Annex 1

EPAM Data Processing Agreement

This Data Processing Agreement ("**DPA**") as Annex 1 (the "**Annex**") to the Master Services Agreement by and between EPAM Systems, Inc. ("**EPAM**") and Coleman Research Group, Inc. ("**Client**"), dated as of May 28, 2013, as previously amended ("**Agreement**") shall govern the processing of Personal Data of EPAM on behalf of Client. In this Annex, unless otherwise stated or unless the context otherwise requires, each capitalized term will have the meaning set out below or as stated in the Agreement:

"**Data Protection Laws**" means all laws and regulations applicable to the processing of Personal Data or Personal Information under the Agreement, including, but not limited to, the Japanese Act on Protection of Personal Information (Act No. 57 of May 30, 2003) and any rules and relevant guidelines thereto.

"**Data Subject**" means is the identified or identifiable person to whom the Personal Data relates.

"**Personal Data**" **or** "**Personal Information**" means (a) any information relating to an identified or identifiable natural person or any information that can be combined with other information to identify a natural person, or (b) other information not covered by the foregoing but that is information protected as personal data under Data Protection Laws.

"Process" The term "process' or "processing" shall have the meaning ascribed to them under the Data Protection Laws.

"**Standard Contractual Clauses**" means the agreement executed by and between the data exporter and data Importer pursuant to Section 4 in the form annexed to the European Commission's decision of 4 June 2021 on Standard Contractual Clauses for the transfer of personal data to third countries.

1. Client shall not make available Personal Data to EPAM other than as expressly set out in a Statement of Work (or other similar agreement) and only to the extent necessary for EPAM to perform the Services or provide products. Client shall notify EPAM in writing before it makes available Personal Data to EPAM and the parties shall (a) agree to an amendment to the relevant Statement of Work and any other necessary documentation, and (b) list the categories of Data Subjects and Personal Data to be processed and the processing activities to be undertaken by EPAM. Any Personal Data shall be located on a Client controlled environment (which includes Client's third party cloud providers) or, if agreed in a Statement of Work, on a secure dedicated area operated by EPAM. Client shall be liable for the reasonable additional costs required to implement such area and any other appropriate technical and organizational measures implemented to protect the Personal Data, including, but not limited to, on a Client controlled environment. EPAM shall only have remote read-only access with no ability to copy or capture such Personal Data, unless otherwise pre-agreed in writing. If Client makes test data available to EPAM it shall ensure that such data is anonymized.

2. The provisions of this Annex shall apply if EPAM processes or otherwise has access to any Personal Data provided or made available by Client when performing Services or providing any products under the Agreement, as indicated in a Statement of Work. In such case, Client shall, without hindering EPAM's ability to provide the Services or products, use commercially reasonable efforts to provide anonymized or pseudonymized data (whether by encrypting, hashing, masking, substituting or otherwise), and will specify such systems, software, databases or other files that are expected to contain Personal Data in the applicable Statement of Work.

3. In the event that EPAM is processing Personal Data governed by EU or UK Data Protection Laws, Client shall be the data controller (where "**data controller**" means an entity which alone or jointly with others determines purposes for which and the manner in which any Personal Data are, or are to be, processed) and appoints EPAM as a data processor (where "**data processor**" means an entity which processes the Personal Data only on behalf of the data controller and not for any purposes of its own) to process Personal Data for the contracted business purposes set out in Exhibit A which serves as a

template to be attached to a Statement of Work or as further described in the Agreement or a Statement of Work (the "**Permitted Purposes**").

