# SCHEDULE 11

# DATA PROTECTION AND GOVERNANCE

## 1 PROCESSING PERSONAL DATA

1.1 This Schedule 11 (*Data Protection and Governance*) supplements Clause 19 (*Protection of Personal Data*) of this Agreement and should be read and interpreted alongside those provisions.

1.2 The contact details of the Authority's Data Protection Officer are: cio-dpa@mod.gov.uk and contact details of the relevant Data Protection Advisor are **[Insert contact details – to be confirmed in line with stand-up of AFR HQ]**.

1.3 The contact details of the Supplier's Data Protection Officer are: dpo@serco.com

1.4 The Parties shall ensure that this Schedule 11 (*Data Protection and Governance*) is kept fully updated to ensure that it accurately reflects Personal Data processed pursuant to the provision of the Services, including populating such further details as come to light during the development of the technical solution during the Transition Phase.

1.5 The Processor shall comply with any further written instructions with respect to processing of Personal Data by the Controller. Any such further instructions shall be incorporated into this Schedule 11 (*Data Protection and Governance*).

1.6 The table below sets out the basis of the processing applicable to this Agreement. In completing the information required, the Authority may take account of the view of the Supplier, however the final decision as to the content (including any updates after the Signature Date) shall be at the Authority's absolute discretion.

| Description | Details |
|---|---|
| Identity of Controller and Processor for each Category of Personal Data | **The Authority is Controller and the Supplier is Processor**<br>The Parties acknowledge that in accordance with Clauses 19.3-19.15 and for the purposes of the Data Protection Legislation, the Authority is the Controller, and the Supplier is the Processor of the following Personal Data:<br>• Personal Data processed for the purposes of carrying out the Services as described in Schedule 2.1 (*Services Description*)<br>**The Parties are Joint Controllers**<br>The Parties agree that as of the Effective Date, there are no circumstances in which the Parties are acting as Joint Controllers for the purposes of the Data Protection Legislation. However, in the event that this should change during the Term, Clause 19.16 shall apply.<br>**The Parties are Independent Controllers of Personal Data**<br>The Parties acknowledge that in accordance with Clauses 19.17-19.28 and for the purposes of the Data Protection Legislation, the Parties are Independent Controllers of the following Personal Data being processed for the purposes of management and administration of this Agreement:<br>• Business contact details of Supplier Personnel;<br>• Business contact details of any directors, officers, employees, agents, consultants and contractors of the Authority (excluding the Supplier Personnel) engaged in the performance of the Authority's duties under this Agreement; and<br>• Personal Data which is respectively provided to or generated by the Parties in their role as employer or contracting counterparty to any physical person including the Personal Data of any Embedded Service Personnel where processed for the purposes of providing the Services as described in Schedule 9.3 (*Embedded Service Personnel*). |
| **Data Subjects / Categories of Data Subject** | Data Subjects will include but are not limited to: candidates including potential candidates from expression of interest through to onboarding, next of kin of candidates, doctors, GPs and other relevant medical professionals, persons engaged in recruitment assessments, Authority staff and Supplier Personnel. |

| | |
|---|---|
| **Type of Personal Data** | Names, telephone numbers, addresses, email addresses, branch/trade, education/qualifications, gender, location (AFCO), organisation (Royal Navy/Royal Air Force/Army), photograph showing physical likeness, rank/grade, service number, staff number, age, video footage, date of birth, identification documents including driving licence and/or passport details, medical information (including but not limited to blood group, med cat, GP notes, primary healthcare records, current medical status, physical statistics), National Insurance number, nationality, next of kin/family details, performance reports, pay/finance details, security clearance, tax/benefit/pension records, welfare information (housing/social services/child protection), physical/mental health or condition, racial or ethnic origin, religious beliefs or other beliefs, Personal Data relating to criminal convictions/offences. |
| **Nature and purposes of the processing (processing operations / activities)** | Personal Data will be processed for the purposes of:<br>• the Services, including employment processing, recruitment analytics, informing marketing strategy, informing recruitment strategy, statutory obligation, recruitment assessment, managing Authority communications and requests pursuant to the Services;<br>• contract management.<br>The nature of the processing will include but not be limited to 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 Personal Data. There shall be no processing solely by automated means without the involvement of a level of human intervention in that processing. |
| Protective Measures that the Supplier and, where applicable, its Sub-contractors have implemented to protect Personal Data processed under this Agreement against a breach of security (insofar as that breach of security relates to data) or a Personal Data Breach | Protective Measures will, as a minimum, meet the requirements set out in Schedule 2.1 (*Services Description*) and Schedule 2.4 (*Security Management*). |

