SCHEDULE B - SPECIFICATION REQUIREMENTS FOR E-BULK DATA PROCESSOR

1 BACKGROUND

1.1 The Disclosure and Barring Service (DBS) was established under the Protection of Freedoms Act 2012 and carries out the functions previously undertaken by the Criminal Records Bureau (DBS) and Independent Safeguarding Authority (ISA). The DBS became operational on the 1st December 2012.

1.2 The primary role of the DBS is to help employers in England and Wales make safer recruitment decisions and prevent unsuitable people from working with vulnerable groups including children.

2 E-BULK SERVICE

2.1 As part of DBS's business strategy, there is an objective for DBS's services to be accessible via electronic channels, wherever this is practical. As a result, DBS has established an electronic interface for submitting applications to its Service. This electronic interface is known as the "E-Bulk Service".

2.2 The E-Bulk Service allows the electronic transfer of multiple applications to DBS so that Registered Bodies (RBs) can avoid the processing of paper application forms. The E-Bulk Service is available to RBs who have the capability and capacity to submit in excess of 3,000 individual applications in any rolling 12 month period.

2.3 A secure internet connection is required, both to submit applications via the E-Bulk Service and to receive the results of these applications, when relevant checks have been carried out by DBS representatives.

2.4 **ANNEX A** provides for a **High Level Process Flowchart** illustrating the distinct processes and stakeholder interfaces which occur when operating the E-Bulk Service.

3 ROLE OF THE CONTRACTOR

3.1 Subject to approval by DBS, the CONTRACTOR shall be responsible for processing sensitive data, which is defined as any action taken with personal data including the collection, use, destruction and holding of data on behalf of DBSDBS and/or its appointed representatives.

3.2 The CONTRACTOR shall either be a Registered Body (RB) or another third party organisation employed or appointed by an RB to handle sensitive criminal records data on its behalf and, ultimately, on behalf of the DBS, to which it shall be contractually accountable.

4 SECURITY REQUIREMENTS

4.1 When processing data on behalf of DBS, the CONTRACTOR shall identify and comply with all specific security provisions in accordance with the Data Protection Act 1998.

4.2 In all circumstances where data is to be processed from outside of the UK mainland, the CONTRACTOR shall obtain prior written consent from DBS, such consent not to be unreasonably withheld.

4.3 In addition, where operating the data processing activities from outside of the UK mainland, the CONTRACTOR shall be required to implement auditable measures, as required by the Data Protection Act. The CONTRACTOR shall implement the auditable measures prior to commencement of the data processing activities.

4.4 **Physical Security Requirements:** The CONTRACTOR shall be required to have in place security measures and shall effectively manage the relevant risks which pertain to the personal data being processed. For the avoidance of doubt, physical measures shall include but shall not be limited to:

a) Boundary protection from external physical threats;

b) Effective compartmentalisation of internal physical fabric to enforce Need To Know (NTK);

c) Effective use of technological barriers such that incidents can be identified and treated quickly; and

d) Provision of controls that all users are properly identified and duly authorised to discharge their work.

4.5 **Communications:** The CONTRACTOR shall ensure that ALL communications with subcontractors, third parties and clients are protected with measures to protect the confidentiality, integrity and availability of the personal data. For the avoidance of any doubt, these measures shall include encryption.

4.6 **Systems Development:** When developing a new capability, the CONTRACTOR shall ensure that developmental governance is in place to manage the additional risks. Such governance infrastructure shall be in line with ISO27001 certification/ compliance.

4.7 **Shared Services:** The CONTRACTOR will be required to notify the DBS of any aspect of its service that is shared with any other service provider and must provide specific assurances that the additional risks arising from any shared service provision are effectively managed.

4.8 **Reporting:** The CONTRACTOR shall provide, upon request, to DBS such reports, as may be required from time to time, on the status of its security arrangements when undertaking data processing activities on behalf of DBS.

4.9 **Need to Know:** The CONTRACTOR shall not permit any person who has not been authorised to access business material containing personal information.

4.10 The CONTRACTOR shall implement business processes, including relevant checks and balances, to prevent unauthorised personnel from accessing the sensitive criminal records data.

4.11 The CONTRACTOR shall provide protection to seek to ensure that any access to its facilities and technical infrastructure is strictly limited to such portion of the same as is required for the proper performance of its obligations.

4.12 **Provenance Checks:** The CONTRACTOR shall ensure that thorough and effective background checks are carried out on all personnel performing the data processing activities.

4.13 When undertaking background checks, the CONTRACTOR shall ensure that its personnel are suitable to work with sensitive criminal records data and have a legitimate right to work in the territory where the activities are being discharged.

4.14 **Change Control:** The CONTRACTOR shall have suitable change control processes in place, such that all proposed changes are impact assessed for their security impact and treated accordingly, prior to implementation.

4.15 **Incident Handling:** The CONTRACTOR shall provide, upon request, such information as may be required for the purpose of allowing DBS to undertake investigations for the purpose of checking compliance with the Contract.

