 1B: Description of Transfer:       |
| Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data:       |
| Annex III: List of Sub processors (Modules 2 and 3 only):       |

### Table 4: Ending this Addendum when the Approved Addendum Changes

|  |  |
| --- | --- |
| 1. **Ending this Addendum when the Approved Addendum changes**
 | 1. Which Parties may end this Addendum as set out in Section ‎19:
2. Importer Yes/No
3. Exporter Yes/No
4. neither Party Yes/No
 |

## Part 2: Mandatory Clauses

### Entering into this Addendum

1. Each Party agrees to be bound by the terms and conditions set out in this Addendum, in exchange for the other Party also agreeing to be bound by this Addendum.
2. Although Annex 1A and Clause 7 of the Approved EU SCCs require signature by the Parties, for the purpose of making Restricted Transfers, the Parties may enter into this Addendum in any way that makes them legally binding on the Parties and allows data subjects to enforce their rights as set out in this Addendum. Entering into this Addendum will have the same effect as signing the Approved EU SCCs and any part of the Approved EU SCCs.

### Interpretation of this Addendum

1. Where this Addendum uses terms that are defined in the Approved EU SCCs those terms shall have the same meaning as in the Approved EU SCCs. In addition, the following terms have the following meanings:

|  |  |
| --- | --- |
| 1. **Term**
 | 1. **Meaning**
 |
| 1. Addendum
 | 1. This International Data Transfer Addendum which is made up of this Addendum incorporating the Addendum EU SCCs.
 |
| 1. Addendum EU SCCs
 | 1. The version(s) of the Approved EU SCCs which this Addendum is appended to, as set out in Table 2, including the Appendix Information.
 |
| 1. Appendix Information
 | 1. As set out in Appendix Information
 |
| 1. Appropriate Safeguards
 | 1. The standard of protection over the personal data and of data subjects’ rights, which is required by UK Data Protection Laws when you are making a Restricted Transfer relying on standard data protection clauses under Article 46(2)(d) UK GDPR.
 |
| 1. Approved Addendum
 | 1. The template Addendum issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section ‎18.
 |
| 1. Approved EU SCCs
 | 1. The Standard Contractual Clauses set out in the Annex of Commission Implementing Decision (EU) 2021/914 of 4 June 2021.
 |
| 1. ICO
 | 1. The Information Commissioner.
 |
| 1. Restricted Transfer
 | 1. A transfer which is covered by Chapter V of the UK GDPR.
 |
| 1. UK
 | 1. The United Kingdom of Great Britain and Northern Ireland.
 |
| 1. UK Data Protection Laws
 | 1. All laws relating to data protection, the processing of personal data, privacy and/or electronic communications in force from time to time in the UK, including the UK GDPR and the Data Protection Act 2018.
 |
| 1. UK GDPR
 | 1. As defined in section 3 of the Data Protection Act 2018.
 |

1. This Addendum must always be interpreted in a manner that is consistent with UK Data Protection Laws and so that it fulfils the Parties’ obligation to provide the Appropriate Safeguards.
2. If the provisions included in the Addendum EU SCCs amend the Approved SCCs in any way which is not permitted under the Approved EU SCCs or the Approved Addendum, such amendment(s) will not be incorporated in this Addendum and the equivalent provision of the Approved EU SCCs will take their place.
3. If there is any inconsistency or conflict between UK Data Protection Laws and this Addendum, UK Data Protection Laws applies.
4. If the meaning of this Addendum is unclear or there is more than one meaning, the meaning which most closely aligns with UK Data Protection Laws applies.
5. Any references to legislation (or specific provisions of legislation) means that legislation (or specific provision) as it may change over time. This includes where that legislation (or specific provision) has been consolidated, re-enacted and/or replaced after this Addendum has been entered into.

### Hierarchy

1. Although Clause 5 of the Approved EU SCCs sets out that the Approved EU SCCs prevail over all related agreements between the parties, the parties agree that, for Restricted Transfers, the hierarchy in Section ‎10 will prevail.
2. Where there is any inconsistency or conflict between the Approved Addendum and the Addendum EU SCCs (as applicable), the Approved Addendum overrides the Addendum EU SCCs, except where (and in so far as) the inconsistent or conflicting terms of the Addendum EU SCCs provides greater protection for data subjects, in which case those terms will override the Approved Addendum.
3. Where this Addendum incorporates Addendum EU SCCs which have been entered into to protect transfers subject to the General Data Protection Regulation (EU) 2016/679 then the Parties acknowledge that nothing in this Addendum impacts those Addendum EU SCCs.

