SCHEDULE 25:

DATA PROTECTION

CONTENTS

1. **General**

[Note to Bidders: It is expected that the Contractor will act in the following roles: (1) as a processor, acting on behalf of the Authority or a Relevant Organisation, (2) as a controller in its own right, processing personal data obtained in the course of this Contract for its own purpose, determining the means and manner of such processing, (3) as a controller acting in common with the Authority or a Relevant Organisation processing the same personal data as the Authority or a Relevant Organisation, but determining itself the means and manner of such processing, and (4) as a joint controller, processing the same personal data as the Authority or a Relevant Organisation and determining together with the Authority or a Relevant Organisation the means and manner of such processing.

Where submitting a bid, bidders (1) understand that it will be expected to enter into the terms set out in this Schedule and are expected to comply with all relevant Data Protection Legislation in respect of each of the four arrangements set out above and (2) acknowledge and agree that the factual circumstances dictate at which point it will fall into which of the four arrangements set out above and they are expected as part of the contractual process to work with the Authority and Relevant Organisation to document the different scenarios where it will be captured by each of these arrangements, including (without limitation) (a) participating in data mapping exercises, (b) supporting the Authority in completing this data protection Schedule (in particular, this paragraph 1 and the data protection particulars within the Appendix), (c) putting in place subsequent data sharing agreements and privacy notices as required by the Authority or as necessary to comply with its legal duties where acting as a controller and (d) comply with the Authority's Policies, including without limitation the Prison Service Instructions]

1.1 The Parties acknowledge that for the purpose of this Contract, the Authority and each Relevant Organisation may be a Data Controller for the purpose of the Data Protection Legislation and the Originating Controller (as defined in **paragraph 2.3 (Data Sharing Obligations)**), as applicable in relation to the Personal Data being processed. For the purpose of this Contract the Authority is appointed to act for and on behalf of itself and the Relevant Organisations to provide instructions and to manage the relationship with the Contractor in relation to the provision of the Services and in doing so the processing of Personal Data. Without prejudice to any other term of this Contract, the Relevant Organisation(s) shall, to the extent applicable, take the benefit of this **Schedule 25 (Data Protection)** and the Contractor acknowledges and agrees that it shall comply with its obligations set out in this Schedule for the benefit of the Authority and each Relevant Organisation. In respect of any obligation(s) which are required to be performed by the Authority, the Authority shall ensure that the Authority or as applicable the Relevant Organisation performs such obligation(s). For the avoidance of doubt any Loss suffered or incurred by a Relevant Organisation due to a breach of this Schedule shall be considered a Direct Loss of the Authority and the Authority shall be able to recover the same under and in accordance with the terms of this Contract.

1.2 Each of the Parties including the personnel of each Party (personnel shall include directors, officers, employees, servants, agents, consultants, suppliers and sub-contractors) will comply with all applicable requirements of the Data Protection Legislation and shall not knowingly or negligently by any act or omission, place the other Party in breach, or potential breach of Data Protection Legislation. This **paragraph 1.2 (General)** is in addition to and does not relieve, remove or replace a Party's obligations under the Data Protection Legislation.

1.3 The Parties shall each Process Personal Data. The Parties acknowledge that the factual arrangements between them dictate the role of each Party in respect of the Data Protection Legislation. The Parties agree that they shall be:

1.3.1 Joint Data Controllers (Processing the same Personal Data as the other Party (or the Relevant Organisation) and determining together with the other Party (or the Relevant Organisation) the means and manner of such processing);

1.3.2 Data Controllers (Processing the same, or a common set of Personal Data as the other Party (or the Relevant Organisation), but determining itself the means and manner of such Processing); or

1.3.3 Data Controllers (acting independently of the other Party (or the Relevant Organisations), by way of Processing the Personal Data obtained in the course of this Contract for its own purpose, and determining itself the means and manner of such Processing); and/or

1.3.4 in some circumstances the Contractor shall act as Data Processor for and on behalf of the Authority.

The roles of each Party in relation to the Personal Data being processed under and in accordance with this Contract is as set out in the data maps contained at Appendix 1.

1.4 The Parties agree to take account of any guidance issued by the Information Commissioner's Office. The Authority may on not less than thirty (30) Business Days' notice to the Contractor amend this Contract to ensure that it complies with any guidance issued by the Information Commissioner's Office.

