

OFFICIAL - SENSITIVE - COMMERCIAL

HMRC Standard Goods and Services Model Contract v1.0

SCHEDULE 2.8

DATA PROCESSING AND LIST OF SUB-PROCESSORS

Data Processing and List of Sub-Processors

DEFINITIONS

In this Schedule, the following definitions shall apply:

“Data Protection Impact Assessment”	means an assessment by the Controller of the impact of the processing on the protection of Personal Data;
“Data Protection Officer”	has the meaning given in the Relevant Data Protection Laws;
“Data Subject”	has the meaning given in the Relevant Data Protection Laws;
“Data Subject Access Request”	a request made by a Data Subject in accordance with rights granted pursuant to the Relevant Data Protection Laws to access his or her Personal Data;
“GDPR”	means the Regulation of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data being enforced in the EU from 25 May 2018 (repealing Directive 95/46/EC), along with the codes of practice, codes of conduct, regulatory guidance and standard clauses and other related or equivalent domestic legislation, as updated from time to time;
“Off-shore Location”	any place outside of the United Kingdom;
“Personal Data Breach”	means: <ul style="list-style-type: none">(a) a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Personal Data transmitted, stored or otherwise Processed;(b) a discovery or reasonable suspicion that there is a vulnerability in any technological measure used to protect any Personal Data that has previously been subject to a breach within the scope of paragraph (a), which may result in exploitation or exposure of that Personal Data; or

- (c) any defect or vulnerability with the potential to impact the ongoing resilience, security and/or integrity of systems Processing Personal Data;

“Processor”

has the meaning given in the Relevant Data Protection Laws;

“Standard Clauses”

Contractual

means the standard contractual clauses for the transfer of personal data to processors established in third countries, as approved by the European Commission in Decision 2010/87/EU, or any set of clauses approved by the European Commission or a supervisory authority (as such term is defined by the GDPR) which subsequently amends, replaces or supersedes these.

1 PROTECTION OF PERSONAL DATA

1.1 With respect to the Parties' rights and obligations under this Agreement, the Parties acknowledge that the Authority is the Controller and that the Supplier is the Processor, and that the processing may not be determined by the Supplier.

1.2 The Supplier shall:

- (a) not Process or transfer the Personal Data other than in accordance with the Authority's written instructions, as set out in Annex 1, unless required by EU or member state law or UK Law to which the Supplier is subject, in which case the Supplier shall promptly inform the Authority of that legal requirement before Processing or transferring that Personal Data, unless prohibited by law;
- (b) acknowledge that the provision of the Services is restricted to the Processing of the types of Personal Data and categories of Data Subject set out in Part 1 of Annex 1, and shall, with the Authority's written consent, update the details in Annex 1 from time to time as necessary;
- (c) ensure that at all times it has in place appropriate technical and organisational measures to guard against unauthorised or unlawful processing of the Personal Data, Personal Data Breaches and/or accidental loss, destruction or damage to the Personal Data, including the measures as are set out in Clause 20 (*Authority Data and Security Requirements*) and having regard to the:
 - (i) nature of the data to be protected;

- (ii) harm that might result from a Personal Data Breach;
 - (iii) state of technological development; and
 - (iv) cost of implementing any measures;
- (d) not disclose or transfer the Personal Data to any third party or Supplier Personnel unless necessary for the provision of the Services and, for any disclosure or transfer of Personal Data to any third party, obtain the prior written consent of the Authority (save where such disclosure or transfer is specifically authorised under this Agreement);
- (e) take all reasonable steps to ensure the reliability and integrity of any Supplier Personnel who have access to the Personal Data and ensure that the Supplier Personnel:
- (i) are aware of and comply with the Supplier's duties under this Paragraph 1 and Clause 20 (*Authority Data and Security Requirements*) and 21 (*Confidentiality*);
 - (ii) are subject to confidentiality undertakings or professional or statutory obligations of confidentiality;
 - (iii) are informed of the confidential nature of the Personal Data and do not publish, disclose or divulge any of the Personal Data to any third party unless directed in writing to do so by the Authority or as otherwise permitted by this Agreement;
 - (iv) have undergone adequate training in the use, care, protection and handling of Personal Data (as defined in the Relevant Data Protection Laws); and
 - (v) retain evidence of the steps taken in respect of Paragraphs 1.2(e)(i) to 1.2(e)(iv) above for the Authority's inspection;
- (f) notify the Authority immediately upon becoming aware of a reasonably suspected, "near-miss" or actual Personal Data Breach or circumstances that may give rise to a Personal Data Breach, providing the Authority with sufficient information and in a timescale which allows the Authority to meet its obligations to report a Personal Data Breach within 72 hours under Article 33 of the GDPR. Such notification shall as a minimum:
- (i) describe the nature of the Personal Data Breach, the categories and approximate numbers of Data Subjects concerned, and the categories and numbers of Personal Data records concerned;
 - (ii) communicate the name and contact details of the Data Protection Officer or other relevant contact from whom more information may be obtained;
 - (iii) describe the likely consequences of the Personal Data Breach; and

