**Introduction**

When contracting a supplier for services which will involve the processing of personal data or access to personal data on behalf of a data controller, the contractual clauses must reference certain specific requirements in accordance with the UK General Data Protection Regulation (UK GDPR).

Data protection legislation specifically requires the data controller to instruct the data processor regarding the use of personal data used and gathered on behalf of the controller.

**Structuring Contracts**

Whether or not the contract is written by the data controller or the data processor, the relationship must be clarified, and the instruction clearly set out. This document contains the relevant content that should be included in a contract.

Some aspects may not be specifically relevant and should be tailored to meet the needs of the data controller these may include the types of data used or the nature of the required retention period. These details may be included in the schedule attached to the contract (Appendix A). Both parties must sign the agreement at the end of Appendix A.

If data is to be transferred or processed outside of the EU, the “International Data Transfer Addendum to the EU Commission Standard Contractual Clauses” muct be included within the contract. This can be found at Appendix B.

**1. Definitions and Interpretation**

* 1. In this agreement, the following terms shall have the meaning set out below:

**Caldicott Principles (1997, 2012 & 2016)** means the Caldicott principles which protect patient identifiable data. These principles are applicable to any processing of health or social care data.

**Contractor** means the service provider.

**Customer** means the contracting organisation, in this case [ORGANISATION NAME].

**Data** means any ‘information’ provided by, obtained or created on behalf of the customer in delivering the services specified in this contract; and in the case of Personal Data, any data processed on behalf of the customer where the customer is the data controller.

**Data Protection Act 2018 (DPA)** means the Data Protection Act 2018 (DPA).

**Data Protection Officer (DPO)** means the role as defined under Chapter IV, Articles 37 – 39 of UK GDPR.

**Environmental Information Regulations 2004 (EIR)** means the Environmental Information Regulations 2004 (EIR) as amended or re-enacted from time to time and any Act substantially replacing the same.

**Freedom of Information Act 2000 (FOIA)** means the Freedom of Information Act 2000 (FOIA) as amended or re-enacted from time to time and any Act substantially replacing the same.

**Good Industry Practice** means the exercise of the degree of skill, diligence, prudence and foresight which would reasonably and ordinarily be expected from a skilled and experienced contractor engaged in the same type of undertaking under the same or similar circumstances as are contemplated by this agreement.

**UK General Data Protection Regulation (UK GDPR)** means the UK General Data Protection Regulation, as amended or re-enacted from time to time and any United Kingdom Act substantially replacing the same.

**Information** has the meaning given under Section 84 of the Freedom of Information Act 2000 (FOIA), which shall include (but is not limited to) information in any form whether relating to the past, present or future and may in particular consist of data, documentation, programs, (including the source code of any programs which the customer has the right to use), computer output, voice transmissions, correspondence, calculations, plans, reports, graphs, charts, statistics, records, projections, maps, drawings, vouchers, receipts and accounting records and may consist of or be stored in any form including paper, microfilm, microfiche, photographic negative, computer software and any electronic medium and references herein to Information shall include reference to the medium in which it is stored.

**Information Legislation** means the DPA, FOIA, UK GDPR and the EIR.

**Information Governance Requirements** means the documented set of additional information governance requirements which the customer applies within itself and requires of its Contractors and of which it has furnished a copy to the Contractor via [information governance](http://thewire.wiltshire.council/index/staff-policies/information-governance.htm).

**Legislation** for the avoidance of doubt includes all Law in particular the Information Legislation.

**Personal Data** means personal data as defined in Sections 3(2) and (3) of the DPA and Article 4(2) of the UK GDPR, which is supplied to the contractor by the customer or obtained by the contractor in the course of performing the services.

**Subject Access Request** means a request for personal data falling within the provisions of Articles 12 and 15 of the UK GDPR.

**2. Resolution of Inconsistency**

2.1 The contractor shall immediately upon becoming aware of the same notify the customer of any inconsistency between its practices and the provisions of information legislation, including related regulation, standards, guidance and policies applicable under this schedule and compliance statements made by the contractor during the contract procurement process.