1.5 The Parties agree to take account of any data sharing agreement , protocol or Authority Policy (including without limitation the Prison Service Instructions, Prison Service Orders or Policy Frameworks) issued by the Authority or any Relevant Organisation or Government Department which provides for the processing and sharing of Personal Data between the

Authority, a Relevant Organisation and each other and the Contractor agrees, where required, the Authority may, at any time on not less than thirty (30) Business Days' notice, amend this Contract to ensure that it complies with any terms of such data sharing agreement, protocol or Authority Policy.

1.6 Within one (1) Month following the Commencement Date, the Contractor shall provide to the Authority details of how it plans to comply with its obligations under this **Schedule 25 (Data Protection)** and its obligations under Data Protection Legislation, including:

1.6.1 copies of data sharing agreements and all necessary agreements and arrangements and an update as to the status of such agreements and arrangements;

1.6.2 an updated, comprehensive and fully completed copy of the data map contained at **Appendix 1 to this Schedule 25 (Data Protection)**;

1.6.3 a copy of the fair processing notices the Contractor is mandated to provide pursuant to Data Protection Legislation and this **Schedule 25 (Data Protection)**,

(the "**Data Protection Roadmap**")

1.7 Within twenty (20) Business Days of receipt of the Data Protection Roadmap, the Authority shall either confirm its acceptance of the Data Protection Roadmap, or mandate amendments to the Data Protection Roadmap, to the extent required to ensure compliance with the Data Protection Legislation and this **Schedule 25 (Data Protection)**. In mandating such changes to the Data Protection Roadmap, the Authority shall act reasonably and in good faith.

1.8 The Contractor shall maintain the Data Protection Roadmap for the duration of the Contract and shall notify the Authority of any proposed changes to the Data Protection Roadmap within five (5) Business Days of proposing such change, following which the process in **paragraph 1.7** shall apply. Regardless of any changes to the Data Protection Roadmap, the Contractor shall be subject to, comply with and give full attention and support to an annual compliance and assurance process, carried out by the Authority. To the extent the Authority is not satisfied with the outcome of such annual compliance and assurance process, the Contractor shall allow for audit by the Authority and/or its designated auditor, in respect of compliance with Data Protection Legislation and this **Schedule 25 (Data Protection)**.

2. **Data Sharing Obligations**

2.1 The Parties each acknowledge and agree that they may need to Process Personal Data relating to each Party's representatives (in their respective capacities as Data Controllers) in order to (as appropriate): (a) administer and provide the Services; (b) request and receive the Services; (c) compile, dispatch and manage the payment of invoices relating to the Services; (d) manage the Contract and resolve any disputes relating to it; (e) respond and/or raise general queries relating to the Service; and (f) comply with their respective obligations.

2.2 Each Party shall Process such Personal Data relating to each Party's representatives for the purposes set out in **paragraph 2.1 (Data Sharing Obligations)** in accordance with their own privacy policies. The Parties acknowledge that they may be required to share Personal Data with their Affiliates, group companies and other relevant parties, within or outside of the country of origin, in order to carry out the activities listed in **paragraph 2.1 (Data Sharing Obligations)**, and in doing so each Party will ensure that the sharing and use of this Personal Data complies with applicable Data Protection Legislation.

2.3 Save in relation to contact Personal Data processed by the Parties in accordance with **paragraph 2.1 (Data Sharing Obligations)**, where and to the extent the Contractor is acting as a Data Controller (except as a Joint Data Controller, in which case **paragraph 2.4** shall apply), and Processing Personal Data in its provision of the Services and compliance with its obligations under this Contract the conditions set out in this **paragraph 2.3 (Data Sharing Obligations)** shall apply. For the purpose of this **paragraph 2 (Data Sharing Obligations)**, the Party from whom the Personal Data originates shall also be referred to as the Originating Controller.