HMRC Standard Goods and Services Model Contract v1.0

- (iv) describe the measures taken or proposed to be taken to address the Personal Data Breach.
- (g) co-operate with the Authority and take such reasonable commercial steps as are directed by it to mitigate or remedy the consequences of a reasonably suspected, “near-miss” or actual Personal Data Breach including but not limited to:
 - (i) documenting any such Personal Data Breaches and reporting them to any supervisory authority;
 - (ii) taking measures to address any such Personal Data Breaches, including where appropriate, measures to mitigate their possible adverse effects; and
 - (iii) conducting Data Protection Impact Assessments of any Processing operations and consulting any supervisory authorities, Data Subjects and their representatives accordingly;
- (h) notify the Authority immediately if it receives:
 - (i) from a Data Subject (or third party on their behalf):
 - (A) a Data Subject Access Request (or purported Data Subject Access Request);
 - (B) a request to rectify, any inaccurate Personal Data;
 - (C) a request to have any Personal Data erased;
 - (D) a request to restrict the Processing of any Personal Data;
 - (E) a request to obtain a portable copy of part of the Personal Data, or to transfer such a copy to any third party;
 - (F) an objection to any Processing of Personal Data;
 - (G) any other request, complaint or communication relating to the Authority’s obligations under the Relevant Data Protection Laws;
 - (ii) any communication from the Information Commissioner’s Office or any other regulatory authority in connection with Personal Data; or
 - (iii) a request from any third party for disclosure of Personal Data where compliance with such request is required or purported to be required by Law;

HMRC Standard Goods and Services Model Contract v1.0

- (i) not, without the Authority's prior written consent, and subject also to Clause 24 (*Publications*), make or permit any announcement in respect of a Personal Data Breach or respond to any request, communication or complaint of the kind listed at Paragraph 1.2(h)(i)-(iii);
 - (j) taking into account the nature of the processing, provide the Authority with full assistance in relation to either Party's obligations under the Relevant Data Protection Laws and any complaint, communication or request as listed at Paragraph 1.2(h) (and insofar as possible within the timescales reasonably required by the Authority) including by promptly providing:
 - (i) the Authority with full details and copies of the complaint, communication or request;
 - (ii) such assistance as is reasonably requested by the Authority to enable the Authority to comply with a Data Subject Access Request within the relevant timescales set out in the Relevant Data Protection Laws;
 - (iii) the Authority, at its request, with any Personal Data it holds in relation to a Data Subject;
 - (iv) assistance as requested by the Authority following any Personal Data Breach;
 - (v) assistance as requested by the Authority with respect to any request from the Information Commissioner's Office, or any consultation by the Authority with the Information Commissioner's Office;
 - (k) without prejudice to Paragraph 1.2(a), not without the prior written consent of the Authority:
 - (i) convert any Personal Data for "big data" analysis or purposes;
or
 - (ii) match or compare any Personal Data with or against any other Personal Data (whether the Supplier's or any third party's);and in each case the Supplier shall only take the steps set out in (i) to (ii) above strictly to the degree required to fulfil its obligations under this Agreement.
- 1.3 The Supplier's obligation to notify under Paragraph 1.2(f) and 1.2(h) shall include the provision of further information to the Authority in phases, as details become available.
- 1.4 Not applicable

