ALACRITY

DATA PROCESSING AGREEMENT

This DPA shall form part of the Agreement between You and the Supplier.

1 INTERPRETATION AND DEFINITIONS

The terms and definitions referred to in the Agreement shall apply herein, unless defined otherwise below:

"**Affiliates**" means any entity that directly or indirectly controls, is controlled by, or is under common control of a party. "Control," for purposes of this definition, means direct or indirect ownership or control of more than 50% of the voting interests of a party.

"**Agreement**" means the agreement between the Supplier and You for the provision of and access to Services and Deliverables via the Alacrity Platform.

"**Customer**" means You.

"**Customer Data**" means data, including Personal Data, of which Customer or its Affiliates is the controller and which the Supplier processes in the course of providing the Services and Deliverables.

"**Data Protection Legislation**" means all applicable privacy and data protection laws including the Data Protection Act 2018, the GDPR and any applicable national implementing laws, regulations and secondary legislation relating to the processing of Personal Data and the privacy of electronic communications, as amended, replaced or updated from time to time, including the Privacy and Electronic Communications Directive (2002/58/EC) and the Privacy and Electronic Communications (EC Directive) Regulations 2003 (SI 2003/2426).

"**DPA**" means this data processing agreement including its schedules.

"**Relevant Personal Data**" means all personal data processed by the Supplier on behalf of the Customer under or in connection with the Agreement.

"**Security Breach**" means any accidental or unlawful, destruction, loss, alteration or unauthorised disclosure or access to the Relevant Personal Data.

"**Security Policy**" means the security policy of the Supplier as amended from time to time and attached to this DPA.

"**Standard Contractual Clauses**" means the standard contractual clauses set out in the European Commission's Decision 2010/87/EU of 5 February 2010 for the transfer of Personal Data to processors established in third countries (as may be amended by agreement of the parties for compliance with applicable Data Protection Legislation requirements) set out in Exhibit B of this DPA.

"**Sub-Processors**" means a person or entity subcontracted by the Supplier to process Relevant Personal Data in accordance with the Supplier's obligations under or in connection with the Agreement.

"**Supplier**" means Alacrity Law Limited of 1 Fore Street, London, EC2Y 9DT, England a company registered in England with company number 10607888.

The terms "controller", "data subject", "processor", "process", "processed", and "processing", "personal data" shall be as defined by the applicable Data Protection Legislation.

2   DATA PROTECTION

2.1   Supplier acknowledges that the Customer Data is the property of the Customer and the Customer owns absolutely all Intellectual Property Rights which may subsist in the Customer Data.

2.2   The parties acknowledge that for the purposes of applicable Data Protection Legislation, the Supplier is the processor of any Relevant Personal Data, and the Customer is the controller.

2.3   The parties shall, and the Supplier shall procure that each its Sub-Processors shall, comply at all times with the Data Protection Legislation and shall not do anything (or fail to do anything) to cause either party to breach any of its obligations under the Data Protection Legislation. The Supplier shall immediately notify the Customer in the event that it becomes aware of any breach of the Data Protection Legislation by the Supplier or any of the Sub-Processors in connection with the Agreement.

2.4   The parties shall take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to Relevant Personal Data does not process them except on the instructions from the

controller unless he or she is required to do so by any Data Protection Legislation.

2.5 The parties and, where applicable, their representatives, shall cooperate, on request, with a supervisory data protection authority in the performance of their respective obligations under this DPA and Data Protection Legislation.