2.3.1 The Contractor shall:

2.3.1.1 only Process the Personal Data for the Permitted Purpose (as defined in **Part 1** of **Appendix 1** to this **Schedule 25 (Data Protection)**);

2.3.1.2 make due notification to the Information Commissioner's Office (or other such regulatory authority as required by Data Protection Legislation), including in relation to its use and Processing of the Personal Data and comply at all times with the Data Protection Legislation;

2.3.1.3 ensure that all fair processing notices have been given (and/or, as applicable, consents obtained) to the relevant Data Subjects, within one (1) month of obtaining the Personal Data and are in accordance

with the requirements of the Data Protection Legislation, Authority Policies, and/or any templates, guidance or instructions of the Authority and/or (where applicable) Originating Controller;

2.3.1.4 maintain complete and accurate records and information to demonstrate its compliance with this **paragraph 2.3 (Data Sharing Obligations)**. This requirement does not apply where the Contractor employs fewer than 250 staff, unless:

(a) the Originating Controller determines that the Processing is not occasional;

(b) the Originating Controller determines 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; or

(c) the Originating Controller determines that the Processing is likely to result in a risk to the rights and freedoms of Data Subjects;

2.3.1.5 prepare and/or support the Originating Controller (as applicable) in preparing, any Data Protection Impact Assessment prior to commencing any Processing;

2.3.1.6 ensure that it has in place Protective Measures, which are appropriate to protect against a Data Loss Event, which the Originating Controller may reasonably reject (but failure to reject shall not amount to approval by the Originating Controller of the adequacy of the Protective Measures), having taken account of the:

(a) nature of the data to be protected;

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

(c) state of technological development; and

(d) cost of implementing any measures;

2.3.1.7 not transfer Personal Data to a Restricted Country unless the prior written consent of the Originating Controller has been obtained and the following conditions are fulfilled:

(a) the Contractor has provided appropriate safeguards in relation to the transfer (in accordance with the Data Protection Legislation) as determined by the Originating Controller;

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

(c) the Contractor complies with its obligations under the Data Protection Legislation by providing an adequate level of protection to any Personal Data that is transferred; and

(d) the Contractor complies with any reasonable instructions notified to it in advance by the Originating Controller with respect to the Processing of the Personal Data;

2.3.1.8 subject to **paragraph 2.3.1.9 (Data Sharing Obligations),** the Contractor shall notify the Originating Controller immediately if it:

(a) receives a Data Subject Request (or purported Data Subject 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's Office or any other regulatory authority (including a supervisory authority as defined in the Data Protection Legislation) in connection with Personal Data Processed under this Contract; or

(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 Legislation; or becomes aware of a Data Loss Event;

2.3.1.9 The Originating Controller shall determine and confirm to the Contractor whether it or the Contractor shall be the primary point of contact and responder to the request, complaint or communication received pursuant to **paragraph 2.3.1.8 (Data Sharing Obligations)** and the parties shall ensure this is reflected within the relevant fair processing notices provided to Data Subjects. Where the Originating Controller:

(a) designates the Contractor as the primary point of contact, the Contractor shall provide updates and further information to the Originating Controller, including (where directed by the Originating Controller) allowing the Originating Controller to have final oversight and approval of any response, prior to such response being released to the relevant party;

(b) designates itself as the primary point of contact, the Contractor shall provide all support as necessary within the timescales directed by the Originating Controller, including providing all Personal Data held by the Contractor in respect of the request, complaint or communication received to the Originating Controller as soon as practicable and in any event within five (5) days, or as otherwise agreed by the parties acting reasonably and in good faith;

2.3.1.10 the Contractor's obligation to notify under **paragraph 2.3.1.8 (Data Sharing Obligations)** shall include the provision of further information to the Originating Controller in phases, as details become available. The Contractor shall be the primary point of contact for any communication in respect of the Data Loss Event and: (a) the Contractor shall act quickly to remedy a Data Loss Event and minimise the impact(s) of a Data Loss Event; and (b) the Contractor, the Originating Controller and where relevant the Authority shall work together (acting reasonably and in good faith) to formulate responses, notifications and other communications in respect of the Data Loss Event;

2.3.1.11 take reasonable steps to ensure the reliability of and adequate training of, any personnel who have access to the Personal Data;

2.3.1.12 hold the information contained in the Personal Data confidentially; and

2.3.1.13 not do anything which shall damage the reputation of its (if applicable) or the Originating Controller's (or the Authority, where the Authority is not the Originating Controller) relationship with the Data Subjects.

