Controller Data Processing Terms and Conditions

These Controller Data Processing Terms and Conditions ("Controller Agreement") are offered by the Veritas entity which is the contracting party to the applicable Veritas agreement(s) in effect between our companies as mutually agreed and varied from time to time ("Agreement"), under which we have determined that the exchange of personal data between us is on an controller to controller basis. This Controller Agreement outlines the terms in which either party discloses personal data on a systematic and routine basis to the other party.

AGREED TERMS

1. INTERPRETATION

The following definitions apply in this Controller Agreement:

Data Protection Legislation: all applicable data protection and privacy legislation in force from time to time in the UK including the General Data Protection Regulation (*(EU) 2016/679*) ("**GDPR**"); the Data Protection Act 2018 and any other European Union legislation relating to personal data and all other legislation and regulatory requirements in force from time to time which apply to a party relating to the use of Personal Data.

Data Discloser means the party disclosing the Shared Personal Data.

Data Receiver means the party receiving the Shared Personal Data.

Shared Personal Data: the personal data to be shared between the parties under this Controller Agreement.

Supervisory Authority: the relevant supervisory authority in the territories where the parties to this Controller Agreement are established.

Term: means the duration of the Agreement.

Controller, **Processor**, **Data Subject**, **Personal Data**, **Special Categories of Personal Data**, **Processing, Personal Data Breach** and "**appropriate technical and organisational measures**" shall have the meanings given to them in the Data Protection Legislation.

2. PURPOSE

2.1 This Controller Agreement sets out the framework for the sharing of Personal Data when one Controller discloses Personal Data to another Controller. It defines the principles and procedures that the parties shall adhere to and the responsibilities the parties owe to each other.

2.2 The parties agree to only process Shared Personal Data for the purpose specified in the Agreement and shall not process Shared Personal Data in a way that is incompatible with such purpose (**Agreed Purpose**). The Shared Personal Data must not be irrelevant or excessive with regard to the Agreed Purposes.

3. COMPLIANCE WITH NATIONAL DATA PROTECTION LAWS

3.1 Each party must ensure compliance with applicable national data protection laws and Data Protection Legislation at all times during the Term of this Controller Agreement and the Agreement.

3.2 Each party acknowledges and confirms that, on request, it will provide the other party at its own expense (unless otherwise agreed) with reasonable assistance, information and cooperation to ensure compliance with

their respective obligations under Data Protection Legislation. Neither party shall do anything or permit anything to be done or avoided which might lead to a breach by the other party of its respective obligations under Data Protection Legislation.

4. LAWFUL, FAIR AND TRANSPARENT PROCESSING

4.1 Each party shall ensure that it processes the Shared Personal Data fairly and lawfully during the Term of this Controller Agreement. In addition, each party shall ensure that it has legitimate grounds under the Data Protection Legislation for the processing of Shared Personal Data.

4.2 The Data Discloser shall, in respect of Shared Personal Data, ensure that it provides clear and sufficient information to the Data Subjects, in accordance with the Data Protection Legislation, of the purposes for which it will process their personal data, the legal basis for such purposes and such other information as is required by Article 13 of the GDPR including:

4.2.1 if Shared Personal Data will be transferred to a third party, that fact and sufficient information about such transfer and the purpose of such transfer to enable the Data Subject to understand the purpose and risks of such transfer; and

4.2.2 if Shared Personal Data will be transferred outside the European Economic Area ("EEA") pursuant to clause 7 of this Controller Agreement, that fact and sufficient information about such transfer, the purpose of such transfer and the safeguards put in place by the controller to enable the Data Subject to understand the purpose and risks of such transfer.

5. DATA SUBJECTS' RIGHTS

5.1 If a Data Subject makes a written request to a party ("first Party") to exercise any of their Data Subject rights under Data Protection Legislation in relation to the Shared Personal Data in respect of which another party ("second Party") is the Controller, the first Party shall forward the request to the second Party immediately. The parties each agree to provide such assistance as is reasonably required to enable the other party to comply with requests from Data Subjects to exercise their rights under the Data Protection Legislation within the time limits imposed by the Data Protection Legislation.

6. DATA RETENTION AND DELETION

6.1 The Data Receiver shall not retain or process Shared Personal Data for longer than is necessary to carry out the Agreed Purposes. Notwithstanding this, parties shall continue to retain Shared Personal Data in accordance with any statutory or professional retention periods applicable in their respective countries and / or industry.

6.2 The Data Receiver shall at the request of the Data Discloser, ensure that any Shared Personal Data are returned to the Data Discloser or destroyed. Following such deletion of Shared Personal Data, the Data Receiver shall notify the Data Discloser that the Shared Personal Data in question has been deleted.

