

# Schedule 15 – Data processing schedule where BTP or HS2 is acting as Controller

## 1. Application of this Schedule

This Schedule applies where the *Service Provider* provides works to BTP or HS2 pursuant to this contract which requires the processing of Personal Data by the *Service Provider*.

Pursuant to clause Y(UK)3, Z18.1.1(B) and as set out in the Contract Data, each of BTP and HS2 are named as beneficiaries for the purposes of enforcing the provisions, including this Schedule, as identified in the Contract Data against the *Service Provider*.

To the extent that any claims are made by one Party against the other in respect of a breach of this Schedule 15, the Parties acknowledge and agree that the provisions of clause X18 apply and that furthermore, in respect of any liability arising as a result of this Schedule 15, references to the Client shall be construed as including BTP and HS2 (as applicable).

A default by the *Service Provider* under this Schedule 15 shall constitute a default for the purposes of the contract.

Where the *Service Provider* provides works to BTP or HS2 pursuant to this contract which requires the processing of Personal Data by the *Service Provider*, this Schedule 15 will take precedence in the event of any conflict between this Schedule 15 and the remainder of the contract as it relates (or may relate) to the processing of personal data, or BTP's or HS2's (as the context requires) ability to enforce this Schedule 15 in accordance with its provisions.

When used in this Schedule, references to:

- (1) *Service Manager* shall be construed as a reference to the *Service Manager* for BTP or HS2, as applicable; and
- (2) *Party* shall be a reference to BTP or HS2 (as applicable) and the *Service Provider*.

## 2. Data protection – General

- (a) The *Service Provider* processes Personal Data and ensures that Service Provider Staff process Personal Data only in accordance with this Paragraph 2.
- (b) The *Service Provider* does not remove any ownership or security notices in or relating to the Government Data.
- (c) The *Service Provider* makes accessible back-ups of all Government Data, stored in an agreed off-site location and send the *Service Manager* copies every 6 months.
- (d) The *Service Provider* ensures that any *Service Provider* system holding any Government Data, including back-up data, is a secure system that complies with the Security Policy and any applicable Security Management Plan.
- (e) If at any time the *Service Provider* suspects or has reason to believe that the Government Data provided under the contract is corrupted, lost or sufficiently degraded, then the *Service Provider* notifies the *Service Manager* and immediately suggests remedial action.
- (f) If the Government Data is corrupted, lost or sufficiently degraded so as to be unusable BTP or HS2 (as applicable) may either or both:
  - (i) tell the *Service Provider* to restore or get restored Government Data as soon as practical but no later than 5 Working Days from the date that the *Service Manager* receives notice, or the *Service Provider* finds out about the issue, whichever is earlier; and/or
  - (ii) restore the Government Data itself or using a third party.

(g) The *Service Provider* must pay each of its and BTP or HS2's (as applicable) reasonable costs of complying with Paragraph 2(f) unless BTP or HS2 (as applicable) is at fault.

(h) The *Service Provider*:

- (i) provides the *Service Manager* with all Government Data in an agreed open format within 10 Working Days of a written request;
- (ii) must have documented processes to guarantee prompt availability of Government Data if the *Service Provider* stops trading;
- (iii) securely destroys all Storage Media that has held Government Data at the end of life of that media using Good Industry Practice;
- (iv) securely erases all Government Data and any copies it holds when asked to do so by the *Service Manager* unless required by Law to retain it; and
- (v) indemnifies BTP or HS2 (as applicable) against any and all Losses incurred by BTP or HS2 where such Losses have been caused by the *Service Provider* or otherwise to the extent that such Losses have been contributed to by the *Service Provider*.

### **.3 Status of the Controller**

3.1 The *Service Provider* and HS2 and BTP (as applicable) acknowledge that for the purposes of the Data Protection Legislation, where the *Service Provider* processes Personal Data for the purposes of performing the Service under a Service Order, the party issuing the Service Order is the Controller and the *Service Provider* is the Processor.

2.2 This Schedule sets out the rights and obligations as required between a Controller and Processor.

### **4 Where one Party is Controller and the other Party its Processor**

4.1 Where a Party is a Processor, it only undertakes Processing to the extent it is authorised to do so as set out in the Annexes to this Schedule 15 (and Schedule 14, to the extent referred to in the Annexes to this Schedule 15).

4.2 A Processor complies with any written instructions with respect to Processing issued by the Controller. Annex 1 sets out the scope of data processing where BTP is the Controller, and Annex 2 sets out the scope of data processing where HS2 is the Controller.

4.3 The Processor notifies the Controller immediately if it considers that any of the Controller's instructions infringe the Data Protection Legislation.