4. Client acknowledges and agrees that the Personal Data may be transferred or stored outside the country where Client and Client employees are located to countries with a different level of data protection for EPAM to provide the Services or products and perform its other obligations under the Agreement. Client shall set out in the relevant Statement of Work if any Personal Data to be provided or made available to EPAM originates in the European Economic Area ("**EEA**"). EPAM shall not process or transfer any Personal Data under its control and/or possession originating from within the EEA to any other country outside the EEA (other than to any country which has not been approved by the EU Commission as having an adequate level of protection for personal data), unless it has taken such measures as are necessary to ensure the transfer is in accordance with Data Protection Laws. EPAM shall transfer the Personal Data to sub-processors located outside the EEA on the basis of the EU Standard Contractual Clauses to legitimize the transfer of Personal Data outside the EEA. For the transfer of Personal Data of EU residents from Client to EPAM, who is located outside the EU or an adequate country, the parties shall conclude the Standard Contractual Clauses attached to this DPA as Exhibit C. For the transfer of Personal Data of UK residents from Client to EPAM, who is located outside the UK or an adequate country, the parties shall conclude the EU standard contractual clauses based on Commission Decision C(2010)593 attached to this DPA as Exhibit D. The agreed Standard Contractual Clauses as well as the EU standard contractual clauses based on Commission Decision C(2010)593 will form an integral part of this DPA and the Agreement. In case of a conflict between the provisions of the documents the following order of precedence shall apply: (i) Standard Contractual Clauses as well as the EU standard contractual clauses based on Commission Decision C(2010)593, (ii) this DPA, (iii) each SOW, (iv) the Agreement.

5. Client shall ensure that it has obtained all necessary consents and it is entitled to transfer the relevant Personal Data to EPAM so that EPAM may lawfully use, process and transfer the Personal Data in accordance with the Agreement on Client's behalf.

6. EPAM shall process Personal Data in accordance with any lawful and reasonable instructions given by Client from time to time as set out in and in accordance with the terms of the Agreement or a Statement of Work. Client acknowledges that EPAM is under no duty to investigate the completeness, accuracy or sufficiency of any instructions of Personal Data. EPAM shall maintain a record of the Processing activities required under applicable Data Protection Laws related to the Processing of Personal Data under this Agreement.

7. EPAM shall take appropriate administrative, technical and organizational measures to protect the Personal Data under its control and/or possession against (a) unauthorized or unlawful processing of the Personal Data, and (b) only and to the extent it is stored on EPAM systems its accidental loss, destruction or damage (a "**Security Incident**"). The minimum level of technical and organizational measures is attached as Exhibit B and includes information on EPAM's (i) antivirus protections, (ii) process for disposal of Personal Data, and (iii) industry standard security used at EPAM premises which are provided at no additional cost to Client. EPAM will regularly review the technical and organizational measures set out in Exhibit B. Additional incurred costs to implement these or additional measures will be borne by Client. If EPAM becomes aware of a confirmed Security Incident, EPAM will use reasonable efforts to promptly provide Client notice following discovery of any such event and such further information and assistance as may be reasonably requested so that Client can fulfil any data breach reporting obligations it may have under Data Protection Laws and shall promptly commence all reasonable efforts to investigate and correct the causes and remediate the results thereof.

8. If EPAM receives a request from a Data Subject for access to Personal Data or any other request relating to Client's obligations under any law, legislation and/or regulations relating to the protection of Personal Data (including the rights of access, correction, objection, erasure and data portability, as applicable), EPAM shall:

   (a) promptly notify Client; and

   (b) provide reasonable cooperation and assistance, at Client's cost, to Client in relation to any such complaint or request by:

(i) providing Client with full details of any such request;

(ii) providing Client with any Personal Data it holds in relation to a Data Subject in a form specified by Client and within 10 days of receipt of the request from a Data Subject or as otherwise reasonably stipulated by Client; and

(iii) comply with the data access request within the relevant timescales set out in the relevant law, legislation and/or regulations and in accordance with explicit authorisation to do so from Client.

9. EPAM shall, upon 60 days prior written notice (at Client's expense) and during normal business hours, (a) allow for audits by any regulatory body which has supervisory authority or jurisdiction over Client or not more than once a year by the Client, and (b) provide reasonable co-operation to Client (at Client's expense) in connection with any data protection impact assessment that may be required under Data Protection Laws. However, Client shall not be allowed to have access to the following information: (i) Information relating to other EPAM customers or information not related to the services; (ii) access to EPAM's locations/premises (or portions thereof) that are not related to Client or the services; (iii) EPAM's records or documents relating to costs, margin or profitability; (iv) EPAM's personnel records; (v) internal audit reports; (vi) Information covered by legal privilege; and (vii) taking photographs of facilities, equipment or to make copies of floor plans, wiring, network or systems diagrams or other technical or infrastructure-related documentation.

10. Upon expiry or termination of this Annex for any reason EPAM shall, upon Client's written request, return, or at Client's option, destroy any Personal Data under its control and/or possession held by it. This requirement shall not apply to the extent that EPAM is required by applicable law to retain some or all of the Personal Data, or to Personal Data it has archived on back-up systems, which EPAM shall securely isolate and protect from any further processing except to the extent required by such law.