7. TRANSFERS AND THIRD PARTIES

7.1 If either party is located outside the EEA, the parties agree that by this Controller Agreement they enter into an agreement for and on behalf of themselves and each of their respective affiliates ("data export agreement") that incorporates the standard contractual clauses for the transfer of Personal Data to controllers established in third countries under the GDPR contained in the annex to European Commission decision 2010/87/EC of 5 February 2010. Each party shall execute (and procure the execution of) and perform (and procure the performance of) all such further export agreements or other appropriate documentation as may be required to ensure that any transfer of Personal Data to third countries undertaken in connection with the Agreement complies with Data Protection Legislation.

7.2 For the purposes of this clause, transfers of Personal Data shall mean any sharing of Personal Data by the Data Receiver with a third party, and shall include, but is not limited to, the following:

7.2.1 subcontracting the processing of Shared Personal Data;

7.2.2 granting a third-party controller access to the Shared Personal Data.

7.3 If the Data Receiver appoints a third-party processor to process the Shared Personal Data it shall comply with Article 28 and Article 30 of the GDPR and shall remain liable to the Data Discloser for the acts and/or omissions of the processor.

7.4 The Data Receiver may not transfer Shared Personal Data to a third party located outside the EEA unless it;

7.4.1 complies with the provisions of Articles 26 of the GDPR (in the event the third party is a joint controller); and

7.4.2 ensures that (i) the transfer is to a country approved by the European Commission as providing adequate protection pursuant to Article 45 of the GDPR; (ii) there are appropriate safeguards in place pursuant to Article 46 of the GDPR; or (iii) one of the derogations for specific situations in Article 49 of the GDPR applies to the transfer.

8. SECURITY AND TRAINING

8.1 The parties undertake to have in place throughout the Term appropriate technical and organisational security measures to:

8.1.1 prevent:

8.1.1.1 unauthorised or unlawful processing of the Shared Personal Data; and

8.1.1.2 the accidental loss or destruction of, or damage to, the Shared Personal Data.

8.1.2 ensure a level of security appropriate to:

8.1.2.1 the harm that might result from such unauthorised or unlawful processing or accidental loss, destruction or damage; and

8.1.2.2 the nature of the Shared Personal Data to be protected.

8.2 It is the responsibility of each party to ensure that its staff members are appropriately trained to handle and process the Shared Personal Data in accordance with the technical and organisational security measures set out in clause 8.1 together with any other applicable national data protection laws and have entered into confidentiality agreements relating to the processing of Personal Data.

9. PERSONAL DATA BREACHES AND REPORTING PROCEDURES

9.1 The parties shall each comply with its obligation to report a Personal Data Breach to the appropriate Supervisory Authority and (where applicable) data subjects under Article 33 of the GDPR and shall each inform the other party immediately and in any event within 48 hours of any Personal Data Breach irrespective of whether there is a requirement to notify any Supervisory Authority or data subject(s). Such notice to the other party shall include reasonable details of the Personal Data Breach including without limitation: (i) a description of the Personal Data Breach; (ii) likely consequences of the Personal Data Breach; (iii) the number of Data Subjects affected, number of records affected and the types of records affected; and (iv) the measures taken or proposed to be taken to address the Data Protection Breach, including measures to mitigate possible adverse effects.

9.2 The parties agree to provide reasonable assistance as is necessary to each other to facilitate the handling of any Personal Data Breach in an expeditious and compliant manner.

9.3 If either party receives any complaint, notice or communication from a Supervisory Authority which relates

directly or indirectly to the other party's: (i) processing of the Shared Personal Data as a controller; or (ii) a potential, alleged or actual failure to comply with Data Protection Legislation in respect to the Shared Personal Data, the Data Receiving Party shall, to the extent permitted by law, promptly forward the complaint, notice or communication to the other party and provide the other party with reasonable co-operation and assistance in relation to the same.

10. CHANGES TO THE APPLICABLE LAW

10.1 If during the Term the Data Protection Legislation change in a way that the Controller Agreement is no longer adequate for the purpose of governing lawful data sharing exercises, the parties agree that they will negotiate in good faith to review the Controller Agreement in the light of the new legislation.

11. MISCELLANEOUS

11.1 In the event of any conflict or inconsistency between the provisions of the Agreement and this Controller Agreement, the provisions of this Controller Agreement shall prevail. Save as specifically modified and amended in this Controller, all the terms, provisions and requirements contained in the Agreement shall remain in full force and effect and govern this Controller.

11.2 This Controller Agreement and any dispute or claim (including non-contractual disputes or claims) arising out of, or in connection with them or their subject matter or formation shall be governed by and interpreted in accordance with the law which governs the Agreement, and the Parties irrevocably agree that the courts that have exclusive jurisdiction to settle any dispute or claim (including non-contractual disputes or claims) that rises out of, or in connection with, the Agreement, or its subject matter or formation, shall also have exclusive jurisdiction in relation to any disputes or claims arising from this Controller Agreement.