4.4 The Processor provides all reasonable assistance to the Controller in the preparation of any Data Protection Impact Assessment prior to commencing any Processing. Such assistance may, at the discretion of the Controller, include:

- (a) a systematic description of the envisaged Processing and the purpose of the Processing;
- (b) an assessment of the necessity and proportionality of the Processing in relation to the service;
- (c) an assessment of the risks to the rights and freedoms of Data Subjects; and
- (d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of Personal Data.

4.5 The Processor, in relation to any Personal Data Processed in connection with its obligations under the contract:

- (a) Processes that Personal Data only in accordance with the *Processing Personal Data Requirements*, unless the Processor is required to do otherwise by Law. If it is so required the Processor promptly notifies the Controller before Processing the Personal Data unless prohibited by Law;
- (b) ensures that it has in place Protective Measures, including in the case of the *Service Provider* the measures set out at Paragraph 2(c), which the Controller may reasonably reject (but failure to reject shall not amount to approval by the Controller of the adequacy of the Protective Measures) having taken account of 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;
- (c) ensures that:
- (i) the Processor Personnel do not Process Personal Data except in accordance with the contract (and in particular the *Processing Personal Data Requirements*);
  - (ii) it takes all reasonable steps to ensure the reliability and integrity of any Processor Personnel who have access to the Personal Data and ensure that they:
    - (A) are aware of and comply with the Processor's duties under this schedule, clause 27 (Disclosure) and Z9 (Freedom of Information);
    - (B) are subject to appropriate confidentiality undertakings with the Processor or any Subprocessor;
    - (C) 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 Controller or as otherwise permitted by the contract; and
    - (D) have undergone adequate training in the use, care, protection and handling of Personal Data;
- (d) does not transfer Personal Data outside of the EU unless the prior written consent of the Controller has been obtained and the following conditions are fulfilled:
- (i) the Controller or the Processor has provided appropriate safeguards in relation to the transfer (whether in accordance with UK GDPR Article 46 or LED Article 37) as determined by the Controller;
  - (ii) the Data Subject has enforceable rights and effective legal remedies;
  - (iii) the Processor complies with its obligations under the Data Protection Legislation by providing an adequate level of protection to any Personal Data that is transferred (or, if it is not so bound, uses its best endeavours to assist the Controller in meeting its obligations); and
  - (iv) the Processor complies with any reasonable instructions notified to it in advance by the Controller with respect to the Processing of the Personal Data; and
- (e) at the written direction of the Controller, delete or return Personal Data (and any copies of it) to the Controller on termination of the contract unless the Processor is required by Law to retain the Personal Data.

4.6 Subject to Paragraph 4.7, the Processor notifies the Controller immediately if in relation to it Processing Personal Data under or in connection with the contract it:

- (a) receives a Data Subject Access Request (or purported Data Subject Access Request);
- (b) receives a request to rectify, block or erase any Personal Data;
- (c) receives any other request, complaint or communication relating to either Party's obligations under the Data Protection Legislation;
- (d) receives any communication from the Information Commissioner or any other regulatory authority in connection with Personal Data Processed under the contract;
- (e) receives 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; or
- (f) becomes aware of a Personal Data Breach.

4.7 The Processor's obligation to notify under Paragraph 4.6 includes the provision of further information to the Controller, as details become available.

4.8 Taking into account the nature of the Processing, the Processor provides the Controller with assistance in relation to either Party's obligations under Data Protection Legislation and any complaint, communication or request made under Paragraph 4.6 (and insofar as possible within the timescales reasonably required by the Controller) including by immediately providing:

- (a) the Controller with full details and copies of the complaint, communication or request;
- (b) such assistance as is reasonably requested by the Controller to enable it to comply with a Data Subject Access Request within the relevant timescales set out in the Data Protection Legislation;

- (c) the Controller, at its request, with any Personal Data it holds in relation to a Data Subject;
- (d) assistance as requested by the Controller following any Personal Data Breach; and/or
- (e) assistance as requested by the Controller with respect to any request from the Information Commissioner's Office, or any consultation by the Controller with the Information Commissioner's Office.

4.9 The Processor maintains complete and accurate records and information to demonstrate its compliance with this Schedule. This requirement does not apply where the Processor employs fewer than 250 staff, unless:

- (a) the Controller determines that the Processing is not occasional;
- (b) the Controller determines the Processing includes special categories of data as referred to in Article 9(1) of the UK GDPR or Personal Data relating to criminal convictions and offences referred to in Article 10 of the UK GDPR; or
- (c) the Controller determines that the Processing is likely to result in a risk to the rights and freedoms of Data Subjects.

4.10 The Processor allows for audits of its data Processing activity by the Controller or the Controller's designated auditor.

4.11 The Parties designate a Data Protection Officer if required by the Data Protection Legislation.

4.12 Before allowing any Subprocessor to Process any Personal Data related to the contract, the Processor must:

- (a) notify the Controller in writing of the intended Subprocessor and Processing;
- (b) obtain the written consent of the Controller;
- (c) enter into a written agreement with the Subprocessor which gives effect to the terms set out in this Schedule such that they apply to the Subprocessor; and
- (d) provide the Controller with such information regarding the Subprocessor as the Controller may reasonably require.