11. Client consents to EPAM engaging third party sub-processors (including any EPAM affiliates) to process the Personal Data for the Permitted Purpose, provided that (a) EPAM maintains an up-to-date list of its sub-processors as set out in the respective Statement of Work and shall update Client in advance of any change in sub-processors, (b) EPAM shall impose data protection terms on the sub-processors set out in a Statement of Work requiring it to protect the Personal Data to the standard required by Data Protection Laws and EPAM remains liable for any breach of this Annex that is caused by an act, error or omission of its sub-processor, and (c) Client may object to EPAM's appointment or replacement of a sub-processor within five (5) business days of receiving notice of the appointment or replacement, provided such objection is based on reasonable grounds relating to complying with Data Protection Laws. EPAM will limit access to Personal Data to EPAM's employees, agents, sub-processors and subcontractors who require access to Personal Data to fulfill EPAM's obligations and will only use such Personal Data in the performance of its obligations or as required by law.

12. In relation to EPAM's processing of Personal Information in its environment that is subject to the California Consumer Privacy Act of 2018 ("**CCPA**"), EPAM is a Service Provider (defined below), and the following shall apply:

(a) Except as otherwise set forth in this Annex, the terms "Business Purpose," "Personal Information" "Processing," "Sell" (or "Selling") and "Service Provider" shall have the meanings ascribed to such terms in the CCPA.

(b) EPAM shall Process Personal Information made available to it for the Permitted Purpose (which the parties agree are for Client's Business Purposes).

(c) EPAM will not Sell any Client Personal Information.

(d) EPAM shall limit Personal Information collection, use, retention, and disclosure to activities reasonably necessary and proportionate to achieve the Permitted Purposes or another compatible operational purpose.

(e) EPAM shall promptly comply with any Client request requiring it to provide, amend, transfer, or delete the Personal Information, or to stop, mitigate, or remedy any unauthorized Processing.

(f) If the CCPA permits, EPAM may aggregate, deidentify, or anonymize Personal Information so it no longer meets the Personal Information definition, and may use such aggregated, deidentified, or anonymized data for its own purposes in accordance with the Client's instructions or written permission.

(g) EPAM shall notify Client if it receives a verifiable consumer request under the CCPA and reasonably cooperate with Client with regard to responding to such requests.

13. This DPA sets forth the entire agreement and understanding between the parties with respect to the subject matter hereof, and supersedes and replaces all prior written or oral agreements, negotiations, understandings with respect thereto. Each party acknowledges that in entering into this DPA it has not relied on any representation, undertaking, warranty, collateral contract or assurance which is not expressly set out or referred to in this DPA.

EPAM Systems, Inc.

Name: Jason Peterson

Position: CFO

Date: 8/12/2022

Signature: DocuSigned by: Jason Peterson A90D87B0D96C415...

Coleman Research Group, Inc.

Name: Izaak Karaev

Position: Execitive Chairman

Date: 8/12/2022

Signature: DocuSigned by: Izaak Karaev 72070B02B09D4A5...

<u>Appendices</u>

Exhibit A - Details of Personal Data and Processing

Exhibit B - Technical and Organizational Measures

Exhibit A – Template for SOW

Details of Personal Data and Processing

This Exhibit forms part of and is incorporated into the Statement of Work to which it is attached.

Subject-Matter, Nature and Purpose of Processing

- Internal application for development and testing of new features.

Categories of Data Subjects

EPAM's Processing concerns the following categories of Data Subjects:

- Client's and its affiliates' employees
- Client's and its affiliates' consultants
- Client's and its affiliates' clients and contacts (obfuscated in testing and development environments).