4.16 If the CONTRACTOR becomes aware of any contravention of the data security requirements of DBS, or of any unauthorised access by its personnel or other connected parties, the CONTRACTOR shall:

a) Report such incidents to DBS immediately;

b) Describe in full detail any accessed material;

c) Return to DBS any copied or removed material; and

d) Comply with all directions and requests made by the DBS.

4.17 If a security incident occurs, the CONTRACTOR shall carry out an immediate investigation into the incident and initiate corrective actions to minimise any reoccurrence. The CONTRACTOR shall retain all documentation for the investigation of the violation and provide copies to DBS immediately upon request.

4.18 **ISO27001:** The CONTRACTOR shall be ISO/IEC 27001 certified/ compliant, with a scope that is appropriate to the provision of handling sensitive criminal records data. The CONTRACTOR shall maintain certification/compliance to ISO/IEC 27001 in the development and operation of all future IT systems specific to the handling of the sensitive criminal records data. Compliance shall be supported by an independent external audit. Security policies shall be made available to the DBS and immediately upon request.

4.19 Following review of the security policies, the DBS may provide review comments and/or suggest areas for improvement. The CONTRACTOR shall address all points, recommendations and/ or concerns raised by DBS.

4.20 The CONTRACTOR shall subject the IT environment to regular IT Security Health Checks in line with its obligations under ISO27001. Reports and treatment plans must be made available to the DBS upon immediate request.

4.21 The CONTRACTOR shall appoint a senior board level executive with permanent and dedicated responsibilities for security requirements.

4.22 The CONTRACTOR shall comply with the relevant aspects of UK Government security policies relating to data protection when processing sensitive criminal records data.

4.23 The CONTRACTOR shall provide assurances to the complete satisfaction of DBS that its solution complies with the provisions of the Data Protection Act 1998.

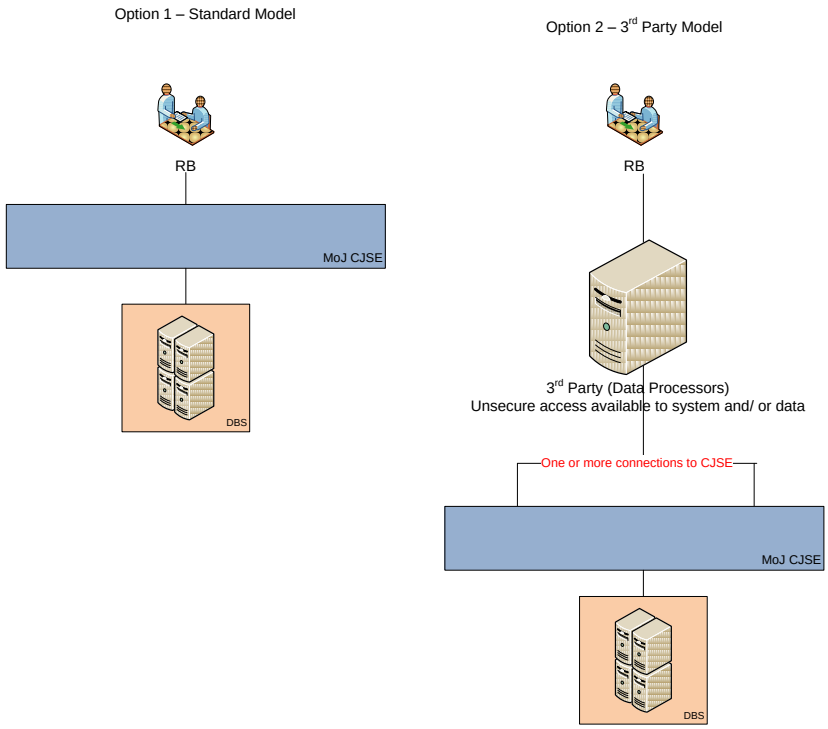
4.24 The CONTRACTOR shall establish and maintain safeguards against the destruction, compromise, loss or alteration of DBS data in its possession.

4.25 DBS may, from time to time and at its sole discretion, convene a meeting of a dedicated security management board to monitor and review the management of security by the CONTRACTOR and to discuss and resolve security issues and share information. The CONTRACTOR shall comply with all requests to participate as directed in such meetings and at their own cost.

4.26 The CONTRACTOR shall implement a secure service IT environment which is commensurate with the value of the personal data in the context of the threats.

4.27 **ISO22301:** The CONTRACTOR shall be ISO22301 certified/ compliant with a scope that is appropriate to the handling of sensitive criminal records data. Compliance must be supported by an independent external audit. Business Continuity Management policies shall be provided to DBS upon immediate request.

ANNEX A – HIGH LEVEL PROCESS FLOWCHART



Option 1 illustrates a connection to DBS through CJSE using a direct link controlled and managed by the RB.

Option 2 illustrates a connection to DBS through CJSE utilising a 3rd party supplier/ data processor between the RB and CJSE.