- 1.5 The Supplier must obtain the prior written consent of the Authority before appointing any Sub-contractor or other third party to Process any Personal Data ("**Sub-processor**") and the Supplier shall remain fully liable to the Authority and any other Service Recipient for any failure by a Sub-processor to fulfil its obligations in relation to the Processing of any Personal Data. Such consent shall be conditional upon:
- (a) the use of any Sub-processor being otherwise in accordance with Clause 15 (*Supply Chain Rights and Protections*), Schedule 4.3 (*Notified and Key Sub-contractors*) and Paragraph 1.7; and
 - (b) the Supplier entering into a continuing obligation to provide the Authority with such information regarding the Sub-processor as the Authority may reasonably require.
- 1.6 In accordance with Paragraph 1.5, the Authority consents to the use by the Supplier as at the Effective Date of the Sub-processors listed in Part B of Annex 1 which shall be updated as required with the written consent of the Authority.
- 1.7 The Supplier shall procure that all Sub-processors:
- (a) prior to commencing the Processing of any Personal Data enter into a written contract in relation to the Processing with either the Authority or the Supplier which shall include substantially the same data protection obligations on the Sub-processor as are imposed on the Supplier by this Agreement and which shall set out the Sub-processor's agreed Processing activities in the same or substantially similar form as provided at Part A of Annex 1; or
 - (b) insofar as the contract referred to at paragraph (a) above involves the transfer of Personal Data to any Off-shore Location in accordance with Paragraph 1.8, it shall incorporate the Standard Contractual Clauses or such other mechanism as directed by the Authority to ensure the adequate protection of the transferred Personal Data;
 - (c) act in accordance with this Paragraph 1.
- 1.8 The Supplier shall not Process or otherwise transfer any Personal Data in or to any Off-shore Location (unless the transfer is required by EU or member state law to which the Supplier is subject, and if this is the case then the Supplier shall inform the Authority of that legal requirement before Processing that Personal Data, unless that law prohibits such information being provided). If, after the Effective Date, the Supplier or any Sub-contractor wishes to Process and/or transfer any Personal Data in or to any Off-shore Location, the following provisions shall apply:
- (a) the Supplier shall submit a Change Request to the Authority which, if the Authority agrees, at its sole discretion, to such Change Request, shall be dealt with in accordance with the Change Control Procedure and Paragraphs 1.8(b) to 1.8(d);

- (b) the Supplier shall set out in its Change Request and/or Impact Assessment details of the following:
- (i) the Personal Data which will be transferred to and/or Processed in any Off-shore Location;
 - (ii) the Off-shore Location in which the Personal Data will be transferred to and/or Processed;
 - (iii) any Sub-processor who will be Processing and/or receiving Personal Data in an Off-shore Location; and
 - (iv) how the Supplier will ensure an adequate level of protection and adequate safeguards in respect of the Personal Data that will be Processed in and/or transferred to Off-Shore Location(s) so as to ensure the Authority's compliance with the Relevant Data Protection Laws;
- (c) in providing and evaluating the Change Request and Impact Assessment, the Parties shall ensure that they have regard to and comply with then-current Authority, Central Government Bodies and Information Commissioner Office policies, procedures, guidance and codes of practice on, and any approvals processes in connection with, the Processing in and/or transfers of Personal Data to any Off-shore Location; and
- (d) the Supplier shall comply with such other instructions and shall carry out such other actions as the Authority may notify in writing, including:
- (i) incorporating Relevant Data Protection Laws Standard Contractual Clauses into this Agreement or a separate data processing agreement between the Parties; and
 - (ii) complying with the provisions of Paragraphs 1.5 to 1.7 in relation to any Sub-contractor or other third party who will be Processing and/or receiving or accessing the Personal Data in any Off-shore Location and shall either enter into:
 - (A) a direct data processing agreement with the Authority on such terms as may be required by the Authority; or
 - (B) a data processing agreement with the Supplier on terms which are equivalent to those agreed between the Authority and the Sub-contractor relating to the relevant Personal Data transfer,

and in each case which the Supplier acknowledges may include the incorporation of Relevant Data Protection Laws Standard Contractual Clauses and technical and organisation measures which the Authority deems necessary for the purpose of protecting Personal.