Types of Personal Data

EPAM's Processing concerns the following categories of Personal Data:

- Client's and its affiliates' employees
    - Name
    - Corporate contact information (phone, email, and office location)
- Client's and its affiliates' consultants
    - Name (Client and its affiliate)
    - Employment history (Client and its affiliate)
        - Title, current and previous employers
    - Contact details
        - Phone and email
    - Home Address
    - Payment details (available to entitled users):
        - Bank Name
        - Bank Address
        - Bank Account Number
        - Routing Number
        - Last 4 digits of social
- Client's and its affiliates' clients and contacts (obfuscated in testing and development environments)

Special categories of Personal Data (if appropriate)

EPAM's Processing concerns the following special categories of Personal Data (as defined in applicable Data Protection Laws):

- None

Exhibit B

Technical and Organizational Measures

Information Security Organization

1. EPAM has an information security organization in place with key roles, responsibilities and accountabilities for information protection clearly defined. EPAM maintains an executive sponsored information security program, aimed at continuous enhancement of EPAM's security capabilities and covering all aspects of information security. EPAM maintains a comprehensive framework of information security policies, standards and procedures applying across the organization.

2. EPAM continuously maintains compliance of the information security management system with the best industry standards such as ISO27001 and ISAE 3402 Type II and regularly undergoes certification to these standards by independent certifying agencies.

Assets Management

3. EPAM maintains accurate inventories of its systems and other information assets.

4. EPAM will perform secure information deletion process prior to disposal of any hardware, software or media that may contain Client's information.

Personnel Security

5. EPAM maintains a comprehensive training and awareness program covering all aspects of information security and data privacy. Training completion is mandatory for all EPAM employees at the time of joining the company and thereafter at least on an annual basis. Training materials are being continuously reviewed and updated. Accurate records of training courses completion are kept and reported to the management. If requested by the Client, EPAM will take reasonable efforts to enhance the training program for specific projects and include additional training modules provided by and agreed upon with the Client.

6. EPAM conducts pre-employment screening on all candidates who are offered employment with the Company. According to Client requirements and/or the job role requirements the background screening can be conducted on three different security levels: basic, medium or high. Just such kind of screening can be run that legally is permissible in the country from where the services are delivered/where the employee is employed.

Physical Security

7. Access to all EPAM premises is restricted to authorized EPAM personnel and authorized visitors only. Physical access control systems are in place in order to manage access and maintain an audit trail of entries / exits and access right changes. If requested by the Client, EPAM will take reasonable efforts to introduce further restrictions of physical access to the premises from where the services are provided for the Client.

8. Video surveillance systems are installed at high security areas. The video recordings usually are kept for 30 days according to the local laws and regulation. If required requested by the Client, EPAM will take reasonable efforts to deploy video surveillance systems at the entrance to or within the areas where the services are provided for the Client, providing it is legally permissible in the country from where the services are delivered.

9. Security guard(s) or person with functions of security guard or security alarm system are present in EPAM premises based on security risk analysis. If requested by the Client, EPAM will take reasonable

efforts to have security guards present at the entrance to or within the areas where the services are provided for the Client.

Access Control

10. EPAM adheres to the best industry practices to manage access to its networks, systems and data, including but not limited to access authorization, reviews, use of 'as-needed' basis for granting access, segregation of duties, identity and authentication management. EPAM uses multifactor authentication techniques for access to EPAM's applications.

11. EPAM shall take reasonable efforts to isolate its systems and environments where Client's data can reside. EPAM will apply its access, identity, authentication and authorization management processes and tools to Client's data residing in EPAM systems and environments. If requested by the Client, EPAM shall take reasonable efforts to apply additional access, authentication and authorization controls, specified by the Client, to the Client's data residing in EPAM systems and environments.

12. Client shall manage access to its network, systems and data to ensure that access is only granted to EPAM employees on 'as-needed' basis. EPAM shall adhere to the Clients access control processes and identity and authentication standards in order to gain access and authenticate to Client's networks, systems and data.

13. EPAM established a set of additional requirements and guidelines for safe work from outside EPAM premises including work from home, coworking areas, hotels, public places. These include physical security related instructions, workstation hardening standards, network hardening standards, mandatory VPN usage to reach EPAM infrastructure, and/or use of Remote Desktop Protocol (RDP), or Secure Shell Protocol (SSH) to allow access to virtual machines (VMs) without any exposure through public IP addresses to reach Client's infrastructure as directed by the Client, and other practical security suggestions.

Network Security

14. EPAM protects its network employing a range of tools, technologies and techniques. Intrusion detection and protection sensors are deployed across key parts of EPAM network. Network segmentation techniques are used to isolate environments that require additional protection against data leaks or security threats. VPN, MPLS and VPLS techniques with industry standard encryption methods are used to protect data transmitted over the network between EPAM offices.

