DPA TERMS AND CONDITIONS

The parties agree to comply with the following provisions with respect to any Personal Data Processed by IgnitionOne for Customer in connection with the provision of the Services. References to the Agreement will be construed as including these DPA Terms and Conditions ("DPA"). To the extent that the terms of this DPA differ from those in the Agreement, the terms of this DPA shall govern to the extent they pertain to Personal Data. Any capitalized terms not defined herein shall have the respective meanings given to them in the Agreement.

1 DEFINITIONS

1.1 "**Affiliates**" means any entity which is controlled by, controls or is in common control with one of the parties.

1.2 "**Data Protection Laws**" means all privacy and data protection laws and regulations applicable to the Processing of Personal Data under the Agreement, including, as applicable: (a) the GDPR; and/or (b) the Federal Data Protection Act of 19 June 1992 (Switzerland) and applicable to the Processing of Personal Data under the Agreement.

1.3 "**Data Subject**" means the individual to whom Personal Data relates.

1.4 "**Effective Date**" shall have the meaning ascribed to such term in the IgnitionOne Data Processing Agreement

1.5 "**GDPR**" means 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.

1.6 "**Privacy Shield**" means the EU-US Privacy Shield Framework and the Swiss-US Privacy Shield Framework as set forth by the US Department of Commerce.

1.7 "**Security Breach**" has the meaning set forth in Section 7 of this DPA.

1.8 "**Sub-processor**" means any sub-processor engaged by IgnitionOne for the Processing of Personal Data.

1.9 "**Term**" means the period from the Effective Date to the date the DPA is terminated in accordance with Section 10.1.

1.10 "**Third Party Partner**" means any entity engaged by Customer for the Processing of Personal Data.

1.11 The terms "**Controller**", "**Personal Data**", "**Processor**," and "**Processing**," have the meanings given to them in Applicable Privacy Laws. If and to the extent that Applicable Privacy Laws do not define such terms, then the definitions given in EU Data Protection Law will apply.

2 PROCESSING OF PERSONAL DATA

2.1 The parties agree that Customer is the Data Controller and IgnitionOne is a Data Processor and that the subject matter and details of the processing of such Personal Data are described in Exhibit 1 to the Data Processing Agreement. To the extent that the data protection legislation of another jurisdiction is applicable to either party's processing of data, the parties acknowledge and agree that the relevant party will comply with any obligations applicable to it under that legislation with respect to the processing of that data. IgnitionOne shall keep a record of all processing activities with respect to Customer's Personal Data as required under GDPR.

2.2 Each party will comply with the obligations applicable to it under the Data Protection Legislation with respect to the processing of Personal Data, including but not limited to providing the other party contact details for each party's Data Protection Officer which are accurate and up to date. Customer shall, in its use or receipt of the Services, Process Personal Data in accordance with the requirements of the Data Protection Laws and Customer will ensure that its instructions for the Processing of Personal Data shall comply with the Data Protection Laws. If IgnitionOne believes or becomes aware that any of Customer's instructions conflicts with any Data Protection Laws, IgnitionOne shall inform Customer. As between the parties, Customer shall have sole responsibility for determining the legal basis for processing of Personal Data and (to the extent legally required) obtain all consents from Data Subjects necessary for collection and Processing of Personal Data in the scope of the Services.

2.3 The objective of Processing of Personal Data by IgnitionOne is the performance of the Services pursuant to the Agreement. During the Term of the Agreement, IgnitionOne shall only Process Personal Data on behalf of and in accordance with the Agreement and Customer's instructions and shall treat Personal Data as Confidential Information. Customer instructs IgnitionOne to Process Personal Data for the following purposes: (i) Processing in accordance with the Agreement in order to provide the Services; and (ii) Processing to comply with other reasonable instructions provided by Customer where such instructions are acknowledged by IgnitionOne as consistent with the terms of the Agreement. IgnitionOne may Process Personal Data other than on the instructions of the Customer if it is mandatory under applicable law to which IgnitionOne is subject. In this situation IgnitionOne shall inform the Customer of such a requirement unless the law prohibits such notice.

3 RIGHTS OF DATA SUBJECTS; DATA DELETION

3.1 As the Data Controller, Customer has the primary responsibility for honouring Data Subject access requests. IgnitionOne shall provide reasonable and timely assistance to the Customer (at the Customer's expense) to enable the Customer to respond to: (i) any request from a Data Subject to exercise any of its rights under Data Protection Law (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 in connection with the processing of the Personal Data. In the event that any such request, correspondence, enquiry or complaint is made directly to the IgnitionOne (a "Direct Access Request"), IgnitionOne shall to the extent legally permitted, promptly inform the Customer providing full details of the same and, upon request, provide the Customer with contact details of the Data Subject(s). If Customer fails to respond to a Direct Access Request within 30 days, IgnitionOne reserves the right to take appropriate steps in its reasonable judgement to respond to such request(s).