3 OBLIGATIONS OF THE SUPPLIER

3.1 In so far as the Supplier processes any Relevant Personal Data on behalf of the Customer, the Supplier shall:

a) process the Relevant Personal Data only to the extent, and in such a manner, as is: (i) necessary for the purposes set out in the Agreement; (ii) in accordance with the Customer's documented instructions from time to time; and (iii) in accordance with the requirements of applicable Data Protection Legislation;

b) process Relevant Personal Data on behalf of the controller and shall take steps to ensure that any person acting under the authority of the processor who has access to Relevant Personal Data shall only process the Relevant Personal Data on the documented instructions of the controller;

c) only process the type(s) of personal data, and only in respect of the categories of data subjects and types of processing, set out in Exhibit A of this DPA;

d) taking into account the nature of the processing and the information available to the Supplier, the Supplier shall assist the Customer by having in place appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Customer's obligation to respond to requests for exercising the data subject's rights and the Customer's compliance with the Customer's data protection obligations in respect of the processing of Relevant Personal Data;

e) promptly comply with any request from the Customer requiring the Supplier to amend, transfer or delete Relevant Personal Data or to restrict processing and shall confirm that such request has been implemented and will not otherwise modify, amend or alter the contents of Relevant Personal Data;

ALACRITY

f)   if the Supplier receives any complaint, notice or communication which relates directly or indirectly to the processing of Relevant Personal Data or to either party's compliance with applicable Data Protection Legislation and the data protection principles set out therein (including from a data subject or any person or regulatory body with responsibility for monitoring and/or enforcing compliance with the Data Protection Legislation), it shall:

   i.   promptly notify the Customer of any complaint, notice or communication which adversely impacts the Customer, unless such notification is not permitted under applicable law or a relevant court order;

   ii.   only respond to any such complaint, notice or communication received at the request of the Customer; and

   iii.   provide the Customer with full co-operation and assistance in relation to any such complaint, notice or communication, including but not limited to:

     (i)   providing the Customer with any information reasonably requested by the Customer;

     (ii)   provide to Customer a copy of all Relevant Personal Data held by it in the format and on the media reasonably specified by the Customer; and

     (iii)   complying with a data access request within the relevant timescales set out in the Data Protection Legislation but strictly in accordance with the Customer's instructions.

g)   only disclose or permit the disclosure of any of Relevant Personal Data to third parties (including Sub Processors or data subjects) specifically authorised in writing by the Customer;

h)   ensure that any person authorised to access Relevant Personal Data shall be subject to written (or statutory) obligations to maintain the confidentiality of Personal Data, comply with the obligations in this DPA and are trained on the requirements of Data Protection Legislation and their obligations in respect of Relevant Personal Data under this DPA;

i)   implement appropriate technical and organisational procedures to protect Relevant Personal Data, taking into account the state of the art, the costs of implementation and the nature, scope, context and

purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons;

j) implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate: (i) the pseudonymisation and encryption of Relevant Personal Data; (ii) the ability to ensure the on-going confidentiality, integrity, availability and resilience of processing systems and services; (iii) the ability to restore the availability and access to Relevant Personal Data in a timely manner in the event of a physical or technical incident; (iv) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing. In accessing the appropriate level of security, account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Relevant Personal Data transmitted, stored or otherwise processed;

k) notify the Customer without undue delay after becoming aware of any Security Breach and shall: (i) provide full details of the Security Breach and the consequences (and potential consequences) of the Security Breach including: (a) the date and time of when the Security Breach occurred; (b) the type of data that was the subject of the Security Breach; (c) where possible, the categories and approximate number of Data Subjects concerned; (d) the identity of each affected Data Subject that has been identified to date; (e) details of any steps taken to remedy the Security Breach and recover or safeguard the Relevant Personal Data concerned; (ii) not make any notifications in relation to the Security Breach to any data subjects or any person or regulatory body with responsibility for monitoring and/or enforcing compliance with the Data Protection Legislation without the Customer's consent, unless required to do so by law (not to be unreasonably withheld or delayed); and (iii) take all commercially reasonable measures to secure the Relevant Personal Data and to limit the effects of any Security Breach;

l) except to the extent that the Supplier is prevented by law from returning or deleting Relevant Personal Data, or where partial data is stored in backups, the Supplier shall at the choice of the Customer return or irretrievably delete (at the Customer's sole option) all Relevant Personal Data, and delete all copies of Relevant Personal

