SCHEDULE 9 – DATA PROTECTION

In this Schedule, in addition to the defined terms set out in Part A1 of the Contract the following words and expressions have the following meanings unless the context otherwise requires:

"Accuracy Data" means Controller Data disclosed by the Service Provider to the Authority correcting or updating any of the Controller Data previously disclosed by the Service Provider to the Authority;

"Adjusted Data" means Controller Data disclosed by the Service Provider to the Authority containing or detailing adjustments required to be made by Applicable Law or by any Supervisory Authority (or any equivalent regulator or body in relation to all or any of the Controller Data) to any Controller Data previously disclosed by the Service Provider to the Authority;

"Applicable Laws" means all laws, regulations, regulatory requirements and codes of practice of any jurisdiction, as amended and in force from time to time which apply to the Authority or the Service Provider as the case may be and/or rights and obligations pursuant to or in relation to this Contract;

"Competent Authority" has the meaning prescribed in Part 3 of the Data Protection Act 2018;

"Contract Personal Data" means Personal Data processed on behalf of the Authority for Law Enforcement Purposes and/or the Personal Data set out or processed for the purposes set out in Annex 1 to this Schedule.

"Controller Data" means Personal Data that is Processed in the course of undertaking the Services for which the Service Provider is a Controller;

"Controller Purpose" means for the purposes as set out in **Annex 3**;

"Data Protection by Design and Default Exercise" means all such steps required to comply Section 57 of the Data Protection Act 2018;

"European Union" and **"EU"** means the European Union as it is made up from time to time;

"Sensitive Data" means the categories of Personal Data described in Section 35(8) of the Data Protection Act 2018; and

"Special Category Personal Data" means the categories of Personal Data described in Article 9(1) GDPR.

the words and expressions set out in

1. AGREEMENT BETWEEN THE PARTIES

1.1 The Parties shall each Process the Authority Data. The Parties acknowledge that the factual arrangement between them dictates the classification of each Party in respect of the Data Protection Laws. Notwithstanding the foregoing, the Parties anticipate that the Authority shall act as a Controller and the Service Provider shall act as a Processor, as follows:

(a) the Authority shall be a Controller where it is Processing the Authority Data in connection with receipt of the Services provided by the Service Provider under the Contract;

(b) the Authority is a Competent Authority for the purposes of the Processing of Personal Data for Law Enforcement Purposes; and

(c) the Service Provider shall be a Processor where it is Processing the Authority Data in relation to the Permitted Purposes (including any Law Enforcement Purposes) in connection with performing its obligations under the Contract.

1.2 Each of the Parties acknowledges and agrees that Annex 1 is an accurate description of the Data Protection Particulars at the Commencement Date.

1.3 The Parties acknowledge that they need to share Personal Data with each other to facilitate the Services being performed by the Service Provider. This is to facilitate Warrants being executed in, and supports the aim of ensuring the actions and directions of the justice system are fulfilled.

1.4 The Service Provider will not Process (including use) Authority Data for any purpose other than providing the Services to the Authority under this Contract, unless such Processing (including use) is Approved in advance.

2. SERVICE PROVIDER OBLIGATIONS

2.1 The Service Provider shall (and shall procure that its Staff) comply with any notification requirements under Data Protection Laws and both Parties will duly observe all their obligations under Data Protection Laws which arise in connection with the Contract.

2.2 The Service Provider will, in conjunction with the Authority, in its own right and in respect of the Services, make all necessary preparations to ensure in particular that it will be compliant with the GDPR and the provisions of Parts 2 and 3 of the Data Protection Act 2018.