| | |
|---|---|
| **Instructions for Disposal of Personal Data once the processing is complete** | See Annex 2 of this Schedule 11 (*Data Protection and Governance*). |
| **Date from which Personal Data is to be processed** | From the Effective Date. |
| **Duration of the processing** | Term of this Agreement plus applicable data retention in line with Annex 2 of this Schedule 11 (*Data Protection and Governance*). |
| **Locations at which the Supplier and/or its Sub-contractors process Personal Data under this Agreement** | The United Kingdom |

## ANNEX 1: DRAFT JOINT CONTROLLER AGREEMENT

### 1 JOINT CONTROLLER STATUS AND ALLOCATION OF RESPONSIBILITIES

1.1 With respect to Personal Data under Joint Control of the Parties, the Parties envisage that they shall each be a Data Controller in respect of that Personal Data in accordance with the terms of this Annex 1 of this Schedule 11 (*Data Protection and Governance*) in replacement of Clause 19.2-19-15 (Where one Party is Controller, and the other Party is Processor) and 19.17-19.27 (Independent Controllers of Personal Data). Accordingly, the Parties each undertake to comply with the applicable Data Protection Legislation in respect of their processing of such Personal Data as Data Controllers.

1.2 The Parties agree that the [Supplier/Authority *[DN: Allocation to be decided by the Parties if Joint Controller Agreement is used depending on nature of relationship and the Party best placed to respond to responsibilities outlined below]*]:

(a) is the exclusive point of contact for Data Subjects and is responsible for all steps necessary to comply with the GDPR regarding the exercise by Data Subjects of their rights under the GDPR;

(b) shall direct Data Subjects to its Data Protection Officer or suitable alternative in connection with the exercise of their rights as Data Subjects and for any enquiries concerning their Personal Data or privacy;

(c) is solely responsible for the Parties' compliance with all duties to provide information to Data Subjects under Articles 13 and 14 of the GDPR;

(d) is responsible for obtaining the informed consent of Data Subjects, in accordance with the GDPR, for processing in connection with the Services where consent is the relevant legal basis for that processing; and

(e) shall make available to Data Subjects the essence of this Joint Controller Agreement (and notify them of any changes to it) concerning the allocation of responsibilities as Joint Controller and its role as exclusive point of contact, the Parties having used their best endeavours to agree the terms of that essence. This must be outlined in the Supplier's privacy policy (which must be readily available by hyperlink or otherwise on all of its public facing services and marketing).

1.3 Notwithstanding the terms of Paragraph 1.2, the Parties acknowledge that a Data Subject has the right to exercise their legal rights under the Data Protection Legislation as against the relevant Party as Data Controller.

### 2 UNDERTAKINGS OF BOTH PARTIES

2.1 The Supplier and the Authority each undertake that they shall:

(a) report to the other Party quarterly (on dates to align with the Authority's reporting cycles):

(i) the volume of Data Subject Requests (or purported Data Subject Requests) from Data Subjects (or third parties on their behalf);

(ii) the volume of requests from Data Subjects (or third parties on their behalf) to rectify, block or erase any Personal Data;

(iii) any other requests, complaints or communications from Data Subjects (or third parties on their behalf) relating to the other Party's obligations under applicable Data Protection Legislation;

(iv) any communications from the Information Commissioner or any other regulatory authority in connection with Personal Data; and

(v) any requests from any third party for disclosure of Personal Data where compliance with such request is required or purported to be required by Law;

that it has received in relation to the subject matter of this Agreement during that period;

(b) notify each other immediately if it receives any request, complaint or communication made as referred to in Paragraphs 2.1(a)(i) to (a)(v);

(c) provide the other Party with full cooperation and assistance in relation to any request, complaint or communication made as referred to in Paragraphs 2.1(a)(i) to (a)(v) to enable the other Party to comply with the relevant timescales set out in the Data Protection Legislation;