BTP or HS2 (as applicable) shall not unreasonably withhold written consent to any Subprocessor where that Subprocessor has been approved in writing in advance by the *Client*.

4.13 The Processor remains fully liable for all acts or omissions of any of its Subprocessors.

4.14 If the *Client* replaces the provisions set out in this Schedule pursuant to clause Z18.3, the Parties shall promptly revise this Schedule so that it is compatible with the provisions relating to the processing of Personal Data as set out in clause Z18.3.

4.15 The Parties agree to take account of any guidance issued by the Information Commissioner's Office. If the *Client* amends the provisions set out in this Schedule pursuant to clause Z18.4, the Parties shall promptly revise this Schedule so that it is compatible with the provisions relating to the processing of Personal Data as set out in clause Z18.4.

## Annex 1 – Data processing Annex where BTP is acting as Controller

This Annex shall be completed by the Controller, who may take account of the view of the Processor, however the final decision as to the content of this Schedule shall be with the Controller at its absolute discretion.

1. The contact details of the Controller's Data Protection Officer are:  
[REDACTED]
2. The contact details of the Processor's Data Protection Officer are [REDACTED]
3. The Processor shall comply with any further written instructions with respect to processing by the Controller.
4. Any such further instructions shall be incorporated into this Schedule.
5. Where this Annex refers out to Schedule 14 – Processing, Personal Data and Data Subjects, any references in that Schedule to 'Controller', 'Client' or 'DfT' shall, for the purposes of this Annex, be construed as references to BTP.

Description	Details
Identity of the Controller and Processor	Where BTP orders a Service pursuant to a Service Order, BTP is the Controller and the Service Provider is the Processor.  BTP the <i>Service Provider</i> acknowledge that for the purposes of Data Protection Legislation, BTP and the <i>Service Provider</i> may in some instances be independent Controllers.
Subject matter of the processing	Processing shall occur as set out in Schedule 14 - Processing, Personal Data and Data Subjects in relation to each work package.
Duration of the processing	The duration of the contract
Nature and purposes of the processing	As set out in Schedule 14 - Processing, Personal Data and Data Subjects in relation to each work package.

Type of Personal Data being Processed	As set out in Schedule 14 - Processing, Personal Data and Data Subjects in relation to each work package.
Categories of Data Subject	As set out in Schedule 14 - Processing, Personal Data and Data Subjects in relation to each work package.
International transfers and legal gateway	There are no known/approved international transfers at contract let.
Plan for return and destruction of the data once the processing is complete	The plan for return and destruction of the data shall be as agreed by the <i>Client</i> and <i>Service Provider</i> as part of exit arrangements, and shall apply to the return or destruction of Personal Data for which BTP is the Controller.

## Annex 2 – Data processing Annex where HS2 is acting as Controller

This Annex shall be completed by the Controller, who may take account of the view of the Processor, however the final decision as to the content of this Schedule shall be with the Controller at its absolute discretion.

1. The contact details of the Controller's Data Protection Officer are: [REDACTED]
2. The contact details of the Processor's Data Protection Officer are: [REDACTED]
3. The Processor shall comply with any further written instructions with respect to processing by the Controller.
4. Any such further instructions shall be incorporated into this Schedule.
5. Where this Annex refers out to Schedule 14 – Processing, Personal Data and Data Subjects, any references in that Schedule to 'Controller', 'Client' or 'DfT' shall, for the purposes of this Annex, be construed as references to HS2.

Description	Details
Identity of the Controller and Processor	Where HS2 orders a Service pursuant to a Service Order, HS2 is the Controller and the Contractor is the Processor.  HS2 and the <i>Service Provider</i> acknowledge that for the purposes of Data Protection Legislation, HS2 and the <i>Service Provider</i> may in some instances be independent Controllers.
Subject matter of the processing	Processing shall occur as set out in Schedule 14 - Processing, Personal Data and Data Subjects in relation to each work package.
Duration of the processing	The duration of the contract

Nature and purposes of the processing	As set out in Schedule 14 - Processing, Personal Data and Data Subjects in relation to each work package.
Type of Personal Data being Processed	As set out in Schedule 14 - Processing, Personal Data and Data Subjects in relation to each work package.
Categories of Data Subject	As set out in Schedule 14 - Processing, Personal Data and Data Subjects in relation to each work package.
International transfers and legal gateway	There are no known/approved international transfers at contract let.
Plan for return and destruction of the data once the processing is complete	The plan for return and destruction of the data shall be as agreed by the <i>Client</i> and the <i>Service Provider</i> as part of exit arrangements, and shall apply to the return or destruction of Personal Data for which HS2 is the Controller.