Data Sharing Agreement

This data sharing agreement as defined below is between the customer as identified by the service agreement, and ELAS, and will be effective on the data of the service request**.**

IT IS AGREED as follows:

To facilitate the provision of the services or functions outlined within a separate agreement for service (the "**Permitted Purposes**"). ELAS and its Customer are required to share personal and special category data in the provision of occupational health, health surveillance and associated services.

(each a "party" and together the "parties").

Data Protection Provisions

1. In this agreement, the following terms shall have the following meanings:

   (a) "**controller**", **"independent controller"**, "**processor**", "**data subject**", "**personal data**", "**processing**" (and "**process**") and "**special categories of personal data**" shall have the meanings given in the UKGDPR;

   (b) "**Applicable Data Protection Laws**" means all applicable laws and regulations relating to the processing of personal data and privacy including, but not limited, to the UKGDPR and the Data Protection Act 2018 and all law and regulations implementing or made under them, any amendment or re-enactment of them and, where applicable, the guidance and codes of practice issued by any applicable regulatory bodies or supervisory authorities;

   (c) **"Agreement Data"** means data necessary to fulfil the obligations of the service agreement and any other legal requirement;

   (d) "**Authorised Person**" means individuals authorised by parties and under this agreement to process personal data;

   (e) **"Customer"** means the organisation that has instructed ELAS and has a service agreement with ELAS for services.

   (f) **"Data Protection Laws"** means, as applicable to either party in its activities:

      1) UK GDPR;

      2) The Data Protection Act 2018;

      3) Any other applicable law relating to the Processing, privacy and/or use of Personal Data;

      4) Any laws which implement such laws.

   (g) **"Data Protection Supervisory Authority"** means any regulator, authority or body responsible for administering Data Protection Laws;

   (h) "**EEA**" means the European Economic Area;

   (i) "**GDPR**" means the 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, and repealing Directive 95/46/EC (General Data Protection Regulation);

   (j) **"ELAS"** has the meaning of a business or division as part of Citation Holdings or the entirety of all Group Companies.

(k) **"Company"** has the meaning of the Supplier used for the delivery of services on behalf of a ELAS.

(l) "**Permitted Purposes**" means the requirements set out in the service order and in accordance with the privacy notice;

(m) **"Permitted Recipients"** means those that need access to the Received Personal Data for the Permitted Purpose.

(n) **"Personal Data Breach"** has the meaning given in Data Protection Laws.

(o) "**Relevant Data Controller**" means the Data Controller, in relation to the personal data affected or in use; and

(p) "**Security Incident**" has the meaning given to the term in clause 1.7.2

(q) **"UK GDPR"** means has the meaning given to it in section 3(10) (as supplemented by section 205(4)) of the Data Protection Act 2018.

1.2. ***Relationship of the parties:*** The Parties agree that they are data controllers for the data shared between them, for the permitted purposes set out in the service agreement or were processing for legal, regulatory or compliance purposes, and governed by the terms and conditions of service. Each party shall use all reasonable endeavours to comply with the obligations that apply to it under the Applicable Data Protection Laws.

1.3. ***The lawful basis:*** for sharing the information between the parties is Article 6 1(b) and Article 9 2(h).

1.4. ***Particular Obligations to data sharing:***

1.3.1 Process the personal data for the agreed Permitted Purposes.

1.3.2 Do not disclose or allow access to the Agreement Personal Data to anyone other than the Permitted Recipients.

1.5. ***Confidentiality of processing:*** Each Party shall ensure that all Authorised Persons that access Agreement Personal Data understand their obligations of confidentiality, have signed confidentiality clauses and shall keep the Agreement Personal Data it processes confidential.

1.6. **Consent:** Where consent or explicit consent is required for the purposes of processing, each Party (the "Relevant Data Controller") shall obtain the necessary consents and authorisations from data subjects of whom personal data is processed.