2.3 Notwithstanding the obligation in paragraph 2.1, to the extent that the Service Provider is acting as a Processor for and on behalf of the Authority (as the Controller) in relation to the Processing that it is carrying out arising out of, or in connection with, the Permitted Purpose, the Service Provider shall:

(a) Process the Contract Processor Data only on documented instructions (including this Contract) from the Authority (in the event that the Service Provider is lawfully entitled under the Data Protection Laws to Process Contract Processor Data outside the documented instructions of the Authority, it does so as a Controller but only so far as is permitted by the Data Protection Laws);

(b) unless prohibited by Applicable Laws, notify the Authority immediately (and in any event within twenty-four (24) hours of becoming aware of the same) if it considers, in its opinion (acting reasonably) that it is required by Applicable Laws to act other than in accordance with the instructions of the Authority, including where it believes that any of the Authority's instructions under paragraph 2.3(a) infringes any of the Data Protection Laws;

(c) implement and maintain Protective Measures which:

(i) are sufficient to comply with at least the obligations imposed on the Service Provider by the Data Security Requirements;

(ii) have regard to the measures as are set out in clause E1 (Authority Data), clause E7 (Security) and Schedule 8 (Security Requirements);

(iii) are sufficient to secure that any Processing of Contract Processor Data undertaken for the Law Enforcement Purposes will meet the requirements of Part 3 of the Data Protection Act 2018 and will ensure the protection of the rights of Data Subjects; and

(iv) are appropriate to protect against a Data Loss Event having taken account of the:

(1) nature of the data to be protected;

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

(3) state of technological development; and

(4) cost of implementing any measures;

(d) not sub-contract the performance of any of its obligations under this Contract or allow the Processing of Contract Processor Data by any Sub-Contractor and/or Affiliates without Approval in accordance with paragraph 3.1;

(e) not disclose Contract Processor Data to a third party (including a Sub-Contractor) in any circumstances without Approval, from the Authority, save in relation to Third Party Requests where the Service Provider is prohibited by European Union Laws or European

Union member state Laws from notifying the Authority, in which case it shall use reasonable endeavours to advise the Authority in advance of such disclosure and in any event as soon as practicable thereafter;

(f) prior to the Processing of any Contract Processor Data under this Contract and where requested by the Authority provide a Data Protection Impact Assessment to the Authority which will include (but not be limited to):

(i) a systematic description of the envisaged processing operations and the purpose of the Processing;

(ii) an assessment of the necessity and proportionality on the Processing operations in relation to the Services;

(iii) an assessment of the risks to the rights and freedoms of Data Subjects; and

(iv) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of Contract Processor Data and compliance with the Data Security Requirements;

(g) prior to the Processing of any Contract Processor Data for any Law Enforcement Purposes, provide all reasonable assistance to the Authority, where requested, in the undertaking of a Data Protection by Design and Default Exercise;

(h) comply with the obligations imposed upon a Processor under the Data Protection Laws and not perform its obligations under the Contract in such a way as to cause the Authority to breach any of its applicable obligations under the Data Protection Laws;

(i) keep and regularly maintain a record of all categories of Processing activities carried out on behalf of the Authority, containing;

(i) the categories of Processing carried out on behalf of the Authority;

(ii) where applicable, any transfers of Contract Processor Data to Restricted Countries or an international organisation; and

(iii) all other information required under Article 30(2) GDPR,

and provide a copy of such record to the Authority upon its request;

(j) notify the Authority promptly (and in any event within forty-eight (48) hours) following its receipt of any:

(i) Data Subject Request;

(ii) other request, complaint or communication relating to either Party's obligations under the Data Protection Laws;

(iii) request from any third party for disclosure of Contract Processor Data where compliance with such request is required or purported to be required by Applicable Law;

(iv) ICO Correspondence;

(v) any other communication from the ICO or any other Regulatory Body in connection with Personal Data processed under this Contract; and/or

(vi) complaints received from Data Subjects;

(k) and shall:

(i) not disclose any Contract Processor Data in response to any Data Subject

Request, request from a third party or ICO Correspondence without Approval;

(ii) provide the Authority with all reasonable co-operation and assistance required by the Authority in relation to any such Data Subject Request, request from a third party or ICO Correspondence; and

(iii) further to its obligation to notify the Authority under this paragraph 2.3, provide further information to the Authority in phases as details become available.