2.2 Where notified or it otherwise becomes aware of inconsistency the customer, as soon as practicable, shall advise the contractor which provision the contractor shall be required to comply with (but not so as to place the contractor in breach of any legislation) by means of an action plan which:

2.2.1 specifies the inconsistency and articulates the resulting risks posed to the customer’s compliance with legislation,

2.2.2 explains how the requirement to resolve the inconsistency meets the contractual requirements and the statements of compliance made during the tender process,

2.2.3 specifies the time period which in the customer’s opinion is reasonable in which to resolve the inconsistency,

2.2.4 explains the means by which the customer intends to satisfy itself that the inconsistency is resolved and specifies the steps the contractor is required to take to facilitate any assessment, and

2.2.5 takes into account the opinion of the contractor on the level of resource required to resolve the inconsistency.

2.3 Where inconsistencies are not resolved within the expectations set out in paragraph 2.2, the customer may use the dispute resolution provisions of this contract

**3. Protection of Information**

3.1 The contractor acknowledges that the confidentiality, integrity and availability of information and on the security provided in relation to Information is a material element of this agreement.

3.2 The contractor shall and at all times provide a level of security which:

3.2.1 is in accordance with legislation and this contract,

3.2.2 is in accordance with compliance regimes representing good industry practice which the customer may specify,

3.2.3 complies with the information governance requirements, and

3.2.3 meets any specific security threats identified from time to time by the customer.

3.3 The contractor shall ensure that it provides comparable technical and policy coverage of security to information as if it were being processed directly by the customer. This shall include but not limited to the following:

3.3.1 All mobile storage systems and hardware shall be encrypted to at least industry standards.

3.3.2 When data is to be sent out, every effort should be made to use secure electronic transfer methods, for example via encrypted email, a secure email portal, psn.

3.3.3 When data is being emailed, every effort should be made to reply to an email, rather than free-typing an email address.

3.3.4 Where electronic transfer is not possible, personal data must sent using Royal Mail recorded delivery, with the recipient address checked by at least two individuals prior to posting.

3.3.5 All employees shall be appropriately vetted before use in the services which are the subject of this agreement.

3.3.6 All employees shall receive adequate information governance training which shall be refreshed over a period of no longer than every two years, and assurances will be provided to the customer in this regard.

3.3.7 the customer reserves the right to see evidence of training completion for all employees subject to this agreement.

3.3.8 All buildings and physical environments shall be subject to appropriate physical security and protection.

3.3.9 When handling NHS data, the contractor shall apply safe haven usage to at least NHS standard and comply with the requirements of the Caldicott Principles.

3.3.10 The contractor shall permit access to information by employees of the customer only.

3.3.11 The contractor shall securely destroy all information provided or created under this agreement, which is no longer required to be retained in accordance with this agreement.

3.4 The contractor will have in place fully tested and effective disaster recovery and business continuity plans.

3.5 The contractor shall observe the following principles when handling personal data for the purpose of carrying out the contractor’s obligations under this agreement.

3.5.1 Every proposed processing of personal data within or outside the contractor’s organisation should be clearly defined and regularly risk assessed and approved by an appropriate information governance role holder.

3.5.2. Personal data must not be processed unless it is absolutely necessary. Personal data should not be used unless there is no alternative.

3.5.3 The minimum necessary personal data is to be used. Where use of personal data is considered necessary, each individual item of information should be justified with the aim of reducing the need for processing personally identifiable information.

3.5.4 Access to personal data should be on a strict need to know basis. Employees should only have access to the data that they need to see, and should only receive the access and functionality permissions required to undertake their roles.

3.5.5 The contractor must ensure that its employees are aware of their responsibility to comply with the common law duty of confidentiality.

3.5.6 All persons handling personal data must understand and comply with the DPA and UK GDPR. All processing of personal data must be lawful.

3.6 Any information received by the contractor from the customer under this agreement or generated by the contractor pursuant to this agreement shall remain at all times the property of the customer. It shall be identified, clearly marked and recorded as such by the contractor on all media and in all documentation.

3.7 The contractor shall not, save as required by this agreement, without the prior written consent of the customer disclose to any other person any information provided by the customer under this agreement.

3.8 Where processing personal data, the contractor shall not procure the services of any other agent or subcontractor in connection with this agreement without the explicit written consent of the customer.

3.9 The contractor shall observe and comply with the customer’s security classification/ protective marking scheme as defined within its information governance requirements.

3.10 The contractor shall take all necessary precautions to ensure that all information obtained from the customer under or in connection with this agreement, is given only to such of the contractor’s employees and professional advisors or consultants engaged to advise the contractor in connection with this agreement as is strictly necessary for the performance of this agreement, and is treated as confidential and not disclosed (without prior written approval) or used by any such employees or such professional advisors or consultants otherwise than for the purposes of this agreement.