(d) not disclose or transfer the Personal Data to any third party unless necessary for the provision of the Services and, for any disclosure or transfer of Personal Data to any third party, save where such disclosure or transfer is specifically authorised under this Agreement or is required by Law that disclosure or transfer of Personal Data is otherwise considered to be lawful processing of that Personal Data in accordance with Article 6 of the UK GDPR or EU GDPR (as the context requires). For the avoidance of doubt to which Personal Data is transferred must be subject to equivalent obligations which are no less onerous than those set out in this Annex 1 of this Schedule 11 (*Data Protection and Governance*);

(e) request from the Data Subject only the minimum information necessary to provide the Services and treat such extracted information as Confidential Information;

(f) ensure that at all times it has in place appropriate Protective Measures to guard against unauthorised or unlawful processing of the Personal Data and/or accidental loss, destruction or damage to the Personal Data and unauthorised or unlawful disclosure of or access to the Personal Data;

(g) take all reasonable steps to ensure the reliability and integrity of any of its Personnel who have access to the Personal Data and ensure that its Personnel:

(i) are aware of and comply with their duties under this Annex 1 of this Schedule 11 (*Data Protection and Governance*) and those in respect of Confidential Information;

(ii) are informed of the confidential nature of the Personal Data, are subject to appropriate obligations of confidentiality and do not publish, disclose or divulge any of the Personal Data to any third party where that Party would not be permitted to do so;

(iii) have undergone adequate training in the use, care, protection and handling of Personal Data as required by the applicable Data Protection Legislation;

(h) ensure that it has in place Protective Measures as appropriate to protect against a Data Loss Event having taken account of the:

(i) nature of the data to be protected;

(ii) harm that might result from a Data Loss Event;

(iii) state of technological development; and

(iv) cost of implementing any measures.

(i) ensure that it has the capability (whether technological or otherwise), to the extent required by Data Protection Legislation, to provide or correct or delete at the request of a Data Subject all the Personal Data relating to that Data Subject that the Supplier holds;

(j) ensure that it notifies the other Party as soon as it becomes aware of a Data Loss Event;

(k) where the Personal Data is subject to UK GDPR, not transfer such Personal Data outside of the UK unless the prior written consent of the non-transferring Party has been obtained and the following conditions are fulfilled:

(i) the transfer is in accordance with Article 45 of the UK GDPR or DPA 2018 Section 73;

(ii) the transferring Party has provided appropriate safeguards in relation to the transfer (whether in accordance with Article 46 of the UK GDPR or DPA 2018 Section 75) as agreed with the non-transferring Party which could include the International Data Transfer Agreement or International Data Transfer Agreement Addendum to the European Commission's SCCs as published by the Information Commissioner's Office as well as any additional measures;

(iii) the Data Subject has enforceable rights and effective legal remedies;

(iv) the transferring Party 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 non-transferring Party in meeting its obligations); and

(v) the transferring Party complies with any reasonable instructions notified to it in advance by the non-transferring Party with respect to the processing of the Personal Data; and

(l) where the Personal Data is subject to EU GDPR, not transfer such Personal Data outside of the EU unless the prior written consent of non-transferring Party has been obtained and the following conditions are fulfilled:

(i) the transfer is in accordance with Article 45 of the EU GDPR;

(ii) the transferring Party has provided appropriate safeguards in relation to the transfer in accordance with Article 46 of the EU GDPR as determined by the non-transferring Party which could include relevant parties entering into Standard Contractual Clauses in the European Commission's decision 2021/914/EU as well as any additional measures;

(iii) the Data Subject has enforceable rights and effective legal remedies;

(iv) the transferring Party complies with its obligations under the EU GDPR 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 non-transferring Party in meeting its obligations); and

(v) the transferring Party complies with any reasonable instructions notified to it in advance by the non-transferring Party with respect to the processing of the Personal Data.

2.2 Each Joint Controller shall use its reasonable endeavours to assist the other Controller to comply with any obligations under applicable Data Protection Legislation and shall not perform its obligations under this Annex 1 of this Schedule 11 (*Data Protection and Governance*) in such a way as to cause the other Joint Controller to breach any of its obligations under applicable Data Protection Legislation to the extent it is aware, or ought reasonably to have been aware, that the same would be a breach of such obligations.