15. Client and EPAM shall agree upon secure connectivity and data transmission methods employing industry standard encryption mechanisms in order to establish connection between EPAM and Client environments, or environment of the third parties acting on behalf of the Client.

End Point Security

16. EPAM employs a range of tools and technologies to ensure that the end points remain protected against security threats or data leaks at all times. The tools protecting the endpoints include but are not limited to EDR, End Point firewalls, disk encryption, data loss prevention, DNS protection, End Point compliance checker, anti-phishing and other tools and technologies. The choice of tools to be deployed is determined by the level of risk related to a particular class of end points. All end point protection tools are being continuously updated to provide safeguards against the latest threats.

17. If required by the Client, EPAM will take reasonable efforts to deploy additional end point security tools specified by the Client, providing the tools are compatible with the technical environment and their use is legally permissible in the country where the tools are used.

Security Testing and Assessments

18. EPAM maintains a comprehensive program of vulnerability scanning, assessments and penetration testing occurring both continuously and periodically (annually). All identified vulnerabilities are being regularly reviewed, classified and resolved in a timely manner. For high risk, large scale or high complexity updates and patches EPAM performs testing, planning and prioritization prior to deployment in production environment.

Security Monitoring

19. EPAM employs a range of tools and technologies to continuously monitor all events and activities related to information security at various layers of its infrastructure and systems. Security Operations Centre is in place providing capability for security events monitoring, correlation, aggregation and incidents identification.

Security Incidents Management

20. EPAM responds to all security incidents within its Security Incidents Management process, with incident classification, reporting and escalation standards and timelines established.

Exhibit C

STANDARD CONTRACTUAL CLAUSES

Controller to Processor

SECTION I

Clause 1

Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) for the transfer of data to a third country.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter ‘entity/ies’) transferring the personal data, as listed in Annex I.A (hereinafter each ‘data exporter’), and

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A (hereinafter each ‘data importer’)

have agreed to these standard contractual clauses (hereinafter: ‘Clauses’).

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2

Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3

Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii) Clause 8.1(b), 8.9(a), (c), (d) and (e);

(iii) Clause 9(a), (c), (d) and (e);

(iv) Clause 12(a), (d) and (f);

(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e);

(viii) Clause 18(a) and (b).

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4

Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6

Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Clause 7 – Optional

Docking clause

(a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.

(b) Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.

(c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

8.1 Instructions

(a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in

Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter ‘personal data breach’). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person’s sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter ‘sensitive data’), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (in the same country as the data importer or in another third country, hereinafter ‘onward transfer’) if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter’s request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

(d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9

Use of sub-processors

(a) The data importer has the data exporter’s general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least 5 business days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10

Data subject rights

(a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

Clause 11

Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12

Liability

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.

(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13

Supervision

(a) The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14

Local laws and practices affecting compliance with the Clauses

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved, and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards;

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g., technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

Obligations of the data importer in case of access by public authorities

15.1 Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary, with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17

Governing law

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of Ireland.

Clause 18

Choice of forum and jurisdiction

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts of Ireland.

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

APPENDIX

ANNEX I

A. LIST OF PARTIES

Data exporter(s): [*Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union]*

Name: Coleman Research Group, Inc., and its UK affiliate, Coleman Research Limited

Address:

Coleman Research Group, Inc., 100 Park Ave, Suite 1600, New York, NY 10017

Coleman Research Limited, Aldwych House, 71-91 Aldwych London WC2B 4HN, United Kingdom

Contact person's name, position and contact details: Conrad Gordon, General Counsel, cgordon@colemanrg.com; +1 (984) 777-3292

Activities relevant to the data transferred under these Clauses:

To facilitate the Services set forth in the Agreement and any applicable SOW.

Signature and date: ____

Role (controller/processor):

- *Controller*

Data importer(s): [*Identity and contact details of the data importer(s), including any contact person with responsibility for data protection]*

Name: EPAM Systems, Inc.

Address: 41 University Drive, Suite 202, Newtown, PA 18940

Contact person's name, position and contact details: Tel.: N/A; fax: N/A; email: privacy@epam.com

Activities relevant to the data transferred under these Clauses:

To facilitate the Services set forth in the Agreement and any applicable SOW.

Signature and date: ____

Role (controller/processor):

- *Processor*

B. DESCRIPTION OF TRANSFER

According to the details of processing as agreed in the respective SOW between the parties.