### Incorporation of and changes to the EU SCCs

1. This Addendum incorporates the Addendum EU SCCs which are amended to the extent necessary so that:
	1. together they operate for data transfers made by the data exporter to the data importer, to the extent that UK Data Protection Laws apply to the data exporter’s processing when making that data transfer, and they provide Appropriate Safeguards for those data transfers;
	2. Sections ‎9 to ‎11 override Clause 5 (Hierarchy) of the Addendum EU SCCs; and
	3. this Addendum (including the Addendum EU SCCs incorporated into it) is (1) governed by the laws of England and Wales and (2) any dispute arising from it is resolved by the courts of England and Wales, in each case unless the laws and/or courts of Scotland or Northern Ireland have been expressly selected by the Parties.
2. Unless the Parties have agreed alternative amendments which meet the requirements of Section ‎12, the provisions of Section ‎15 will apply.
3. No amendments to the Approved EU SCCs other than to meet the requirements of Section ‎12 may be made.
4. The following amendments to the Addendum EU SCCs (for the purpose of Section ‎12) are made:
5. References to the “Clauses” means this Addendum, incorporating the Addendum EU SCCs;
6. In Clause 2, delete the words:
	* 1. “and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679”;
7. Clause 6 (Description of the transfer(s)) is replaced with:
	* 1. “The details of the transfers(s) and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred) are those specified in Annex I.B where UK Data Protection Laws apply to the data exporter’s processing when making that transfer.”;
8. Clause 8.7(i) of Module 1 is replaced with:
	* 1. “it is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer”;
9. Clause 8.8(i) of Modules 2 and 3 is replaced with:
	* 1. “the onward transfer is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer;”
10. References to “Regulation (EU) 2016/679”, “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 (General Data Protection Regulation)” and “that Regulation” are all replaced by “UK Data Protection Laws”. References to specific Article(s) of “Regulation (EU) 2016/679” are replaced with the equivalent Article or Section of UK Data Protection Laws;
11. References to Regulation (EU) 2018/1725 are removed;
12. References to the “European Union”, “Union”, “EU”, “EU Member State”, “Member State” and “EU or Member State” are all replaced with the “UK”;
13. The reference to “Clause 12(c)(i)” at Clause 10(b)(i) of Module one, is replaced with “Clause 11(c)(i)”;
14. Clause 13(a) and Part C of Annex I are not used;
15. The “competent supervisory authority” and “supervisory authority” are both replaced with the “Information Commissioner”;
16. In Clause 16(e), subsection (i) is replaced with:
	* 1. “the Secretary of State makes regulations pursuant to Section 17A of the Data Protection Act 2018 that cover the transfer of personal data to which these clauses apply;”;
17. Clause 17 is replaced with:
	* 1. “These Clauses are governed by the laws of England and Wales.”;
18. Clause 18 is replaced with:
	* 1. “Any dispute arising from these Clauses shall be resolved by the courts of England and Wales. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of any country in the UK. The Parties agree to submit themselves to the jurisdiction of such courts.”; and
19. The footnotes to the Approved EU SCCs do not form part of the Addendum, except for footnotes 8, 9, 10 and 11.

### Amendments to this Addendum

1. The Parties may agree to change Clauses 17 and/or 18 of the Addendum EU SCCs to refer to the laws and/or courts of Scotland or Northern Ireland.
2. If the Parties wish to change the format of the information included in Part 1: Tables of the Approved Addendum, they may do so by agreeing to the change in writing, provided that the change does not reduce the Appropriate Safeguards.
3. From time to time, the ICO may issue a revised Approved Addendum which:
4. makes reasonable and proportionate changes to the Approved Addendum, including correcting errors in the Approved Addendum; and/or
5. reflects changes to UK Data Protection Laws;

The revised Approved Addendum will specify the start date from which the changes to the Approved Addendum are effective and whether the Parties need to review this Addendum including the Appendix Information. This Addendum is automatically amended as set out in the revised Approved Addendum from the start date specified.

1. If the ICO issues a revised Approved Addendum under Section ‎18, if any Party selected in section “Ending the Addendum when the Approved Addendum changes”, will as a direct result of the changes in the Approved Addendum have a substantial, disproportionate and demonstrable increase in:
	1. its direct costs of performing its obligations under the Addendum; and/or
	2. its risk under the Addendum,

and in either case it has first taken reasonable steps to reduce those costs or risks so that it is not substantial and disproportionate, then that Party may end this Addendum at the end of a reasonable notice period, by providing written notice for that period to the other Party before the start date of the revised Approved Addendum.

1. The Parties do not need the consent of any third party to make changes to this Addendum, but any changes must be made in accordance with its terms.

## Alternative Part 2 Mandatory Clauses:

|  |  |
| --- | --- |
| 1. **Mandatory Clauses**
 | 1. Part 2: Mandatory Clauses of the Approved Addendum, being the template Addendum B.1.0 issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section ‎‎18 of those Mandatory Clauses.
 |

**Document control panel (template agreement)**

|  |  |
| --- | --- |
| Document name/ title | Data Processing Agreement |
| Version number | 2.0 |
| Status (draft, published or superseded) | Published |
| Department / Team | Legal, Governance and Assurance |
| Relevant or related policies | Data Protection Policy |
| Distribution (internal or external) | External when incomplete |
| Author / Owner (if different name both) | Eloise Rosser, Data Protection Officer  |
| Date of sign off | 31/1/23 |
| Review date | 31/1/24 |
| Security Classification | Public when incomplete |

**Version history panel (template agreement)**

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Changes made** | **Date** | **Made by** |
| 1.1 | Original | Unknown | Unknown |
| 1.2 | Minor wording changes  | Unknown | Unknown |
| 2.0 | Amendments made following the introduction of the UK GDPR and the International Data Transfer Agreement and Addendum, specific security requirements added | 31/1/23 | Eloise Rosser, Data Protection Officer |
| 2.1 | Format Changes to make the document accessible and more usable | 2022-02-21 | Kevin Mears, Records Manager |
|  |  |  |  |