**3 DATA PROTECTION BREACH**

3.1 Without prejudice to Paragraph 3.2, each Party shall notify the other Party promptly and without undue delay, and in any event within forty-eight (48) hours, upon becoming aware of any Personal Data Breach or circumstances that are likely to give rise to a Personal Data Breach, providing the other Party and its advisors with:

(a) sufficient information and in a timescale which allows the other Party to meet any obligations to report a Personal Data Breach under the Data Protection Legislation;

(b) all reasonable assistance, including:

(i) co-operation with the other Party and the Information Commissioner investigating the Personal Data Breach and its cause, containing and recovering the compromised Personal Data and compliance with the applicable guidance;

(ii) co-operation with the other Party including taking such reasonable steps as are directed by the Authority to assist in the investigation, mitigation and remediation of a Personal Data Breach;

(iii) co-ordination with the other Party regarding the management of public relations and public statements relating to the Personal Data Breach;

(iv) providing the other Party and to the extent instructed by the other Party to do so, and/or the Information Commissioner investigating the Personal Data Breach, with complete information relating to the Personal Data Breach, including, without limitation, the information set out in Paragraph 3.2; and

(c) in relation to data security incidents, the Parties shall comply with any requirements and timeframes imposed by the Authority's warning and reporting point (WARP) and/or the Data Protection Support Team.

3.2 Each Party shall take all steps to restore, re-constitute and/or reconstruct any Personal Data where it has lost, damaged, destroyed, altered or corrupted as a result of a Personal Data Breach as if it was that Party's own data at its own cost with all possible speed and shall provide the other Party with all reasonable assistance in respect of any such Personal Data Breach, including providing the other Party, as soon as possible and within forty-eight (48) hours of the Personal Data Breach relating to the Personal Data Breach, in particular:

(i) the nature of the Personal Data Breach;

(ii) the nature of Personal Data affected;

(iii) the categories and number of Data Subjects concerned;

(iv) the name and contact details of the Supplier's Data Protection Officer or other relevant contact from whom more information may be obtained;

(v) measures taken or proposed to be taken to address the Personal Data Breach; and

(vi) describe the likely consequences of the Personal Data Breach.

**4 AUDIT**

4.1 The Supplier shall permit:

(a) the Authority, or a third-party auditor acting under the Authority's direction, to conduct, at the Authority's cost, data privacy and security audits, assessments and inspections concerning the Supplier's data security and privacy procedures relating to Personal Data, its compliance with this Annex 1 of this Schedule 11 (*Data Protection and Governance*) and the Data Protection Legislation; and

(b) the Authority, or a third-party auditor acting under the Authority's direction, access to premises at which the Personal Data is accessible or at which it is able to inspect any relevant records, including the record maintained under Article 30 GDPR by the Supplier so far as relevant to this Agreement, and procedures, including premises under the control of any third party appointed by the Supplier to assist in the provision of the Services.

4.2 The Authority may, in its sole discretion, require the Supplier to provide evidence of the Supplier's compliance with Paragraph 4.1 in lieu of conducting such an audit, assessment or inspection.

**5 IMPACT ASSESSMENTS**

5.1 The Parties shall:

(a) provide all reasonable assistance to each other to prepare any Data Protection Impact Assessment as may be required (including provision of detailed information and assessments in relation to processing operations, risks and measures);

(b) maintain full and complete records of all processing carried out in respect of the Personal Data in connection with this Agreement, in accordance with the terms of Article 30 GDPR.

**6 ICO GUIDANCE**

The Parties agree to take account of any guidance issued by the Information Commissioner and/or any relevant Central Government Body. The Authority may on not less than thirty (30) Working Days' notice to the Supplier amend this Agreement to ensure that it complies with any guidance issued by the Information Commissioner and/or any relevant Central Government Body.

**7 LIABILITIES FOR DATA PROTECTION BREACH**

7.1 If financial penalties are imposed by the Information Commissioner on either the Authority or the Supplier for a Personal Data Breach ("**Financial Penalties**") then the following shall occur:

(a) If in the view of the Information Commissioner, the Authority is responsible for the Personal Data Breach, in that it is caused as a result of the actions or inaction of the Authority, its employees, agents, contractors (other than the Supplier) or systems and procedures controlled by the Authority, then the Authority shall be responsible for the payment of such Financial Penalties. In this case, the Authority will conduct an internal audit and engage at its reasonable cost, when necessary, an independent third party to conduct an audit of any such data incident. The Supplier shall provide to the Authority and its third-party investigators and auditors, on request and at the Supplier's reasonable cost, full co-operation and access to conduct a thorough audit of such data incident;