1.7. **Security:** Both Parties shall at all times:

1.7.1 Put in place and maintain appropriate technical and organisational measures as required by Data Protection Laws;

1.7.2 Implement and maintain appropriate technical and organisational measures to protect the Agreement Personal Data in its possession or control against accidental, un-authorised or unlawful destruction, loss, alteration, disclosure or access, takin into account:

(a) The nature of the data to be protected

(b) Proportionality

(c) The harm that might result from any failure to so protect the Agreement Personal Data

(d) The state of technological development; and

(e) The cost of implementing measures

1.7.3 Regularly monitor compliance with such security safeguards and ensure that there is no material decrease in the level of security afforded to each Parties personal data during the duration of the processing.

1.8. **Personal Data Breaches**

1.7.1 Both Parties shall promptly (and in any event within 24 hours) notify each Party, if it becomes aware of a Personal Data Breach in respect of any Agreement Personal Data which is processed by each Party. In such circumstances, the Party where the breach occurred shall promptly provide (to the extent permitted by applicable law in the United Kingdom):

1.7.1.1 Sufficient information as each Party (or its advisors) reasonable requires to meet any obligations to report a Personal Data Breach under Data Protection laws (in a timescale which facilitates compliance).

1.7.1.2 The Data Protection Supervisory Authorities investigating the Personal Data Breach with complete information as requested by those Data Protection Supervisory Authorities from time to time.

1.7.2 All reasonable assistance to each Party including:

(a) Cooperation with Data Protection Supervisory Authorities (including with investigations or actions to mitigate or remediate a Personal Data Breach);

(b) Making available all relevant data and records required for either Party to comply with Data Protection Laws or as otherwise reasonable required;

(c) Taking such reasonable steps as are directed by the affected Party to assist in the investigation, mitigation and remediation of a Personal Data Breach (which may include providing the affected Party with physical access to any facilities affected and facilitating the interview with staff and others involved in the matter) and

(d) Coordination with the affected Party regarding the management of public relations and public statements relating the Personal Data Breach.

1.7.3 The Supplier obligations under this section 1.7 shall be performed at the expense of the Party where the breach originated unless the Personal Data Breach arose out of negligence or wilful default of the Supplier or the Supplier should have known better or any breach by the Supplier of its obligations under this Agreement, in which case the costs shall be borne by the Supplier.

1.9. **Data Protection Impact Assessment:** If a Party believes or becomes aware to a reasonable degree of certainty that its processing of personal data for the Permitted Purposes is likely to result in a high risk to the Data Protection rights and freedoms of data subjects, it shall inform the affected Party and provide reasonable cooperation to that Party in connection with any Data Protection impact assessment that may be required under the Applicable Data Protection Laws.

1.10. **International transfers:** Both Parties are permitted to transfer Agreement Data outside of the UK. Agreement Data can only be transferred outside the UK to an adequate country, or, if a transfer risk assessment has been conducted, suitable controls put in place and the transfer is permissible under Data Protection laws with a binding transfer mechanism. Evidence of the legal transfer mechanism and controls shall be in place in advance of the data transfers.

1.11. **Appointing contractors or sub-processors**: There is general written authorisation in place for ELAS to appoint a contractor or sub-processor who will access Agreement Data.

1.12. **Cooperation and data subjects' rights:** Both Parties shall provide reasonable assistance to each other to enable a response to: (i) any request from a data subject to exercise any of its rights under the UK GDPR (including its rights of access, correction, objection, erasure and data portability, as applicable); and (ii) any other correspondence, enquiry or complaint received from a data subject, regulator or other third party in connection with the processing of personal data. In the event that any such request, correspondence, enquiry or complaint is made directly to either Party, the relevant Party shall inform the relevant Data Protection Officer within 24 hours of receipt. To the extent required by the Applicable Data Protection Laws, the relevant Party shall further provide such cooperation and information to the relevant Party as is reasonably necessary for the relevant Party to demonstrate compliance with its obligations pursuant to the Applicable Data Protection Laws.

1.13. **Records:** Each Party shall maintain complete, accurate and up to date written records of all its Processing of the Agreement Personal Data and as necessary to demonstrate its compliance with this Agreement and all applicable Data Protection Laws

1.14. **Deletion or return of personal data:** Upon the written request of the Supplier following the termination or expiry of this agreement, ELAS shall destroy or return to the Supplier all personal data in its possession or control to the extent legally permissible and/or technically practicable. This requirement shall not apply to the extent where ELAS are required or requested by applicable legal, regulatory, court, audit or bona fide internal compliance requirements to retain some or all personal data. ELAS further consents that the Supplier may delete in its sole discretion personal data where such data is shared with the Supplier but is not, in the reasonable opinion of ELAS, required or necessary for the Permitted Purposes.