2.4 The Service Provider shall promptly (and in any event within 3 Working Days of receipt), provide the Authority with full co-operation and assistance in relation to either Party's obligations under Data Protection Laws or any complaint, communication or request made as referred to in paragraph 2.3(j), including by promptly providing:

(a) the Authority with full details and copies of the complaint, communication or request, including details of the Data Subject concerned and the details of the requestor, if different;

(b) where applicable, taking into account the nature of the Processing, assist the Authority by any appropriate means (including appropriate technical and organisation means) to ensure compliance with any Data Subject Request within the relevant timescales set out in the Authority's Data Protection Policy and the Data Protection Laws; and

(c) the Authority, on request by the Authority, with any Contract Processor Data it holds in relation to a Data Subject; and

(d) assistance as required by the Authority with respect to any request from the ICO or any consultation by the Authority with the ICO.

2.5 The Service Provider shall, if requested by the Authority, provide a written description of the measures that it has taken and technical and organisational security measures in place, for the purpose of compliance and requirement / ability to provide assurance with its obligations pursuant to this Schedule and provide to the Authority copies of all documentation relevant to such compliance including, processing records, procedures, guidance, training and manuals.

2.6 The Service Provider shall allow:

(a) the Authority (subject to reasonable and appropriate confidentiality undertakings);

(b) any third party nominated by the Authority (subject to reasonable and appropriate confidentiality undertakings); and

(c) any statutory auditor, including the National Audit Office;

to inspect and audit, in accordance with Clause E9 (Audit), the Service Provider's Personal Data Processing activities (and/or those of Staff), will contribute to such audits and inspections, (which for the avoidance of doubt may be conducted by the Authority or another auditor mandated by the Authority), will make available to the Authority all information and employees necessary to demonstrate compliance with the obligations laid down in the Data Protection Laws and will comply with all reasonable requests or directions by the Authority to enable the Authority and/or any statutory auditor to:

(a) verify and/or procure that the Service Provider is in full compliance with its obligations under the Contract; and

(b) identify the causes of any actual, threatened or 'near-miss' Data Loss Event and any measures that may be implemented to prevent a repeat of the actual, threatened or 'near-miss' Data Loss Event.

2.7 The Service Provider will notify the Authority immediately and in any event no later than 12 hours upon becoming aware of any actual, threatened or 'near-miss' Data Loss Event and in particular the Service Provider will:

(a) adhere to the Data Loss Protocol and reporting procedures as set out in Schedule 10 when notifying the Authority of a Data Loss Event, describe the nature of the event including the categories and approximate number of categories of Personal Data (and details of any Special Category Personal Data and/or Personal Data relating to criminal allegations and/or offences) concerned and the number of Data Subjects affected or potentially affected by the Data Loss Event;

(b) cooperate fully with any Authority investigation into the Data Loss Event including but not limited to the causes and effects (actual or potential);

(c) provide immediate access to the relevant Premises and the Service Provider Systems for the purposes of any Authority investigation under paragraph 2.6;

(d) take all necessary actions to remedy the causes of the Data Loss Event and to ensure the protection of Personal Data from any further loss;

(e) not make any public statement of any kind without Approval;

(f) where appropriate, provide all assistance necessary to enable the Authority to fulfil its obligations to notify the ICO within 72 hours after becoming aware of the Data Loss Event; and

(g) further to its obligation to notify the Authority under this paragraph 2.7 provide further information to the Authority in phases as details become available.

2.8 Except to the extent required by any European Union Laws or European Union member state Laws, upon the earlier of:

(a) termination or expiry of this Contract (as applicable); and/ or

(b) the date on which the Contract Processor Data is no longer relevant to, or necessary for, the Permitted Purpose; and/or

(c) at any time upon request,

at the option of the Authority, the Service Provider will (and will procure that each Sub-Contractor will) promptly and securely delete or return to the Authority (in the format required by the Authority) all Contract Processor Data, and securely delete any remaining copies and promptly certify (via a director) when this exercise has been completed. For the avoidance of doubt, this obligation does not apply to Contract Processor Data that the Service Provider is required by law to store copies of.