3.11 The contractor shall not use any information it receives from the customer otherwise than for the purposes of this agreement.

3.12 With regard to authority data:

3.12.1 The contractor shall not delete or remove any proprietary notices contained within or relating to the customer data.

3.12.2 The contractor shall not store, copy, disclose, or use the customer data except as necessary for the performance by the contractor of its obligations under this agreement or as otherwise expressly authorised in writing by the customer.

3.12.3. To the extent that authority data is held and/or processed by the contractor, the contractor shall supply that authority data to the customer as requested by the customer in the format it is held.

3.12.4. The contractor shall take responsibility for preserving the integrity of authority data and preventing the corruption or loss of authority data.

3.12.5 The contractor shall perform secure back-ups of all authority data and shall ensure that up-to-date back-ups are stored off-site in accordance with the business continuity and disaster recovery plan. The contractor shall ensure that such back-ups are available to the customer at all times upon request and are delivered to the customer at no less than monthly intervals.

3.12.6 The contractor shall ensure that any system on which the contractor holds any authority data, including back-up data, is a secure system that complies with the customer’s information governance requirements.

3.12.7 If the customer data is corrupted, lost or sufficiently degraded as a result of the contractor's default so as to be unusable, the customer may:

3.12.7.1 require the contractor (at the contractor's expense) to restore or procure the restoration of authority data in full and in not later than three days (subject to any agreed business continuity and disaster recovery plan); and/or

3.12.7.2 in default thereof itself restore or procure the restoration of authority data, and shall be repaid by the contractor any reasonable expenses incurred in doing so.

3.12.8 If at any time the contractor suspects or has reason to believe that authority data has or may become corrupted, lost or sufficiently degraded in any way for any reason, then the contractor shall notify the customer immediately and inform the customer of the remedial action the contractor proposes to take.

**4. Data Protection**

4.1 the customer is and will remain the data controller in relation to the personal information processed under this agreement, and that the contractor will act as data processor with respect to such personal information. As such, the contractor must follow the direction of the customer as to how personal data is processed.

4.2 All personal data acquired by the contractor from the customer shall only be used for the purposes of this agreement and shall not be further processed or disclosed without the prior written consent of the customer.

4.3 The contractor shall comply with the UK GDPR requirements with regard to appointing a Data Protection Officer.

4.4 The contractor warrants that it has complied with its notification requirements under the DPA to undertake the subject matter of this agreement. Where notification is required, the contractor is operating under registration number [number].

4.5 The contractor shall comply with all relevant codes of practice issued under the DPA and UK GDPR.

4.6 The contractor shall assist the customer in safeguarding the legal rights of the data subject.

4.7 The contractor will have in place at all times appropriate technical and organisational security measures to safeguard authority data in compliance with UK GDPR, DPA and National Cyber Security Centre (NSNC) guidance.

4.8 The Contractor shall indemnify the customer against loss, destruction or processing contrary to information legislation by itself, its employees, contractors or agents.

4.9 The contractor shall ensure the reliability and ongoing training of all its relevant employees to ensure awareness of and compliance with the contractor’s obligations under the DPA and the UK GDPR.

4.10 The customer shall respond to all Subject Access Requests (SAR), whether received by the contractor or the customer.

4.10.1 On receipt of a SAR made directly to them, the Contractor will forward the request immediately, and no later than two working days after receipt, to [ORGANISATION DP LEAD]

4.10.2 If requested by the customer, the Contractor shall provide to the customer the personal data requested by the data subject (as defined in the DPA) within 10 working days of receipt of instruction by the customer for supply of the data.

4.10.3 The information shall be supplied to the customer in pdf form in full, with any proposed redactions highlighted.

4.11 The contractor shall immediately and no later than two working days after receipt, forward to [ORGANISATION DP LEAD]:

4.11.1 a request from any person whose personal data it holds to access his or her personal data; or

4.11.2 a complaint or request relating to the customer’s obligations under the DPA and the UK GDPR

4.12 The contractor will assist and co-operate with the customer in relation to any complaint or request received, including:

4.12.1 providing full details of the complaint or request,

4.12.2 providing the customer with any information relating to a SAR within 10 working days of receipt of the request,

4.12.3 promptly providing the service manager with any personal data and other information requested by him, and

4.12.4 respond to any further requests from the customer’s Data Protection Officer when investigating information security incidents.