1.15. **Security of Transfer:** Each Party shall ensure that where data is shared between either Party of the data subject it is done so using the appropriate technical measures to ensure the security and confidentiality of the data such as using encryption or signed for delivery.

1.16. **Amendment:** The terms of this agreement and the obligations of the parties under this agreement may only be amended or modified by written agreement between authorised parties within each business. Authorised individuals are limited to Directors and Data Protection Officer's.

1.17. **Governing law:** This agreement and obligations arising out of or in connection with it shall be governed by and construed in accordance with English Law and the parties irrevocably submit to the non-exclusive jurisdiction of the Courts of England and Wales in respect of any claim, dispute or difference arising out of or in connection with this agreement.

Data Processing Agreement

This data sharing agreement as defined below between the customer as identified by the service agreement and ELAS and will be effective on the data of such request**.**

Background

(A) The Provider provides services to the Customer pursuant to a separate services agreement or other arrangement agreed by the Parties that may require the Provider to process Personal Data on behalf of the Customer.

(B) This Personal Data Processing Agreement sets out the additional terms, requirements and conditions on which the Provider will process Personal Data when providing services to the Customer. This Agreement contains the mandatory clauses required by Article 28(3) of the UK General Data Protection Regulation for contracts between controllers and processors.

(C) For the avoidance of doubt and for the purpose of this data processing agreement, the Customer is the data controller and the Provider is the data processor.

1. Data Protection Provisions

1.1 The Provider shall:

(a) Comply with all applicable data protection law.

(b) Maintain accountability documentation in relations to agreement data

(c) Do so for the purpose of meeting our obligations under the Terms and Conditions and Service Agreement, or where the law permits us to do so.

(d) Act in accordance with your instructions or requests regarding the processing of personal data.

(e) Take appropriate organisational and technical measures to protect personal data against unauthorised or unlawful processing, and accidental loss, destruction or damage.

Those measures may take account of:

(f) The nature of the information and the harm which could arise from such processing, loss, destruction or damage; and

(g) The technology available; and

(h) The proportionality of taking those measures; and

(i) The cost of implementation.

1.2 We will not allow personal data to be transferred out of, or processed outside, the UK unless we have taken such measures as are necessary to ensure the transfer is compliant with all applicable data protection law.

1.3 We will not pass this personal data to any third party unless there is a legal or statutory obligation to do so, or:

(a) We have your permission; or

(b) We have entered into a written contract with a third party and they agree to meet obligations that are equivalent to those set out in this clause; or

(c) Where necessary in relation to, as part of, mergers and acquisitions.

1.4 The customer acknowledges we have general consent to appoint sub-processors in connection with the services provided.

We will only engage sub-processors where we have a written contract in place that imposes upon the sub-processor data protection obligations to the standard requried by applicable data protection laws

1.5 We will provide reasonable and timely assistance to assist you in dealing with data protection related requests relating to the data we hold, including to respond to:

(a) Requests from a data subject to exercise their rights under applicable data protection law.

(b) Not provide any information to the data subject relating to their rights without your prior written authorization.

(c) Any other correspondence, enquiry or complaint received from a data subject, regulator or other third party in connection with the data we hold.

1.6 We will provide reasonable assistance, with data protection impact assessments.

1.7 We will inform you of data breaches relating to your data without undue delay. Providing information on the nature of the breach, categories and number of affected individuals, description of likely consequences and measures we have taken to mitigate.

1.8 At the end of the contract, we will delete personal data provided for the purpose of this Contract unless we are requried by law, regulation or compliance to maintain it.

1.9 Upon customers written request, no more than once annually and subject to adequate confidentiality provisions, and in accordance with applicable data protection laws, make available to the customer such reasonable information in our possession or control to demonstrate compliance with obligations as a data processor and to satisfy customers data audit rights.