4 IGNITIONONE PERSONNEL

4.1 IgnitionOne shall ensure that its personnel engaged in the Processing of Personal Data are informed of the confidential nature of the Personal Data as well as any security obligations with respect to such Data.

4.2 IgnitionOne will take appropriate steps to ensure compliance with the Security Measures outlined in **Appendix 1** by its personnel to the extent applicable to their scope of performance, including ensuring that all persons authorized to process Customer Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality and that any such obligations survive the termination of that individual's engagement with IgnitionOne.

4.3 IgnitionOne shall ensure that access to Personal Data is limited to those personnel who require such access to perform the Services.

5 SUB-PROCESSORS

5.1 Customer acknowledges and agrees that (i) IgnitionOne Affiliates may be retained as Sub-processors; and (ii) IgnitionOne may engage third-party Sub-processors in connection with the provision of the Services. Any such Sub-processors will be permitted to obtain Personal Data only to deliver the services IgnitionOne has retained them to provide, and are prohibited from using Personal Data for any other purpose. IgnitionOne will have a written agreement with each Sub-processor and agrees that any agreement with a Sub-processor will include substantially the same data protection obligations as set out in this DPA.

5.2 A list of Sub-processors is available in the IgnitionOne user interface or at a particular web page hosted by IgnitionOne. IgnitionOne may change the list of such other Sub-processors by no less than 5 business days' notice via the IgnitionOne user interface. If Customer objects to IgnitionOne's change in such Sub-processors, IgnitionOne may, as its sole and exclusive remedy, terminate the portion of the Agreement relating to the Services that cannot be reasonably provided without the objected-to new Sub-processor by providing 30 days' written notice to Customer.

5.3 IgnitionOne shall be liable for the acts and omissions of its Sub-processors to the same extent IgnitionOne would be liable if performing the services of each Sub-processor directly under the terms of this DPA, except as otherwise set forth in the Agreement.

5.4 Customer acknowledges and agrees that Third Party Partners are not Sub-processors and IgnitionOne assumes no responsibility or liability for the acts or omissions of such Third Party Partners.

6 SECURITY; AUDIT RIGHTS; PRIVACY IMPACT ASSESSMENTS

6.1 IgnitionOne shall maintain administrative, physical and technical safeguards for protection of the security, confidentiality and integrity of Customer's Personal Data. IgnitionOne will implement and maintain technical and organizational measures to protect Personal Data against accidental or

unlawful destruction, loss, alteration, unauthorized disclosure or access as described in Appendix 1 (the "Security Measures"). As described in Appendix 1, the Security Measures include measures to encrypt Personal Data; to help ensure ongoing confidentiality, integrity, availability and resilience of IgnitionOne's systems and services; to help restore timely access to Personal Data following an incident; and for regular testing of effectiveness. IgnitionOne may update or modify the Security Measures from time to time provided that such updates and modifications do not result in the degradation of the overall security of the Services.

6.2 IgnitionOne will (taking into account the nature of the processing of Customer Personal Data and the information available to IgnitionOne) assist Customer in ensuring compliance with any of Customer's obligations with respect to the security of Personal Data and Personal Data breaches, including (if applicable) Customer's obligations pursuant to Articles 32 to 34 (inclusive) of the GDPR, by: (a) implementing and maintaining the Security Measures in accordance with Appendix 1; and (b) complying with the terms of Section 7 of this DPA.

6.3 No more than once per year, Customer may engage a mutually agreed upon third party to audit IgnitionOne solely for the purposes of meeting its audit requirements pursuant to Article 28, Section 3(h) of the General Data Protection Regulation ("GDPR"). To request an audit, Customer must submit a detailed audit plan at least four (4) weeks in advance of the proposed audit date describing the proposed scope, duration, and start date of the audit. Audit requests must be sent to auditrequests@IgnitionOne.com. The auditor must execute a written confidentiality agreement acceptable to IgnitionOne before conducting the audit. The audit must be conducted during regular business hours, subject to IgnitionOne's policies, and may not unreasonably interfere with IgnitionOne's business activities. Any audits are at Customer's expense.

6.4 Any request for IgnitionOne to provide assistance with an audit is considered a separate service if such audit assistance requires the use of resources different from or in addition to those required by law. Customer shall reimburse IgnitionOne for any time spent for any such audit at the rates agreed to by the parties. Before the commencement of any such audit, Customer and IgnitionOne shall mutually agree upon the scope, timing, and duration of the audit in addition to the reimbursement rate for which Customer shall be responsible. All reimbursement rates shall be reasonable, taking into account the resources expended by IgnitionOne.

6.5 Customer shall promptly notify IgnitionOne with information regarding any non-compliance discovered during the course of an audit.

7 SECURITY BREACH MANAGEMENT AND NOTIFICATION

7.1 If IgnitionOne becomes aware of any accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to any Customer Personal Data transmitted, stored or otherwise Processed on IgnitionOne's equipment or facilities ("Security Breach"), IgnitionOne will promptly notify Customer of the Security Breach. Notifications made pursuant to this section will describe, to the extent possible, details of the Security Breach, including steps taken to mitigate the potential risks and steps IgnitionOne recommends Customer take to address the Security Breach.