2.9 The Service Provider shall assist the Authority to comply with any obligations under the Data Protection Laws, including:

2.9.1 compliance with the Data Security Requirements (to ensure a level of security appropriate to the risk presented by Processing the Contract Processor Data, in particular from a Personal Data Breach);

2.9.2 in documenting any Personal Data Breaches and reporting any Personal Data Breaches to any Supervisory Authority and/or Data Subjects;

2.9.3 taking measures to address Personal Data Breaches, including, where appropriate, measures to mitigate their possible adverse effects; and

2.9.4 conducting privacy impact assessments of any Processing operations and consulting with Supervisory Authorities, Data Subjects and their representatives accordingly,

and shall not perform its obligations under this Contract in such a way as to cause the Authority to breach any of the Authority's obligations under the Data Protection Laws to the extent the Service Provider is aware, or ought reasonably to have been aware, that the same would be a breach of such obligations.

2.10 Nothing in this Schedule shall be construed as requiring the Service Provider or any relevant Sub-Contractor to be in breach of any Data Protection Laws.

2.11 Notwithstanding anything in this Contract to the contrary, the provision of this Schedule applies during the Contract Period and shall continue in full force and effect for so long as Service Provider Processes any Contract Processor Data.

3. APPOINTING SUB-CONTRACTORS

3.1 The Service Provider shall be permitted to appoint a Sub-Contractor in accordance with this Schedule and to disclose Authority Data to such Sub-Contractors for Processing in accordance with the Service Provider's obligations under this Contract, provided always that:

(a) the Service Provider undertakes thorough due diligence on the proposed Sub-Contractor, including a risk assessment of the information governance-related practices and processes of the proposed Sub-Contractor, which shall be used by the Service Provider to inform any decision on appointing the proposed Sub-Contractor;

(b) the Service Provider provides the Authority with full details of the proposed Sub-Contractor (including evidence of and the results of the due diligence undertaken in accordance with paragraph 3.1(a)) before its appointment and the Authority has Approved the appointment of the proposed Sub-Contractor;

(c) the Sub-Contractor contract (as it relates to the Processing of Personal Data) is on terms which are the same as the terms set out in this Schedule, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the Processing will meet the requirements of the Data Protection laws;

(d) the Sub-Contractor's right to Process Authority Data terminates automatically on expiry or termination of the Contract for whatever reason; and

(e) the Sub-Contractor has obtained Approval in accordance with paragraph 2.3(d).

3.2 Where the Service Provider appoints a Sub-Contractor to Process Contract Processor Data, and that Sub-Contractor fails to fulfil the obligations imposed on it in accordance with paragraph 3.1(c), the Service Provider will be fully liable to the Authority for the performance of that Sub-Contractor's obligations.

4. DATA TRANSFERS OUTSIDE THE EEA

4.1 The Service Provider shall not make (nor instruct or permit a third party to make) a transfer of any Authority Data that is Personal Data to any Restricted Country unless it:

(a) first obtains Approval from the Authority;

(b) provides, in advance of any such transfer, a Data Transfer Risk Assessment to the Authority; and

(c) has put in place such measures to ensure the Authority's compliance with Data Protection Laws (and as otherwise may reasonably be required by the Authority).

4.2 If, after the Commencement Date, the Service Provider or any Sub-Contractor wishes to Process and/or transfer any Personal Data in or to any Restricted Country, the Service Provider shall, in seeking consent, submit such information as the Authority shall require in order to enable it to consider the request and acknowledges that such consent may be given subject to conditions which will, if appropriate, be incorporated into this Contract at the Service Provider's cost and expense using the "procedure set out under Clause F9 (Variation) and Schedule 5 (Change Control)";.