2.3.2 Where acting as a Data Controller for the purposes of the Personal Data, the Originating Controller shall:

2.3.2.1 ensure that all fair processing notices have been given (and/or, as applicable, consents obtained), and are sufficient in scope to allow the Originating Controller to disclose the Personal Data to the Contractor in accordance with the Data Protection Legislation and for the purposes set out in the Contract; and

2.3.2.2 ensure that all Personal Data disclosed or transferred to, or accessed by, the Contractor is accurate and up-to-date, as well as adequate, relevant and not excessive to enable the Contractor to Process the Personal Data, for the Permitted Purpose.

2.3.3 For the purposes of **paragraph 2.3.2.1,** at the discretion and instruction of the Authority and/or Originating Controller, the Contractor shall support the Originating Authority and/or provide on the Originating Controller's behalf, all fair processing notices to the relevant Data Subjects (and/or as applicable, obtain the necessary consents of such Data Subjects), within a reasonable time frame to be determined and provided by the Authority and/or Originating Controller.

2.3.4 Each Party warrants, represents and undertakes that it is not subject to any prohibition or restriction which would prevent or restrict it from disclosing or transferring the relevant Personal Data (as applicable) to the other party in accordance with the terms of this Contract.

2.4 Where and to the extent the Contractor is acting as a Joint Data Controller with another party (being the Authority and/or a Relevant Organisation) the conditions set out in this **paragraph 2.4 (Data Sharing Obligations)** shall apply.

2.4.1 Each Party shall:

2.4.1.1 collaboratively ensure that all fair processing notices have been given (and/or, as applicable, consents obtained), and are sufficient in scope

to allow the envisaged Processing in accordance with the Data Protection Legislation and for the purposes set out in the Contract. For the purposes of this **paragraph 2.4.1.1** the Authority and/or Relevant Organisation shall have the final approval and oversight as to whether it or the Contractor is to provide any relevant fair processing notice and/or as applicable, obtain necessary consents, on behalf of both parties;

2.4.1.2 make due notification to the Information Commissioner's Office (or other such regulatory authority as required by Data Protection Legislation), including in relation to its use and Processing of the Personal Data and comply at all times with the Data Protection Legislation;

2.4.1.3 maintain complete and accurate records and information to demonstrate its compliance with this **paragraph 2.4 (Data Sharing Obligations)**. This requirement does not apply where the Party employs fewer than 250 staff, unless:

(a) any of the Parties determine that the Processing is not occasional;

(b) any of the Parties determine 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; or

(c) any of the Parties determine that the Processing is likely to result in a risk to the rights and freedoms of Data Subjects;

2.4.1.4 work together (acting reasonably and in good faith) in the preparation of any Data Protection Impact Assessment prior to commencing any Processing;

2.4.1.5 where the Personal Data has been transmitted by it, or is in its possession or control, ensure that it has in place Protective Measures, which are appropriate to protect against a Data Loss Event, having taken account of the:

(a) nature of the data to be protected;

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

(c) state of technological development; and

(d) cost of implementing any measures;

2.4.1.6 subject to **paragraph 2.4.2 (Data Sharing Obligations)** notify the other promptly (and in any event within twenty-four (24) hours) if it:

(a) receives a Data Subject Request (or purported Data Subject 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's Office or any other regulatory authority (including a supervisory authority as defined in the Data Protection Legislation) in connection with Personal Data Processed under this Contract; or

(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 Legislation.

2.4.2 Each Party's obligation to notify under **paragraph 2.4.1.6 (Data Sharing Obligations)** shall include the provision of further information in phases, as details become available. The Authority and/or Relevant Organisation shall determine and confirm to the Contractor whether it or the Contractor shall be the primary point of contact and responder to the request, complaint or communication received pursuant to **paragraph 2.4.1.6 (Data Sharing Obligations)** and the parties shall ensure this is reflected within the relevant fair processing notices provided to Data Subjects. Where the Authority and/or Relevant Organisation:

2.4.2.1 designates the Contractor as the primary point of contact, the Contractor shall provide updates and further information to the Authority and/or Relevant Organisation, including (where directed by the Authority and/ or Relevant Organisation) allowing the Authority and/or Relevant Organisation to have final oversight and approval of

any response, prior to such response being released to the relevant party;

2.4.2.2 designates itself as the primary point of contact, the Contractor shall provide all support as necessary within the timescales directed by the Authority and/or Relevant Organisation, including providing all Personal Data held by the Contractor in respect of the request, complaint or communication received to the Authority and/or Relevant Organisation as soon as practicable and in any event within five (5) days, or as otherwise agreed by the parties acting reasonably and in good faith.