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with Clause 13

UK Information Commissioner’s Office

ANNEX II

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

According to Exhibit B of the DPA between the parties.

ANNEX III

LIST OF SUB-PROCESSORS

According to agreed upon Sub-Processors as stated in the relevant SOW between the parties.

Exhibit D

Standard Contractual Clauses

EUROPEAN COMMISSION
DIRECTORATE-GENERAL JUSTICE

Directorate C: Fundamental rights and Union citizenship
Unit C.3: Data protection

Commission Decision C(2010)593
Standard Contractual Clauses (processors)

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection

Name of the data exporting organisation:Coleman Research Limited

Address: Aldwych House, 71-91 Aldwych London WC2B 4HN, United Kingdom

Tel.: +1 (984) 777-3292; fax:N/A; email: cgordon@colemanrg.com

Other information needed to identify the organisation:

Reference number: ZB137643

…………………………………………………………………
(the data **exporter**)

And

Name of the data importing organisation: EPAM Systems, Inc.

Address: 41 University Drive, Suite 202, Newtown, PA 18940

Tel.: N/A; fax: N/A; email: privacy@epam.com

Other information needed to identify the organisation:

…………………………………………………………………
(the data **importer**)

each a “party”; together “the parties”,

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

Clause 1

Definitions

For the purposes of the Clauses:

(a) *'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject'* and '*supervisory authority'* shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data[1];

(b) '*the data exporter'* means the controller who transfers the personal data;

(c) *'the data importer'* means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

(d) *'the subprocessor'* means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

(e) '*the applicable data protection law'* means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

(f) *'technical and organisational security measures'* means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2

Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

Clause 3

Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

[1] Parties may reproduce definitions and meanings contained in Directive 95/46/EC within this Clause if they considered it better for the contract to stand alone.

3. The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b) that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

(g) to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

(j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5

Obligations of the data importer[2]

The data importer agrees and warrants:

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;

(d) that it will promptly notify the data exporter about:

(i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,

(ii) any accidental or unauthorised access, and

(iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(h) that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing services by the subprocessor will be carried out in accordance with Clause 11;

(j) to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter.

[2] Mandatory requirements of the national legislation applicable to the data importer which do not go beyond what is necessary in a democratic society on the basis of one of the interests listed in Article 13(1) of Directive 95/46/EC, that is, if they constitute a necessary measure to safeguard national security, defence, public security, the prevention, investigation, detection and prosecution of criminal offences or of breaches of ethics for the regulated professions, an important economic or financial interest of the State or the protection of the data subject or the rights and freedoms of others, are not in contradiction with the standard contractual clauses. Some examples of such mandatory requirements which do not go beyond what is necessary in a democratic society are, *inter alia,* internationally recognised sanctions, tax-reporting requirements or anti-money-laundering reporting requirements.

Clause 6

Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or subprocessor is entitled to receive compensation from the data exporter for the damage suffered.

2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity.

   The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the subprocessor agrees that the data subject may issue a claim against the data subprocessor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the subprocessor shall be limited to its own processing operations under the Clauses.

Clause 7

Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

   (a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

   (b) to refer the dispute to the courts in the Member State in which the data exporter is established.

2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8

Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5(b).

Clause 9

Governing Law

The Clauses shall be governed by the law of the Member State in which the data exporter is established, namely England.

Clause 10

Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11

Subprocessing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses[3]. Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.
2. The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.
3. The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established, namely England.
4. The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the data exporter’s data protection supervisory authority.

Clause 12

Obligation after the termination of personal data processing services

1. The parties agree that on the termination of the provision of data processing services, the data importer and the subprocessor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the

[3] This requirement may be satisfied by the subprocessor co-signing the contract entered into between the data exporter and the data importer under this Decision.

personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

2. The data importer and the subprocessor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

On behalf of the data exporter:

Name (written out in full):

Position:

Address:

Other information necessary in order for the contract to be binding (if any):

Signature……………………………………….

(stamp of organisation)

On behalf of the data importer:

Name (written out in full):

Position:

Address:

Other information necessary in order for the contract to be binding (if any):

Signature……………………………………….

(stamp of organisation)

APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed by the parties.

The details of processing are included the the respective SOW under which the personal data is processed.

APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed by the parties.

Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached):

According to Exhibit B of the DPA between the parties.