5. STAFF

5.1 The Service Provider shall:

(a) only disclose the Authority Data to its Staff that are required by the Service Provider to assist it in meeting its obligations under the Contract (the "**Project Staff**");

(b) ensure that no other Staff shall have access to such Authority Data; and

(c) identify and disclose to the Authority on request those members of Staff with access to or who are involved in handing the Authority Data.

5.2 The Service Provider shall only disclose the Authority Data to the Project Staff where the following conditions have been satisfied in relation to such Project Staff:

(a) the Service Provider shall have taken (and shall continue to take) all reasonable steps to ensure the reliability and integrity of each member of the Project Staff;

(b) each member of the Project Staff shall have undergone, and shall continue to receive on an annual basis, reasonable levels of training in Data Protection Laws and in the care and handling of Personal Data; and

(c) each member of the Project Staff shall have entered into appropriate contractually-binding confidentiality undertakings;

(d) each member of the Project Staff are aware of and comply with the Service Provider's duties under this Schedule and Clauses E1 (Authority Data) and E4 (Confidentiality);

(e) each member of the Project Staff are informed of the confidential nature of the Authority Data and do not publish, disclose or divulge any of the Authority Data to any third party unless directed in writing to do so by the Authority or as otherwise permitted by this Contract; and

(f) the BPSS or BS7858 or equivalent.

6. DATA PROCESSED FOR LAW ENFORCEMENT PURPOSES

6.1 In relation to Personal Data processed for Law Enforcement Purposes, the Service Provider shall:

(a) maintain logs for its processing operations in respect of:

(i) collection;

(ii) alteration;

(iii) consultation;

(iv) disclosure (including transfers);

(v) combination; and

(vi) erasure,

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

(b) ensure that:

(i) 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;

(ii) 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

(iii) the Logs are made available to the Authority (including any third party authorised by the Authority), any statutory auditor or regulator, including the Information Commissioner's Office on request from either;

(c) use the Logs only to:

(i) verify the lawfulness of processing;

(ii) assist with self-monitoring by the Authority or (as the case may be) the Service Provider, including the conduct of internal disciplinary proceedings;

(iii) ensure the integrity of Personal Data; and

(iv) assist with criminal proceedings;

(d) as far as possible, distinguish between Personal Data based on fact and Personal Data based on personal assessments; and

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

(i) persons suspected of having committed a criminal offence;

(ii) persons convicted of a criminal offence;

(iii) persons who are or are suspected or alleged victims of a criminal offence; and

(iv) witnesses or other persons with information about actual or alleged offences.

7. DATA PROTECTION INDEMNITY

7.1 The Service Provider shall indemnify on demand and keep indemnified the Authority on a continuing basis from and against:

(a) any monetary penalties or fines levied by the ICO on the Authority;

(b) the costs of an investigative, corrective or compensatory action required by the ICO, or of defending proposed or actual enforcement taken by the ICO;

(c) any and all losses suffered or incurred by, awarded against, or agreed to be paid by, the Authority pursuant to a claim, action or challenge made by a third party against the Authority (including by a Data Subject) in relation to the processing undertaken under this Contract; and

(d) except to the extent that any of paragraphs 7.1(a) to (c) apply, any losses suffered or incurred, awarded against, or agreed to be paid by, the Authority,

in each case to the extent arising as a result of a breach by the Service Provider (or its Sub-Contractors) of this Schedule and/or their respective obligations under the Data Protection Laws.

8. AUTHORITY AND ICO GUIDANCE

The Parties agree to take account of any guidance issued by the Authority, Home Office, (the European Data Protection Board for as long as the ICO remains a full member of it) and the ICO. The Parties shall, within 30 Working Days of notification by the Authority to the Service Provider, agree appropriate amendments to the Contract to ensure that it complies with any guidance issued by the Authority's DPO and the ICO.

9. SERVICE PROVIDER AS CONTROLLER

9.1 Where the Service Provider is acting as a Controller in relation to any Controller Data, the obligations in this paragraph 9 apply.