Data, in accordance with the Supplier's data retention practices as highlighted in the Security Policy;

m) keep a record, in accordance with Article 30(2) of the GDPR, of any processing of Relevant Personal Data it carries out on behalf of the Customer and shall make such records available to the Customer on request;

n) reasonably assist the Customer in meeting its obligation to carry out data protection impact assessments ("DIAS"), taking into account the nature of the processing and the information available to the Supplier;

o) comply with all reasonable requests of the Customer (and / or its auditors and internal or external representatives, subject to reasonable and appropriate confidentiality undertakings being given by the Customer's auditors or representatives) to inspect and audit the Supplier's data processing activities to enable the Customer to verify that the Supplier is complying fully with its obligations under this DPA, provided that (i) the audit is carried out at the Customer's expense; (ii) limited in scope to matters specific to the Customer and agreed in advance; (iii) carried out during UK business hours and upon reasonable notice which shall be not less than 4 weeks unless an identifiable material issue has arisen; and (iv) conducted in a way which does not interfere with the Supplier's day-to-day business;

p) promptly inform the Customer, if in the Supplier's opinion, any of the instructions regarding the processing of Relevant Personal Data provided by the Customer, breaches any Data Protection Legislation.

3.2 In so far as a Sub-Processor Supplier processes any Relevant Personal Data:

a) The Customer acknowledges and agrees that: (i) Affiliates of the Supplier may be used as Sub-Processors; and (ii) the Supplier and its Affiliates respectively may engage Sub-Processors in connection with the provision of the Services and Deliverables;

b) The Supplier is permitted to transfer Relevant Personal Data to the Sub-Processors as amended from time to time. The Supplier shall provide at least 30 days written notice of any intended changes to the list of Sub-Processors (as amended from time to time and attached to this DPA) concerning the addition or replacement of

Sub-Processors. The Customer may object to the use of a new or replacement Sub-Processor, by notifying the Supplier promptly in writing within ten (10) business days after receipt of the Supplier's notice. If the Customer objects to a new or replacement Sub-Processor, the Customer may terminate the Agreement with respect to those Services or Deliverables which cannot be provided by the Supplier without the use of the new or replacement Sub-Processor;

c) Sub-Processors shall only process Relevant Personal Data in order to perform one or more of the Data Processor's specified obligations under the Agreement;

d) Prior to transferring any Relevant Personal Data to a Sub-Processor, the Supplier shall enter into a written agreement with that Sub-Processor, requiring the Sub-Processor to:

   i. process the Relevant Personal Data only in accordance with the written instructions of the Supplier;
   ii. abide by equivalent data protection obligations as those on the Supplier set out in this Data Processing Agreement; and
   iii. the Supplier shall ensure each such Sub-Processor complies with all such obligations.

e) The Supplier is responsible and liable for Sub-Processors' compliance with its obligations under this Data Processing Agreement.

3.3 The Supplier may transfer Customer Data to a third country outside the European Economic Area, provided that:

a) it obtains the express prior written consent of the Customer;

b) it ensures there is adequate protection for such Relevant Personal Data in accordance with applicable Data Protection Legislation. Adequate protection may include: (i) where such country is deemed by the European Commission to provide adequate levels of privacy protection; or (ii) the Supplier enters into the Standard Contractual Clauses with the Customer; and

c) if either: (i) the means by which adequate protection for the transfer is achieved ceases to be valid; or (ii) any person or regulatory body with responsibility for monitoring and/or enforcing compliance with

the Data Protection Legislation requires transfers of Personal Data pursuant to Standard Contractual Clauses to be suspended, then the Customer may, at its discretion, require the Supplier to immediately cease data transfers, to return all Relevant Personal Data previously transferred and for a senior officer or director of the Supplier to certify that this has been done.

4 OBLIGATIONS OF THE CUSTOMER

4.1 The Customer shall comply with this DPA and its obligations under Data Protection Legislation.

4.2 The Customer has obtained any and all necessary permissions and authorisations necessary to permit the Supplier, its Affiliates and Sub-Processors, to execute their rights or perform their obligations under this DPA.

4.3 Affiliates of the Customer who use the Services or Deliverables shall comply with the obligations of the Customer set out in this DPA.