(b) If in the view of the Information Commissioner, the Supplier is responsible for the Personal Data Breach, in that it is not a breach that the Authority is responsible for, then the Supplier shall be responsible for the payment of these Financial Penalties. The Supplier will provide to the Authority and its auditors, on request and at the Supplier's sole cost, full co-operation and access to conduct a thorough audit of such data incident; or

(c) If no view as to responsibility is expressed by the Information Commissioner, then the Authority and the Supplier shall work together to investigate the relevant data incident and allocate responsibility for any Financial Penalties as outlined above, or by agreement to split any Financial Penalties equally if no responsibility for the Personal Data Breach can be apportioned. In the event that the Parties do not agree such apportionment then such Dispute shall be referred to the Dispute Resolution Procedure set out in Schedule 8.3 (*Dispute Resolution Procedure)*.

7.2 If either the Authority or the Supplier is the defendant in a legal claim brought before a court of competent jurisdiction ("**Court**") by a third party in respect of a Personal Data Breach, then unless the Parties otherwise agree, the Party that is determined by the final decision of the Court to be responsible for the Personal Data Breach shall be liable for the losses arising from such breach. Where both Parties are liable, the liability will be apportioned between the Parties in accordance with the decision of the Court.

7.3 In respect of any losses, cost claims or expenses incurred by either Party as a result of a Personal Data Breach (the "**Claim Losses**"):

(a) if the Authority is responsible for the relevant breach, then the Authority shall be responsible for the Claim Losses;

(b) if the Supplier is responsible for the relevant breach, then the Supplier shall be responsible for the Claim Losses: and

(c) if responsibility is unclear, then the Authority and the Supplier shall be responsible for the Claim Losses equally.

7.4 Nothing in Paragraphs 7.2-7.3 shall preclude the Authority and the Supplier reaching any other agreement, including by way of compromise with a third-party complainant or claimant, as to the apportionment of financial responsibility for any Claim Losses as a result of a Personal Data Breach, having regard to all the circumstances of the breach and the legal and financial obligations of the Authority.

**8 TERMINATION**

If the Supplier is in material Default under any of its obligations under this Annex 1 of this Schedule 11 (*Data Protection and Governance*), the Authority shall be entitled to terminate this Agreement by issuing a Termination Notice to the Supplier in accordance with Clause 29 (*Termination Rights*).

## 9 SUB-PROCESSING

9.1 In respect of any processing of Personal Data performed by a third party (which may include but is not limited to a Sub-contractor of the Supplier) on behalf of a Party, that Party shall:

(a) carry out adequate due diligence on such third party to ensure that it is capable of providing the level of protection for the Personal Data as is required by this Agreement, and provide evidence of such due diligence to the other Party where reasonably requested; and

(b) ensure that a suitable agreement is in place with the third party as required under applicable Data Protection Legislation.

## 10 DATA RETENTION

The Parties agree to erase Personal Data from any computers, storage devices and storage media that are to be retained as soon as practicable after it has ceased to be necessary for them to retain such Personal Data under applicable Data Protection Legislation and in accordance with Annex 2 of this Schedule 11 (*Data Protection and Governance*) (save to the extent (and for the limited period) that such information needs to be retained by a Party for statutory compliance purposes or as otherwise required by this Agreement), and taking all further actions as may be necessary to ensure its compliance with Data Protection Legislation.

**ANNEX 2: Data Retention Periods**

1. The Supplier, when acting as Processor shall, and shall ensure that any Sub-processor shall, comply with the data retention periods set out in the Authority's Data Retention Policy, a copy of which is attached to this Annex 2 of this Schedule 11 (*Data Protection and Governance*).

2. While the Data Retention Policy attached to this Annex 2 of this Schedule 11 (*Data Protection and Governance*) is the most up to date version as at the Signature Date, the Parties acknowledge that the Data Retention Policy is subject to change as per the review process set out in the Data Retention Policy. Where such a review:

   (a) results in any changes to, or a further version of, the Data Retention Policy, the Authority shall provide the Supplier with written notice of such change, together with a copy of the latest version which the Supplier shall follow from the time of such notice being received;

   (b) gives rise to a Contract Change, that change shall be subject to the Change Control Procedure.

## ANNEX 3: Data Governance

### PART ONE: DATA WORKING GROUP TERMS OF REFERENCE - REDACTED

### PART TWO: AFRP DATA GOVERNANCE ORGANISATION CHART AND ESCALATION ROUTE - REDACTED