**INTERPRETATION**

* 1. In this agreement:
1. **“Data Protection Laws”** means the GDPR and the Privacy and Electronic Communication Regulations 2003, any amendment, consolidation or re-enactment thereof, any legislation of equivalent purpose or effect enacted in the United Kingdom, or, where relevant, the European Union, and any orders, guidelines and instructions issued under any of the above by relevant national authorities, a judicial authority in England and Wales or, where relevant, a European Union judicial authority;
2. **“GDPR”** means the General Data Protection Regulation (EU) 2016/679 as in force from time to time;
3. **“Personal Data”** has the meaning given to it by the GDPR, but shall only include personal data to the extent that such personal data, or any part of such personal data, is processed in relation to the services provided under this agreement; and
4. **“Replacement National Legislation”** means legislation in the United Kingdom which is enacted to cover, in whole or part, the same subject matter as the GDPR.
	1. Words and phrases with defined meanings in the GDPR have the same meanings when used in this Agreement.
	2. If the GDPR ceases to apply to the United Kingdom, references to the GDPR, to provisions within it and to words and phrases with defined meanings in it, shall be deemed references to Replacement National Legislation, the nearest equivalent provisions in it and the nearest equivalent words and phrases in it (as the case may be).
	3. For the avoidance of doubt, compliance with this Agreement shall not relieve the Supplier of any of its direct obligations under the GDPR.
5. **DETAILS OF PROCESSING**
	1. The following details apply to the processing being carried out under this agreement:
		1. The Personal Data will be processed for the provision of Services as set out in the agreement.
6. **OBLIGATIONS**
	1. Each party shall comply with the Data Protection Laws applicable to it in connection with this agreement, and shall not cause the other party to breach any of its obligations under Data Protection Laws.
	2. Where a party, or a sub-contractor of a party, processes Personal Data (that party being the **"Processor"**) on behalf of the other party or a member of its group (that party being the **"Controller"**) in connection with this agreement, the Processor shall, or shall ensure that its sub-contractor shall:
		1. process the Personal Data only on behalf of the Controller, only for the purposes of performing its obligations under this agreement, and only in accordance with instructions contained in this agreement or instructions received in writing from the Controller from time to time. The Processor shall notify the Controller if, in its opinion, any instruction given by the Controller breaches Data Protection Laws or other applicable law;
		2. not publish, disclose or divulge any of the Personal Data to any third party (including for the avoidance of doubt the data subject itself), unless directed to do so in writing by the Controller;
		3. document all processing in accordance with Article 30 of the GDPR;
		4. only grant access to the Personal Data to persons who need to have access to it for the purposes of performing this agreement and, to the extent such persons are granted access, that they are only granted access to the part or parts of the Personal Data necessary for carrying out their role in performance of this agreement;
		5. ensure that all persons with access to the Personal Data are:
			1. reliable**,** trustworthy and suitably trained on Data Protection Laws and as a result are aware of the Processor’s duties as a processor and their personal obligations with regards to this agreement and Data Protection Laws;
			2. subject to an obligation of confidentiality or are under an appropriate statutory obligation of confidentiality; and
			3. notified of the confidential nature of the Personal Data;
		6. as a minimum, take all measures required pursuant to Article 32 of the GDPR in accordance with best practiceand provide a written description of, and rationale for, each of the technical and organisational measures implemented, or to be implemented, to:
			1. protect the Personal Data against unauthorised or unlawful processing and accidental loss, destruction, damage, alteration or disclosure; and
			2. detect and report Personal Data breaches within good time;
		7. not engage another processor (a **“Sub-Processor”**) to process the Personal Data on its behalf without specific written consent of the Controller, approving a named Sub-Processor, such consent always subject to:
			1. the Processor binding any Sub-Processor by written agreement, imposing on the Sub-Processor obligations in relation to the Personal Data equivalent to those set out in this agreement, and a right to procure that the Sub-Processor ceases processing without delay on termination of this agreement; and
			2. the Processor remaining liable to the Controller for the acts and omissions of any Sub-Processor, as if they were the acts and omissions of the Processor;