HMRC Standard Goods and Services Model Contract v1.0

- 1.9 The Supplier shall ensure that the Authority complies with any obligations under the Relevant Data Protection Laws and shall not perform its obligations under this Agreement in such a way as to cause the Authority to breach any of the Authority's obligations under the Relevant Data Protection Laws to the extent the Supplier is aware, or ought reasonably to have been aware, that the same would be a breach of such obligations. In connection with this obligation, the Supplier shall:
- (a) immediately inform the Authority if, in its opinion, any instruction infringes, or might reasonably be considered to infringe, the Relevant Data Protection Laws;
 - (b) provide all reasonable assistance to the Authority in the preparation of any Data Protection Impact Assessment prior to commencing any processing, such assistance including, at the discretion of the Authority:
 - (i) a systematic description of the envisaged processing operations and the purpose of the processing;
 - (ii) an assessment of the necessity and proportionality of the processing operations in relation to the Services;
 - (iii) an assessment of the risks to the rights and freedoms of Data Subjects; and
 - (iv) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of Personal Data;
 - (c) implement, review and maintain organisational and technical security measures to ensure the security of Personal Data in accordance with Article 32 of the GDPR, including by:
 - (i) pseudonymising or encrypting Personal Data with the written consent of the Authority;
 - (ii) ensuring the on-going confidentiality, integrity, availability and resilience of Processing systems and services;
 - (iii) ensuring a means to restore the availability of and access to Personal Data in a timely manner following any physical or technical incident; and
 - (iv) having in place a process for regularly testing, assessing and evaluating the effectiveness of the organisational and technical security measures; and
 - (d) at the written direction of the Authority, promptly and securely delete or return to the Authority or transfer to any Replacement Supplier Personal Data (and any copies of it) in such format as is requested by the Authority, unless the Supplier is required by Law to retain the Personal Data.

- 1.10 The Supplier shall not cause the Authority to breach any obligation under the Relevant Data Protection Laws and shall itself comply fully with its obligations under the Relevant Data Protection Laws including by:
- (a) adhering to any relevant codes of conduct published pursuant to Article 40 of the GDPR;
 - (b) designating a Data Protection Officer if required by the Relevant Data Protection Laws;
 - (c) maintaining complete and accurate records of its Processing of Personal Data containing the information set out in Article 30(2) of the GDPR, this requirement applying only where the Supplier employs 250 or more staff, unless:
 - (i) the Processing is not occasional;
 - (ii) the Processing includes special categories of data as referred to in Article 9(1) of the GDPR or Personal Data relating to criminal convictions and offences referred to in Article 10 of the GDPR; and
 - (iii) the Processing is likely to result in a risk to the rights and freedoms of Data Subjects; and
 - (d) reporting any suspected non-compliance or actual non-compliance with this Paragraph 1 to the Authority immediately upon becoming aware of such non-compliance.
- 1.11 The Supplier shall allow for audits of its Data Processing activity by the Authority or the Authority's designated auditor, and make available to the Authority or the Authority's designated auditor all information necessary to demonstrate compliance with this Paragraph.
- 1.12 For the avoidance of doubt, nothing in this Agreement relieves the Supplier of its own direct responsibilities and liabilities under the GDPR.

ANNEX 1 - DATA PROCESSING AND LIST OF SUB-PROCESSORS

Introduction

Part A of this Annex lists the types of Personal Data and categories of Data Subject which the Supplier will Process in its provision of the Services together with a description of the nature, purposes and duration of the Processing, the subject matter of the Processing, and the retention policy in respect of that data, and has been collated in accordance with Paragraph 1.2(a) and (b).

Part B of this Annex lists the Sub-Processors agreed by the Parties in accordance with Paragraph 1.5.

Part A: Data Processing

1. The Supplier shall comply with any further written instructions from the Authority with respect to Processing.
2. Any such further instructions shall be incorporated into this Schedule.

Description	Details
Subject matter of the processing	
Duration of the processing	
Nature and purposes of the processing	

Type of personal data	
Categories of data subjects	
Plan for return and destruction of the data once the processing is complete UNLESS requirement under UK Law or EU or member state law to preserve that type of data	

Part B: Sub-processors as at the Effective Date

List of Sub-processors to be populated