9.2 The Parties agree that the Authority expects to receive the following categories of Controller Data from the Service Provider (and, where such categories can vary in their format, such as dates, the Service Provider will provide that Controller Data in the same format as set out in this paragraph 9.2):

Category	Description	Access/Format
Third Party Data	Personal data separately sourced, outside of this Contract, from third parties, including Credit Reference Agencies and Trace Agencies	Client Portal/Web Page
Service Provider Data	Personal data separately sourced, outside of this Contract, from the Service Provider's Enforcement Instance of Edge.	Client Portal/Web Page

9.3 The Service Provider shall store and use the Controller Data in accordance with Applicable Laws and in respect of any Authority Data provided to the Service Provider by the Authority, in accordance with the Authority's retention and deletion policies, as they may be updated from time to time. In the event of a conflict between the Authority's retention and deletion policies and any statutory or professional retention or deletion rules that apply to the Service Provider ("**Other Rules**"), those Other Rules will prevail.

9.4 The Service Provider agrees to promptly notify the Authority in writing if it reasonably believes that any of the Controller Data is incorrect, in each case providing the Authority with the necessary Accuracy Data, together with reasonable, relevant supporting evidence for the change(s) required.

9.5 The Service Provider will undertake a periodic sampling exercise of the Controller Data it shares with the Authority to ensure that the Controller Data it shares with the Authority is accurate.

9.6 The Service Provider agrees to promptly notify the Authority in writing (and in any event within 72 hours of receipt) of any adjustment to the Controller Data, and/or its use and/or retention required pursuant to Applicable Laws and which the Service Provider is obliged to notify to the Authority and/or which the Authority is obliged to implement as a result, by promptly providing the Adjusted Data, together with reasonable, relevant supporting evidence for the adjustment(s) required.

9.7 The Parties acknowledge and agree that in respect of the Controller Data:

9.7.1 each Party is a Controller in its own right in the course of its own organisation or business, in particular as it relates to the Processing of Personal Data not relevant to this Contract;

9.7.2 the Service Provider and the Authority are not joint Controllers of the Controller Data, using it independently of each other in relation to the Controller Purpose; and

9.7.3 the disclosure of the Controller Data by the Service Provider to the Authority for the Controller Purpose is made on the lawful basis as set out in **Annex 2.**

9.8 The Service Provider shall Process the Controller Data in accordance with the Data Protection Laws and in particular shall in relation to the Controller Data:

9.8.1 implement technical and organisational measures to ensure a level of security appropriate to the risk presented by the Processing of the Controller Data including having regard to the risk of varying likelihood and severity for the rights and freedoms of Data Subjects, in particular from a Personal Data Breach;

9.8.2 conduct checks, inspections and audits to ensure compliance with its obligations under this Schedule and the Data Protection Laws and promptly take action to enforce compliance with them in the event it becomes aware of any breaches of them;

9.8.3 not do or omit to do anything to put the Authority in breach of its obligations under the Data Protection Laws;

9.8.4 promptly (and in any event within 72 hours of receipt) (to the extent permitted by law) inform it in writing (with reasonable, relevant details) of any:

(a) request relating to any of the Controller Data, from any third party, including any law enforcement authority ("**Third Party Request**");

(b) communication in relation to the Controller Data, from any relevant competent regulator or similar body, or Supervisory Authority ("**Regulatory Request**"); and/or

(c) complaint or request by a Data Subject relating to their Controller Data, including in relation to the exercise of his or her rights under Data Protection Laws ("**Data Subject Rights Request**"),

9.8.5 provide prompt and reasonable assistance, co-operation, information and records to the Authority in respect of any notified Third Party Requests, Regulatory Requests and Data Subject Rights Requests, in order that the Authority may deal with the relevant request(s) in accordance with the timescales as set out therein or in accordance with its own applicable obligations and their timeframes under the Data Protection Laws;