2.4.3 Before further sharing the Personal Data with a third party (including using a Processor or any Sub-processor to Process any Personal Data related to this Contract), the Contractor must:

2.4.3.1 notify the Originating Controller in writing of the intended third party (including any Processor and/or Sub-processor) and Processing;

2.4.3.2 obtain the written consent of the Originating Controller;

2.4.3.3 enter into a written contract with the third party (including any Processor and/or Sub-processor) which give effect to the terms set out in this Schedule (as applicable); and

2.4.3.4 provide the Originating Controller with such information regarding the third party as the Originating Controller may reasonably require.

2.4.4 The Contractor shall remain fully liable for all acts or omissions of any third party to which it transfers the relevant Personal Data.

3. **Processor Obligations**

For the purposes of this **paragraph 3 (Processor Obligations)**, a reference to the "Data Controller" shall be a reference to the Authority or the Relevant Organisation as the context dictates.

3.1 Where and to the extent the Contractor is acting as a Processor, the conditions set out in this **paragraph 3 (Processor Obligations)** shall apply.

3.2 The only Processing that the Processor is authorised to do is listed in **Part 2** of **Appendix 1** to this **Schedule 25 (Data Protection)** by the Data Controller and may not be determined by the Processor.

3.3 The Processor shall notify the Data Controller immediately if it considers that any of the Data Controller's instructions infringe the Data Protection Legislation.

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

3.4.1 a systematic description of the envisaged Processing operations and the purpose of the Processing;

3.4.2 an assessment of the necessity and proportionality of the Processing operations in relation to the Services;

3.4.3 an assessment of the risks to the rights and freedoms of Data Subjects; and

3.4.4 the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of Personal Data.

3.5 The Processor shall, in relation to any Personal Data Processed in connection with its obligations under this Contract:

3.5.1 Process that Personal Data only in accordance with **Part 2** of **Appendix 1** to this **Schedule 25 (Data Protection)** unless the Processor is required to do otherwise by Legislation. If it is so required the Processor shall promptly notify the Data Controller before Processing the Personal Data unless prohibited by Legislation;

3.5.2 ensure that it has in place Protective Measures, which are appropriate to protect against a Data Loss Event, which the Data Controller may reasonably reject (but failure to reject shall not amount to approval by the Data Controller of the adequacy of the Protective Measures), having taken account of the:

3.5.2.1 nature of the data to be protected;

3.5.2.2 harm that might result from a Data Loss Event;

3.5.2.3 state of technological development; and

3.5.2.4 cost of implementing any measures;

3.5.3 ensure that:

3.5.3.1 the Processor Personnel do not Process Personal Data except in accordance with this Contract (and in particular **Part 2** of **Appendix 1** to this **Schedule 25 (Data Protection)**);

3.5.3.2 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 **paragraph 3 (Processor Obligations)**;

(b) are subject to appropriate confidentiality undertakings with the Processor or any Sub-processor;

(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 Data Controller or as otherwise permitted by this Contract; and

(d) have undergone adequate training in the use, care, protection and handling of Personal Data; and

3.5.3.3 not transfer Personal Data to a Restricted Country unless the prior written consent of the Data Controller has been obtained and the following conditions are fulfilled:

(a) the Data Controller or the Processor has provided appropriate safeguards in relation to the transfer (in accordance with the Data Protection Legislation) as determined by the Data Controller;

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

(c) 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 Data Controller in meeting its obligations);

(d) the Processor complies with any reasonable instructions notified to it in advance by the Data Controller with respect to the Processing of the Personal Data; and

(e) at the written direction of the Data Controller, delete or return Personal Data (and any copies of it) to the Data Controller on termination of the Contract unless the Processor is required by Legislation to retain the Personal Data.