4.4 The Customer shall implement appropriate technical and organisational procedures to protect Relevant Personal Data, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons. The Customer shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk.

4.5 The Customer acknowledges and agrees that some instructions from the Customer, including destruction or return of data, the Supplier assisting with audits, data subject requests, inspections, DPIAs or providing any assistance under this DPA, may result in additional fees. The Supplier shall be entitled to charge the Controller for its costs and expenses in providing any such assistance.

4.6 The Customer shall notify the Supplier within a reasonable time, of any changes to Data Protection Legislation which may affect the contractual duties of the Supplier. The Supplier shall respond within a reasonable timeframe in respect of any changes that need to be made to the terms of this DPA or to the technical and organisational measures to maintain compliance. If the parties agree that amendments are required, but the Supplier is unable to accommodate the necessary changes, the Customer may terminate the part or parts of the Services or Deliverables which give

rise to the non-compliance. To the extent that other parts of the Services or Deliverables provided are not affected by such changes, the provision of those Services or Deliverables shall remain unaffected.

5   LIABILITY

5.1   The limitations on liability set out in the Agreement apply to all claims made pursuant to any breach of the terms of this DPA.

5.2   The parties agree that the Customer shall be liable for any breaches of this DPA caused by the acts and omissions or negligence of its Affiliates as if such acts, omissions or negligence had been committed by the Customer itself.

5.3   The Customer shall not be entitled to recover more than once in respect of the same loss.

6   TERM AND TERMINATION

6.1   The Supplier will only process Personal Data for the term of the DPA. The term of this DPA shall coincide with the commencement of the Agreement and this DPA shall terminate automatically together with termination or expiry of the Agreement.

7   GENERAL

7.1   This DPA sets out the entire understanding of the parties with regards to the subject matter herein.

7.2   Should a provision of this DPA be invalid or become invalid then the legal effect of the other provisions shall be unaffected. A valid provision is deemed to have been agreed which comes closest to what the parties intended commercially and shall replace the invalid provision. The same shall apply to any omissions.

7.3   Subject to any provision of the Standard Contractual Clauses to the contrary, this DPA shall be governed by the laws of England and Wales. The courts of England shall have exclusive jurisdiction for the settlement of all disputes arising under this DPA.

7.4   The parties agree that this DPA is incorporated into and governed by the terms of the Agreement.

ALACRITY

Exhibit A

Overview of data processing activities to be performed by the Processor

1. Controller

The controller transfers Personal Data identified in sections 3, 4 and 5 below, as it relates to the processing operations identified in section 6 below.

The controller is the Customer.

2. Processor

The processor receives data identified in sections 3, 4 and 5 below, as it relates to the processing operations identified in section 6 below.

The processor is the Supplier.

3. Data Subjects

The Personal Data transferred includes but is not limited to the following categories of data subjects:

- Persons associated with the parties to legal matters on which a Legal Provider has been instructed, including without limitation directors, employees, contractors and suppliers of Clients, experts, legal and other professionals, and witnesses. Users, Affiliates and other participants from time to time to whom the controller has granted the right to access the Services and Deliverables in accordance with the terms of the Agreement.
- Clients of the controller and individuals with whom those end users communicate with by email and/or other messaging media.
- Employees of clients of the controller.
- Suppliers and service providers of the controller.
- Other individuals to the extent identifiable in the content of emails or their attachments or in archiving content.

4. Categories of Personal Data

The Personal Data transferred includes but is not limited to the following categories of data:

- Personal details, including first name and surname, contact details, positions held, user names, passwords, email addresses of Users.

- Personal Data derived from the Users use of the Services and Deliverables such as records and business intelligence information including communications, statements, diary entries, opinions held.
- Personal Data within email and messaging content which identifies or may reasonably be used to identify, data subjects.
- Meta-data including sent, to, from, date, time, subject, which may include Personal Data.
- Financial data.
- Data concerning education and profession.
- Matter scopes and file attachments that may contain Personal Data.
- Survey, feedback and assessment messages.
- Information offered by Users as part of support enquiries.
- Audit trail log of platform actions including IP address.
- Other data added by the Controller from time to time.