9.8.6 at all times maintain complete and accurate records of all action taken in connection with, and all supporting documentation in relation to, the performance of its obligations under this Contract (the **"Records**") and retain the Records during the duration of this Contract and thereafter for as long as is required by, and in compliance with, Applicable Laws;

9.8.7 in order that the Authority, their representatives (including external or independent auditors) and Supervisory Authorities (or equivalent regulators or bodies) may audit the Service Provider's compliance with the terms of this Schedule, and/or as may be necessary for the Authority to comply with the requirements of any Supervisory Authority (or equivalent regulatory or body) or Applicable Laws, the Service Provider will promptly provide to them (as relevant) on request from time to time, at no additional charge, during the term of the Contract and any period after that for so long as Controller Data is retained and/or Records retained:

(a) reasonable access to and copies of the Records;

(b) reasonable access to all relevant information, premises, data, IT systems, employees, agents, Sub-contractors, suppliers and assets at all locations from which obligations of the Service Provider pursuant to this Contract are being carried out; and

(c) all reasonable assistance in carrying out the audit; and

(d) any inspection or audit, or failure to inspect or audit, shall not in any way relieve the Service Provider from its obligations under the Contract.

9.9 The Service Provider will notify the Authority promptly of becoming aware of any Personal Data Breach, where in the reasonable opinion of the Service Provider, it is likely to present a material risk to the Authority (whether in relation to its IT systems or security, individuals affected, compliance, liability, and/or reputation) and provide it with all relevant information relating to the same as soon as is reasonably possible (to the extent not prohibited by Applicable Laws, and/or this can be done without compromising any confidentiality obligations owed by the Service Provider to any third party) including:

9.9.1 the nature of the Personal Data Breach and details of its likely consequences;

9.9.2 the categories of Authority Data affected (or potentially affected) and numbers and types of Data Subject affected;

9.9.3 any measure(s) proposed to be taken to address the incident and to mitigate its possible adverse effects; and

9.9.4 whether details of the Personal Data Breach have been disclosed to any other parties,

and may not delay such notification on the basis that any investigation in relation to the Personal Data Breach is incomplete or ongoing.

9.10 To the extent that the Authority reasonably considers that the Parties act as joint Controllers in respect of any Personal Data, the Service Provider will act reasonably to agree documented details of the Processing operations undertaken by each of the Parties in that role and the other information required by the Data Protection Laws prior to any such Processing as joint Controllers taking place.

9.11 The Parties will assess the ongoing effectiveness of their sharing of Controller Data at least once every six calendar months. If either Party raises any concerns in relation to the sharing of Controller Data, the Parties will act reasonably and in good faith in seeking to agree how to resolve such concerns as soon as reasonably practicable.

9.12 The Authority will not Process Controller Data for any purposes other than those envisaged under this Contract.

ANNEX 1

DATA PROCESSING PARTICULARS

[redacted]

3. The Service Provider shall comply with any further written instructions with respect to Processing by the Authority.

4. Any such further instructions shall be incorporated into this Annex.

Description	**Details**
Identity of the Controller and Processor	The Parties acknowledge that for the purposes of the Data Protection Laws, when processing Contract Processor Data the Authority is the Controller and the Contractor is the Processor in accordance with paragraph 1.1. Notwithstanding paragraph 1.1 the Parties acknowledge that they are also independent Controllers for the purposes of the Data Protection Laws in respect of Controller Data.
The subject matter and duration of the Processing	**Subject matter** Personal Data relating to: • Defendants, debtors and any other persons who are the subjects of Warrants and Orders; • service users, including complainants, correspondents and enquirers, business or other contacts, employees of other organisations; • Judges; • the Authority's staff, contractors, sub-contractors, consultants or other employees **Duration** The Contract Period and any period thereafter during which the Service Provider processes Authority Data.
The nature and purpose of the Processing	Processing in connection with the delivery of the Services under this Contract, particularly relating to the provision of Approved Enforcement Agency services; accounts and records; public relations and legal services.
The type of Personal Data being Processed	In relation to the Services: for Defendants, debtors and any other persons who are the subjects of Warrants and Orders: name, personal details and personal circumstances; offences; Court proceedings and outcomes; financial information. For the purposes of administering the Contract: in relation to Authority staff, contractors, sub-contractors, consultants or other employees, contact information: name, business email address, business telephone number held for the purposes of administering the Services.
The categories of Data Subjects	All categories of service users, including:

	• Defendants, debtors and any other persons who are the subjects of Warrants and Orders; • service users, including complainants, correspondents and enquirers, business or other contacts, employees of other organisations; • the Authority's staff, contractors, sub-contractors, consultants or other employees
Plan for return and destruction of the Personal Data once the Processing is complete **UNLESS any requirement under any European Union Laws or European Union member state Laws to preserve that type of Personal Data**	**Data retention:** In accordance with item 21, Magistrates Courts Records Retention and Disposition Schedule, all Personal Data processed in connection with the delivery of the services will be retained for 6 years from the date processing is complete on the customer's last active case, with the exception of: • Video and audio recordings (retained for 1 year from recording date) • Evidence of vulnerability containing sensitive information such as health records is retained for 2 days following completion of an accepted vulnerability assessment • Evidence from a new occupier of an address recorded for a defendant confirming that the defendant is no longer resident is retained for 2 days following acceptance of the evidence **Data destruction** All Personal Data is stored electronically on the Service Provider's case management system, Edge. Edge uses two data stores – a PostgreSQL relational database for structured data and an object store (AWS S3) for unstructured data such as photos and scans. The structured data is deleted using an update report that overwrites the personal data with the X character. The unstructured object is overwritten with a text placeholder file explaining that the data has been removed under the Service Provider Data Retention Policy.

ANNEX 2

LAWFUL BASIS FOR SHARING AND USE

Part of Controller Purpose	Lawful Basis of Use for Purpose
As required for compliance with legal or regulatory requirements including (audit obligations) and the operation of the contract	**Personal Data** Public Task, under Article 6 of the GDPR. **Special Category Personal Data (under GDPR)** Necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Authority and otherwise in its legitimate interests to facilitate the execution of Warrants in a reasonable and proportionate manner. Administration of Justice includes; - Criminal and civil enforcement of fines; - Research for the development of justice policies and statistics and - To improve the services. **Personal Data relating to criminal allegations and/or offences** Article 10 of the GDPR.
Sharing Controller Data with the Authority.	**Personal Data** Legitimate Interest under Article 6 of the GDPR. **Special Category Personal Data (under GDPR)** It is in the substantial public interest under Article 9 of the GDPR – in particular, to protect the interests of vulnerable people (based on paragraph 18 of Schedule 1 of the Data Protection Act 2018, safeguarding of children and individuals at risk). **Personal Data relating to criminal allegations and/or offences** Paragraph 34 (Judicial acts) of Part 3 of Schedule 1 of the Data Protection Act 2018, and Article 10 under GDPR.

ANNEX 3

Controller Purpose

Details
Service Provider - Controller Purposes The Service Provider is: • sharing the Controller Data with the Authority. The Authority is permitted to use the Controller Data pursuant to the Enforcement Legislation and other Applicable Laws. Authority - Controller Purposes In addition, the Authority is permitted to use the Controller Data as required for the operation of the Contract including for: 1.1.1 the placing of insurance; 1.1.2 taking legal or insurance or technical advice; 1.1.3 compliance with legal or regulatory obligations and requirements, including audit obligations imposed on the Authority; 1.1.4 evidencing compliance with legal or regulatory obligations and requirements; 1.1.5 exercising, establishing and/or defending legal rights 1.1.6 investigating complaints 1.1.7 reporting to the Secretary of State; and 1.1.8 necessary services to support such Processing, including data storage or hosting, IT / records management, maintenance and related support.