4.13 In addition to the obligation undertaken in paragraph 3.8, the contractor shall not further process information outside of the EEA as defined by the DPA and UK GDPR without full prior written consent from the customer.

4.14 The contractor shall cooperate with data protection compliance audits as and when requested.

4.15 The contractor shall comply with UK GDPR requirements for maintaining accurate, current and comprehensive Records of Processing Activities (RoPA).

**5. Caldicott Principles**

[DELETE SECTION 5 IF THE PROCESSING DOES NOT INVOLVE HEALTH OR SOCIAL CARE DATA]

The Contractor must also observe the Caldicott Principles when processing health and/or social care data, which are set out below.

**1. Justify the purpose(s)**

Every proposed use or transfer of personal confidential data within or from an organisation should be clearly defined, scrutinised and documented, with continuing uses regularly reviewed, by an appropriate guardian.

**2. Don’t use personal confidential data unless it is absolutely necessary**

Personal confidential data items should not be included unless it is essential for the specified purpose(s) of that flow. The need for patients to be identified should be considered at each stage of satisfying the purpose(s).

**3. Use the minimum necessary personal confidential data**

Where use of personal confidential data is considered to be essential, the inclusion of each discrete item of data should be considered and justified so that the minimum amount of personal confidential data is transferred or accessible as is necessary for a given function.

**4. Access to personal confidential data should be on a strict need-to-know basis**

Only those individuals who need access to personal confidential data should have access to it, and they should only have access to the data items that they need to see. This may mean introducing access controls or splitting data flows where one data flow is used for several purposes.

**5. Everyone with access to personal confidential data should be aware of their responsibilities**

Action should be taken to ensure that those handling personal confidential data, both clinical and non-clinical employees, are made fully aware of their responsibilities and obligations to respect patient confidentiality.

**6. Comply with the law**

Every use of personal confidential data must be lawful. Someone in each organisation handling personal confidential data should be responsible for ensuring that the organisation complies with legal requirements.

**7. The duty to share information can be as important as the duty to protect patient confidentiality.**

Health and social care professionals should have the confidence to share information in the best interests of their patients within the framework set out by these principles. They should be supported by the policies of their employers, regulators and professional bodies.

**8. Inform patients and service users about how their confidential information is used.**

A range of steps should be taken to ensure no surprises for patients and service users, so they can have clear expectations about how and why their confidential information is used, and what choices they have about this. These steps will vary depending on the use: as a minimum, this should include providing accessible, relevant and appropriate information - in some cases, greater engagement will be required.

**6. The FOIA and the EIR**

[DELETE THIS SECTION IF THE DATA CONTROLLER IS NOT SUBJECT TO THE FOIA]

6.1 the customer is subject to the provisions of the FOIA and the EIR and the contractor shall assist the customer (at the contractor’s expense) to enable the customer to comply with these Acts. The contractor acknowledges that the customer may be obliged to disclose information relating to this agreement. Notwithstanding any other term of this agreement, the contractor hereby gives its consent for the customer to publish this agreement in its entirety, including from time to time agreed changes to the agreement, to the general public in whatever form the customer decides.

6.2 The contractor must transfer any request for information under FOIA and EIR to the customer as soon as practicable after receipt and in any event within two working days of receipt.

6.3 Where the customer so requires for the purpose of compliance with the information legislation, the contractor shall provide the customer with a copy of all Information in its possession or power, in the form that the customer requires, within 10 working days (or such other reasonable period as the customer may specify) of the customer requesting the information.

6.4 Without prejudice to paragraph 6.6 and subject to paragraph 6.8 below, where the contractor believes the disclosure of information would prejudice its commercial interests or constitute an actionable breach of confidentiality, the customer shall consider any case made where it is provided within 10 working days (or such other reasonable period as the customer may specify) of the customer requesting the information.

6.5 The contractor shall provide all necessary assistance as requested by the customer under paragraph 6.3 above so as to enable the customer to respond to a request for information within the time for compliance set out in section 10 of the FOIA or regulation 5 of the EIR.

6.6 As between the parties, the customer will determine at its absolute discretion whether any information is exempt from disclosure in accordance with the provisions of the FOIA or the EIR.

6.7 In no event will the contractor respond directly to a request for information unless expressly authorised to do so by the customer, save to acknowledge receipt (if so requested by the customer).

6.8 The contractor acknowledges that the customer may be obliged under the FOIA or the EIR to disclose information without consulting with the contractor, or following consultation with the contractor and having taken its views into account.