5. Special Categories of Data

No sensitive data or special categories of data are permitted to be transferred, and shall not be contained in the content of or attachments to, emails.

6. Processing Operations

The Personal Data transferred will be subject to the following basic processing activities:

- Personal Data will be processed to the extent necessary to provide the Services and Deliverables in accordance with both the Agreement and the Controller's instructions. The Processor processes Personal Data only on behalf of the Controller.
- Processing operations include but are not limited to: The processing of personal data for the purposes of assisting the Client and their legal advisers in the conduct of legal matters including the processing of personal data of individuals who are connected with legal matters undertaken by Legal Providers on behalf of Clients. These operations relate to all aspects of Personal Data processed.
- Technical support, issue diagnosis and error correction to ensure the efficient and proper running of the systems and to identify, analyse and resolve technical issues both generally in the provision of the Services and Deliverables and specifically in answer to a Controller query. This operation may relate to all aspects of Personal Data processed but will be limited to metadata where possible.

ALACRITY

- Virus, anti-spam and Malware checking in accordance with the Services and Deliverables provided. This operation relates to all aspects of Personal Data processed.

ALACRITY

Exhibit B

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

the Controller, (the data "**exporter**")

and

the Processor, (the data "**importer**")

each a "**party**"; together "**the parties**",

HAVE AGREED on the following Standard Contractual Clauses (the "**Standard Contractual 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 Exhibit A of the DPA.

ALACRITY

Clause 1

Definitions

For the purposes of the Standard Contractual Clauses all terms used in capitals shall have the meaning given to them in the DPA unless defined otherwise below:

(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;

(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 Standard Contractual 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 Standard Contractual 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.

ALACRITY

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 Exhibit A of the DPA which forms an integral part of the Standard Contractual 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.

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 Standard Contractual 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 Standard Contractual Clauses;

(c)   that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in the Security Policy;

(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 Standard Contractual Clauses, with the exception of the Security Policy, 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 Standard Contractual Clauses, unless the Standard Contractual 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 Standard Contractual Clauses; and

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

Clause 5

Obligations of the data importer

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 Standard Contractual 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 Standard Contractual 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 the Security Policy 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 Standard Contractual 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 Standard Contractual Clauses, or any existing contract for subprocessing, unless the Standard Contractual Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of the Security Policy 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 Standard Contractual Clauses to the data exporter.

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 Standard Contractual 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 Standard Contractual 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 Standard Contractual 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 Standard Contractual Clauses shall be governed by the law of the Member State in which the data exporter is established.

ALACRITY

Variation of the contract

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

Clause 11

Subprocessing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Standard Contractual Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Standard Contractual 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 Standard Contractual Clauses. 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 Standard Contractual 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.

4. The data exporter shall keep a list of subprocessing agreements concluded under the Standard Contractual 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 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.

Clause 13

Miscellaneous

1. These Standard Contractual Clauses take priority over any other agreement between the parties, whether entered into before or after the date these Standard Contractual Clauses are entered into.

2. Unless the Standard Contractual Clauses are expressly referred to and expressly amended, the parties do not intend that any other agreement entered into by the parties, before or after the date the Standard Contractual Clauses are entered into, will amend the terms or the effects of the Standard Contractual Clauses, or limit any liability under the Standard Contractual Clauses, and no term of any such other agreement should be read or interpreted as having that effect.

3. The parties intend that these Standard Contractual Clauses should only become effective if Art 44 of the General Data Protection Regulation (the "GDPR") applies to a transfer of personal data from the EEA to the UK, because the UK has left the European Union, and the transfer is not permitted under Art 45 of the GDPR.

4. On that basis, the Standard Contractual Clauses will become effective on:

    (a) the first date Article 44 GDPR applies to a transfer of personal data from the EEA to the UK, and that transfer is not permitted under Article 45 GDPR; or

    (b) the date the parties enter into the DPA, if later.

5. In this clause, 'a transfer of personal data' has the same meaning as in Article 44 of the GDPR.