3.5.4 Subject to **paragraph 3.5.5 (Processor Obligations)**, the Processor shall notify the Data Controller immediately if it:

3.5.4.1 receives a Data Subject Request (or purported Data Subject Request);

3.5.4.2 receives a request to rectify, block or erase any Personal Data;

3.5.4.3 receives any other request, complaint or communication relating to either Party's obligations under the Data Protection Legislation;

3.5.4.4 receives any communication from the Information Commissioner's Office or any other regulatory authority (including a supervisory authority as defined in the Data Protection Legislation) in connection with Personal Data Processed under this Contract;

3.5.4.5 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 Legislation; or

3.5.4.6 becomes aware of a Data Loss Event.

3.5.5 The Processor's obligation to notify under **paragraph 3.5.4 (Processor Obligations)** shall include the provision of further information to the Data Controller in phases, as details become available. The Data Controller shall either, at its sole election: (a) assume full control of the responses to the events set out in **paragraph 3.5.4 (Processor Obligations)**; or (b) direct the Processor in its response, save where the Processor is required to act quickly and solely within its internal business to minimise the impact(s) of a Data Loss Event.

3.5.6 Taking into account the nature of the Processing, the Processor shall provide the Data Controller with full assistance in relation to either Party's obligations under Data Protection Legislation and any complaint, communication or request made under **paragraph 3.5.4 (Processor Obligations)** (and insofar as possible within the

timescales reasonably required by the Data Controller) including by promptly providing:

3.5.6.1 the Data Controller with full details and copies of the complaint, communication or request;

3.5.6.2 such assistance as is reasonably requested by the Data Controller to enable the Data Controller to comply with a Data Subject Request within the relevant timescales set out in the Data Protection Legislation;

3.5.6.3 the Data Controller, at its request, with any Personal Data it holds in relation to a Data Subject;

3.5.6.4 assistance as requested by the Data Controller following any Data Loss Event; and

3.5.6.5 assistance as requested by the Data Controller with respect to any request from the Information Commissioner's Office, or any consultation by the Data Controller with the Information Commissioner's Office.

3.5.7 The Processor shall maintain complete and accurate records and information to demonstrate its compliance with this **paragraph 3 (Processor Obligations)**. This requirement does not apply where the Processor employs fewer than 250 staff, unless:

3.5.7.1 the Data Controller determines that the Processing is not occasional;

3.5.7.2 the Data Controller determines 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; or

3.5.7.3 the Data Controller determines that the Processing is likely to result in a risk to the rights and freedoms of Data Subjects.

3.5.8 The Processor shall allow for audits of its Data Processing activity by the Data Controller or the Data Controller's designated auditor.

3.5.9 Each Party shall designate its own data protection officer if required by the Data Protection Legislation.

3.5.10 Before allowing any Sub-processor to Process any Personal Data related to this Contract, the Processor must:

3.5.10.1 notify the Data Controller in writing of the intended Sub-processor and processing;

3.5.10.2 obtain the written consent of the Data Controller;

3.5.10.3 enter into a written contract with the Sub-processor which give effect to the terms set out in this **paragraph 3 (Processor Obligations)** such that they apply to the Sub-processor; and

3.5.10.4 provide the Data Controller with such information regarding the Sub-processor as the Data Controller may reasonably require.

3.5.11 The Processor shall remain fully liable for all acts or omissions of any of its Sub-processors.

3.5.12 The Data Controller may, at any time on not less than thirty (30) Business Days' notice, revise this **paragraph 3 (Processor Obligations)** by replacing it with any applicable controller to processor standard clauses or similar terms forming part of an applicable certification scheme (designated as such pursuant to Data Protection Legislation) (which shall apply when incorporated by attachment to this Contract).

3.5.13 The Parties agree to take account of any guidance issued by the Information Commissioner's Office. The Data Controller may on not less than thirty (30) Business Days' notice to the Processor amend this Contract to ensure that it complies with any guidance issued by the Information Commissioner's Office.

3.5.14 The Parties agree to take account of any data processing agreement or protocol issued by the Authority or any Relevant Organisation or Government Department which provides for the Processing of Personal Data between the Authority and/or a Relevant Organisation and the Contractor agrees, where required, the Authority may, at any time on not less than thirty (30) Business Days' notice, amend this Contract to ensure that it complies with any terms of such data processing agreement or protocol.