		8. notify the Controller within five business days if it receives any communication from a third party relating directly or indirectly to the processing of the Personal Data, including but not limited to requests to exercise rights under Data Protection Laws, complaints or general correspondence and shall provide the Controller with a copy of any such communication. The Processor shall not take action in relation to such communication, unless compelled by law, without the Controller’s prior approval, and shall comply with any instructions the Controller gives in relation to such communication;
		9. taking into account the nature of the processing and so far as is possible, assist the Controller with the fulfilment of the Controller’s obligation to respond to requests for exercising data subject’s rights under the Data Protection Laws and in responding to any other request, complaint or communication by, but not limited to, providing information requested by the Controller and relevant Personal Data within a reasonable time and in a commonly used electronic format, taking into account the timescales for the Controller complying with the data subject’s request under Data Protection Laws;
		10. taking into account the nature of the processing and the information available to the Processor, assist the Controller in ensuring compliance with its obligations pursuant to Articles 32 to 36 of the GDPR inclusive. Such assistance shall include, but shall not be limited to:
			1. notifying the Controller immediately upon discovering a Personal Data breach, providing all information it has, or reasonably should have, in relation to the Personal Data breach, so that the Controller is able to satisfy its obligations under Articles 33 and 34 of the GDPR and is able to properly investigate the Personal Data breach;
			2. assisting in the risk assessment of the processing of the Personal Data which the Processor carries out under this agreement in order that the Controller is able to complete a data protection impact assessment in compliance with Article 35 of the GDPR, and consult with a relevant supervisory authority if necessary in compliance with Article 36 of the GDPR,including providing information about the Processor’s current technical and organisational measures, and what further measures it could put in place to mitigate any risks to the rights and freedoms of data subjects, and the risks of Personal Data breach in relation to the Personal Data, as identified by it or the Controller;
		11. at the Controller’s option, delete or return to the Controller the Personal Data, and procure that any party to whom the Processor has disclosed the Personal Data does the same:
			1. when the Controller instructs the Processor to do so, in which case the Processor shall be excused from its obligations under this agreement to the extent that such action prevents it from complying with those obligations; or
			2. after the termination of Services under this agreement which involve processing the Personal Data,
7. such obligation to include deleting or returning all copies of the Personal Data, unless applicable law requires the Processor to retain the Personal Data. Where the Controller requests the return of Personal Data, the Processor shall use all reasonable endeavours to ensure it is in the format and on the media specified by the Controller;
	* 1. comply with any instructions of the Controller to modify the Personal Data, or restrict its processing, and procure that any party to whom the Processor has disclosed the Personal Data does the same;
		2. where reasonably possible, store the Personal Data in a structured, commonly used and machine readable format;
		3. not transfer Personal Data outside of the European Economic Area without the prior written consent of the Controller. Where the Controller consents to the transfer of Personal Data outside the European Economic Area, the Processor shall comply with:
			1. the obligations of a controller under Articles 44 to 50 of the GDPR inclusive by providing an adequate level of protection to any Personal Data transferred; and
			2. any reasonable instructions of the Controller in relation to such transfer;
		4. have a data protection officer where required by the GDPR, and where a data protection officer is not required, have a named individual that is responsible and available to deal with data protection issues as and when they arise in conjunction with the Controller;
		5. make available to the Controller all information necessary to demonstrate compliance with this agreement insofar as it relates to data protection; and
		6. allow the Controller, or its external advisers (subject to reasonable and appropriate confidentiality undertakings), to inspect and audit the Processor’s data processing activities and those of its relevant agents, group companies and sub-contractors, and comply with all reasonable requests or directions by the Controller, to enable to Controller to verify and procure that the Processor is in full compliance with its obligations under this agreement insofar as it relates to data protection**.**
	1. Notwithstanding anything in this agreement, information provided by a Processor to a Controller, whether through audit or otherwise, may be disclosed by the Controller if requested or required generally or specifically by applicable law, a court of competent jurisdiction, a supervisory authority, a certification body (as referred to by Article 43 of the GDPR) or a monitoring body (as referred to by Article 41 of the GDPR) for the purposes of responding to a claim, request for information, inquiry or investigation.