6.9 The contractor must ensure that all Information produced in the course of this agreement or relating to this agreement is retained for disclosure in line with the customer’s policy on information retention periods and must permit the customer to inspect such records as requested from time to time.

6.10 The contractor acknowledges that any lists or schedules provided by it outlining confidential information are of indicative value only and that the customer may nevertheless be obliged to disclose confidential Information.

**7. Disclosures by [ORGANISATION]**

7.1 Nothing in this agreement shall prevent the customer disclosing any Information:

7.1.1 for the purpose of the examination and certification of the customer’s accounts; or

7.1.2 any examination pursuant to Section 6 (1) of the National Audit Act 1983 of the economy, efficiency and effectiveness with which the customer has used its resources; or

7.1.3 to any government department or any other contracting authority (as defined in The Public Contracts Regulations 2006). All government departments or contracting authorities receiving such confidential information shall be entitled to further disclose the confidential information to other government departments or other contracting authorities on the basis that the information is confidential and is not to be disclosed to a contractor which is not part of any government department or any contracting authority; or

7.1.4 to any person engaged in providing any services to the customer for any purpose relating to or ancillary to this agreement provided that in disclosing information the customer discloses only the information which is necessary for the purpose concerned and requires that the information is treated in confidence and that a confidentiality undertaking is given where appropriate.

**8. Accessibility of data**

Where the contractor is undertaking work on behalf of the customer to develop new systems, practices or documentation in processing of data, the contractor shall ensure that there remains the ability to extract data in a format accessible to and useable by the customer (with regard to paragraph 11.3) supported by an Impact Assessment which is approved by the customer.

**9. Know-how**

Nothing in this agreement shall prevent either party from using any techniques, ideas or know-how gained during the performance of this agreement in the course of its normal business, to the extent that this does not result in a disclosure of Information the subject of this agreement.

**10. Information breaches**

10.1 The contractor shall ensure all losses or breaches of security or information are reported to the customer within 24 hours whether actual, potential or attempted, in order for the customer to notify the regulator and, where necessary, the data subjects, as required by UK GDPR.

10.2 The contractor will ensure all breaches are internally investigated, and appropriate remedial action taken, along with supporting the customer and the Information Commissioner’s Office (ICO) in any investigation by it. A copy of the investigation report must be provided to the customer.

10.3 The contractor will immediately take all reasonable steps to remedy such breaches and to protect the integrity of both parties against any actual, potential or attempted breach or threat and any equivalent attempted breach in the future.

**11. Breach, termination and continuance**

11.1 The contractor shall indemnify the customer for any breach of the requirements of this schedule which renders the customer liable for any costs, fines, claims or expenses under legislation howsoever arising.

11.2 Failure on the part of the contractor to comply with the provisions of this schedule shall amount to a breach of this contract and shall give the customer the right to exercise any and all of the remedies in this contract and recover all costs incurred as a consequence of the contractor’s breach.

11.3 On termination of this agreement howsoever arising the contractor shall when directed to do so by the customer, and instruct all its agents and subcontractors to:

11.3.1 transfer to the customer the whole or any part of the personal data and other Information received or acquired by the contractor for the purposes of or in the course of the delivery of the services the subject of this agreement; and

11.3.2 ensure the data is supplied in an agreed usable format; and

11.3.3 ensure that such a transfer is made securely in a manner specified by the customer and the data complies with the requirement at paragraph 7; and

11.3.4 securely destroy or erase the whole or any part of such personal data and other Information retained by the contractor and provide to the customer such proof of destruction as the customer may reasonably specify.

11.4 The provisions of this paragraph shall continue in effect notwithstanding termination of this agreement.

**Appendix A: Data Processing Schedule**

The Provider shall comply with any further written instructions with respect to processing by the customer. Any such further instructions shall be incorporated into this Schedule.