4. **Data Processed For Law Enforcement Purposes**

4.1 In relation to Personal Data processed for Law Enforcement Purposes, the Contractor shall:

4.1.1 maintain logs for its processing operations in respect of:

4.1.1.1 collection;

4.1.1.2 alteration;

4.1.1.3 consultation;

4.1.1.4 disclosure (including transfers);

4.1.1.5 combination; and

4.1.1.6 erasure,

(together the "**Logs**");

4.1.2 ensure that:

4.1.2.1 the Logs of consultation make it possible to establish the justification for, and date and time of, the consultation; and as far as possible, the identity of the person who consulted the data;

4.1.2.2 the Logs of disclosure make it possible to establish the justification for, and date and time of, the disclosure; and the identity of the recipients of the data; and

4.1.2.3 the Logs are made available to the Information Commissioner's Office on request;

4.1.3 use the Logs only to:

4.1.3.1 verify the lawfulness of processing;

4.1.3.2 assist with self-monitoring by the Authority and/or Relevant Organisation or (as the case may be) the Supplier, including the conduct of internal disciplinary proceedings;

4.1.3.3 ensure the integrity of Personal Data; and

4.1.3.4 assist with criminal proceedings;

4.1.4 as far as possible, distinguish between Personal Data based on fact and Personal Data based on personal assessments; and

4.1.5 where relevant and as far as possible, maintain a clear distinction between Personal Data relating to different categories of Data Subject, for example:

4.1.5.1 persons suspected of having committed or being about to commit a criminal offence;

4.1.5.2 persons convicted of a criminal offence;

4.1.5.3 persons who are or maybe victims of a criminal offence; and

4.1.5.4 witnesses or other persons with information about offences.

5. **Indemnity**

Notwithstanding any other term of the Contract, the Contractor shall indemnify and keep indemnified and hold harmless the Authority or the Relevant Organisation (as applicable) and from and against all Losses suffered or incurred by the Authority or the Relevant Organisation (as applicable) arising out of or in connection with claims and proceedings arising from any breach of the Contractor's obligations under this **Schedule 25 (Data Protection).**

6. **Compensation**

6.1 To the extent that the Contractor has an entitlement under Data Protection Legislation to claim from the Authority or a Relevant Organisation (as applicable) compensation paid by the Contractor to a Data Subject or third party as a result of a breach of Data Protection Legislation (in full or in part) by the Authority or a Relevant Organisation (as applicable), the Authority or Relevant Organisation (as applicable) shall be liable only for such amount as directly relates to the Authority's or Relevant Organisation's (as applicable) responsibility for any damage caused to the relevant Data Subject or third party. For the avoidance of doubt the Authority or Relevant Organisation (as applicable) shall only be liable to make payment to the Contractor under this **paragraph 6.1 (Compensation)** upon receipt of evidence from the Contractor, which shall be to the Authority's or Relevant Organisation's (as applicable) reasonable satisfaction and that clearly demonstrates:

6.1.1 that the Authority or Relevant Organisation (as applicable) has breached Data Protection Legislation;

6.1.2 that such breach contributed (in part or in full) to the harm caused entitling the relevant Data Subject or third party to receive compensation in accordance with Data Protection Legislation; and

6.1.3 the proportion of responsibility for the harm caused to the relevant Data Subject or third party which is attributable to the Authority or Relevant Organisation (as applicable).

APPENDIX 1

DATA PROTECTION PARTICULARS

PART 1

1. **Schedule of Data Sharing Particulars**

[Note to Bidders: The successful bidder will be expected to work with the Authority in completing this schedule of particulars.]

This **Part 1** to **Appendix 1** of **Schedule 25 (Data Protection)** sets out the data sharing particulars to be completed by the Parties, acting reasonably and in good faith.

Description	**Details**
Data mapping	[Insert data map template]
Permitted Purpose	[**Note to Bidders: This should include the purpose for which the Personal Data will be used**]

PART 2

1. Schedule of Data Processing Particulars

[Note to Bidders: The successful bidder will be expected to work with the Authority in completing this schedule of particulars.]

This **Part 2** to **Appendix 1** of **Schedule 25 (Data Protection)** sets out the data processing particulars to be completed by the Data Controller, who may take account of the view of the Processor(s), however the final decision as to the content of this Schedule shall be with the Data Controller at its absolute discretion.

1.1 The Processor shall comply with any further written instructions with respect to processing by the Data Controller.

1.2 Any such further instructions shall be incorporated into this schedule of data processing particulars.

Description	Details
Data mapping	[Insert data map template]