|  |  |
| --- | --- |
| **Description** | **Details** |
| Names of Parties | 1. [DATA CONTROLLER]  2. [THE PROVIDER] |
| Purpose | [Brief outline of service provided] |
| Subject matter of the processing | Personal data will be processed by [contractor name] for the specific purposes of [eg provision of XXXX services for [client organisation name]. [XXXX] for the specific purposes of [XXX] etc.] |
| Duration of the processing | The contract term is [state contract duration here] |
| Nature and purposes of the processing | Purpose of the processing: [State the nature of the processing here e.g. the taking and storing of photographs of [xxxxx].[xxxxxx] will only be shared with [client name] by secure means [state agreed secure method] and will not be published on contractor website or otherwise shared with any other third party etc.].  *The nature of the processing may include (not exhaustive) the 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).* |
| Type of personal data | This will include [state what personal data will be included here eg photographic images, names etc. amend as necessary].  *This may include: number, telephone number, biometric data, religion, ethnicity, professional involvements, physical and mental health reports and correspondence, care and support assessments and planning, desired outcomes, family and relationships and case notes.* |
| Categories of Data Subject | This may include [state data subjects here eg customers / clients / persons taking part in [activity]]. |
| Plan for return and destruction of the data once the processing is complete unless a legislative requirement to preserve that type of data | The Contractor shall retain such documents and records in accordance with its obligations under the Data Protection Act 2018.  Subject to the legal obligations, upon termination of the contract the personal data shall be returned to the customer and any copies held by the contractor shall be securely destroyed. |

|  |  |
| --- | --- |
| Signed for and on behalf of  **Data Controller** [DATA CONTROLLER] | Signed for and on behalf of  **Data Processor** [Provider] |
| Authorised Signatory  **Signature**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  **Name:** [OFFICER NAME]  **Position:** [OFFICER JOB TITLE]  **Date:** [DATE] | Authorised Signatory  **Signature**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  **Name:** [OFFICER NAME]  **Position:** [OFFICER JOB TITLE]  **Date:** [DATE] |

**Appendix B: International Data Transfer Addendum to the EU Commission Standard Contractual Clauses**

**Entering into this Addendum**

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.

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**

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:

|  |  |
| --- | --- |
| Addendum | This International Data Transfer Addendum which is made up of this Addendum incorporating the Addendum EU SCCs. |
| Addendum EU SCCs | The version(s) of the Approved EU SCCs which this Addendum is appended to. |
| Appropriate Safeguards | 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. |
| Approved Addendum | 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. |
| Approved EU SCCs | The Standard Contractual Clauses set out in the Annex of Commission Implementing Decision (EU) 2021/914 of 4 June 2021. |
| ICO | The Information Commissioner. |
| Restricted Transfer | A transfer which is covered by Chapter V of the UK GDPR. |
| UK | The United Kingdom of Great Britain and Northern Ireland. |
| UK Data Protection Laws | 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. |
| UK GDPR | As defined in section 3 of the Data Protection Act 2018. |

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.

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.

If there is any inconsistency or conflict between UK Data Protection Laws and this Addendum, UK Data Protection Laws applies.

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.

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**

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.

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.

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**

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.

Unless the Parties have agreed alternative amendments which meet the requirements of Section ‎12, the provisions of Section ‎15 will apply.

No amendments to the Approved EU SCCs other than to meet the requirements of Section ‎12 may be made.

The following amendments to the Addendum EU SCCs (for the purpose of Section ‎12) are made:

1. References to the “Clauses” means this Addendum, incorporating the Addendum EU SCCs;
2. In Clause 2, delete the words:

“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”;

1. Clause 6 (Description of the transfer(s)) is replaced with:

“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.”;

1. Clause 8.7(i) of Module 1 is replaced with:

“it is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer”;

1. Clause 8.8(i) of Modules 2 and 3 is replaced with:

“the onward transfer is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer;”

1. 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;
2. References to Regulation (EU) 2018/1725 are removed;
3. References to the “European Union”, “Union”, “EU”, “EU Member State”, “Member State” and “EU or Member State” are all replaced with the “UK”;
4. The reference to “Clause 12(c)(i)” at Clause 10(b)(i) of Module one, is replaced with “Clause 11(c)(i)”;
5. Clause 13(a) and Part C of Annex I are not used;
6. The “competent supervisory authority” and “supervisory authority” are both replaced with the “Information Commissioner”;
7. In Clause 16(e), subsection (i) is replaced with:

“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;”;

1. Clause 17 is replaced with:

“These Clauses are governed by the laws of England and Wales.”;

1. Clause 18 is replaced with:

“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

1. 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**

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.

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.

From time to time, the ICO may issue a revised Approved Addendum which:

1. makes reasonable and proportionate changes to the Approved Addendum, including correcting errors in the Approved Addendum; and/or
2. 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.

If the ICO issues a revised Approved Addendum under Section ‎18, if any Party selected in Table 4 “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.

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:**

|  |  |
| --- | --- |
| **Mandatory Clauses** | 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. |