7.2 Customer agrees that an unsuccessful Security Breach attempt will not be subject to this Section. An unsuccessful Security Breach attempt is one that results in no unauthorized access to

Customer Personal Data or to any of IgnitionOne's equipment or facilities storing Customer Personal Data, and may include, without limitation, pings and other broadcast attacks on firewalls or edge servers, port scans, unsuccessful log-on attempts, denial of service attacks, or similar incidents.

7.3 Notification(s) of Security Breaches, if any, will be delivered to one or more of Customer's business, technical or administrative contacts by any means IgnitionOne selects, including via email. It is Customer's sole responsibility to ensure it maintains accurate contact information on IgnitionOne's support systems at all times.

7.4 IgnitionOne's notification of or response to a Security Breach under this Section 7 will not be construed as an acknowledgement by IgnitionOne of any fault or liability with respect to the Security Breach.

7.5 IgnitionOne shall implement reasonable technical and organizational Security Measures to provide a level of security appropriate to the risk in respect to the Customer Personal Data. As technical and organisational measures are subject to technological development, IgnitionOne is entitled to implement alternative measures provided they do not fall short of the level of data protection set out by Data Protection Law.

8 RETURN AND DELETION OF PERSONAL DATA

8.1 IgnitionOne will delete all directly identifying Personal Data seven (7) days after it has been transferred (exported) to Customer. When transferring such data to Customer, IgnitionOne will add a record per Data Subject that documents how and when consent for Processing of his/her directly identifying Personal Data was obtained by Customer.

8.2 IgnitionOne may enable Customer to delete Personal Data during the Term in a manner consistent with the functionality of the Services. If Customer uses the Services to delete any Personal Data during the Term, this use will constitute an instruction to IgnitionOne to delete the relevant Personal Data from IgnitionOne's systems in accordance with Data Protection Laws.

8.3 IgnitionOne will comply with instructions from the Customer to delete certain Personal Data as soon as reasonably practicable and within a maximum period of 30 days, unless Data Protection Law (or, in the case the data is not subject to Data Protection Law, applicable law) requires further storage.

8.4 On expiry of the Agreement, Customer instructs IgnitionOne to delete all Personal Data (including existing copies) from IgnitionOne's systems and discontinue processing of such Personal Data in accordance with Data Protection Law. IgnitionOne will comply with this instruction as soon as reasonably practicable and within a maximum period of 30 days, unless Data Protection Law (or, in the case the data is not subject to Data Protection Law, applicable law) requires further storage. This requirement shall not apply to the extent that IgnitionOne has archived Customer Data on back-up systems so long as IgnitionOne securely isolates and protect such data from any further processing except to the extent required by applicable law. Without prejudice to this Section, Customer acknowledges and agrees that Customer will be responsible for exporting, before the Agreement expires, any Personal Data it wishes to retain afterwards. Notwithstanding the

foregoing, the provisions of this DPA will survive the termination of this Agreement for as long as the IgnitionOne retains any of the Customer Personal Data.

9 CROSS-BORDER DATA TRANSFERS, PRIVACY SHIELD

9.1 IgnitionOne may, subject to this Section 9, store and process the relevant Personal Data in the European Economic Area, the United States and Sri-Lanka.

9.2 IgnitionOne self-certified to and complies with the Privacy Shield, and IgnitionOne shall maintain its self-certification to and compliance with the Privacy Shield with respect to the Processing of Personal Data that is transferred from the European Economic Area or Switzerland to the United States.

9.3 At the request of Customer, or if the Services involve the storage and/or Processing of Customer Personal Data which transfers Customer Personal Data out of the European Economic Area to a jurisdiction other than the United States that does not have adequate data protection laws, and the EU Data Protection Laws apply to the transfers of such data ("Transferred Personal Data"), the parties will enter into Model Contract Clauses or find an alternative legal basis for such Transferred Personal Data which is in compliance with Data Protection Laws.

10 MISCELLANEOUS

10.1 This DPA will take effect on the Effective Date and will remain in effect until, and automatically expire upon, the deletion of all Personal Data by IgnitionOne or Customer through the Services as described in this DPA.

10.2 Nothing in this DPA shall confer any benefits or rights on any person or entity other than the parties to this DPA.

10.3 Where Customer's Affiliates are Data Controllers of the Personal Data, they may enforce the terms of this DPA against IgnitionOne directly.

10.4 Nothing in this Section 10 will affect the terms of the Agreement relating to liability (including any specific exclusions from any limitation of liability).

APPENDIX 1 SECURITY MEASURES

IgnitionOne implements the following security measures in relation to its Services:

1. **Physical Controls:**
Physical access to the IgnitionOne premises is controlled through a key card controlled entry gate. Any non-employees entering the premises are required to register themselves at a manned reception desk before being granted access to the premises.

2. **Access Control:**
IgnitionOne has established adequate procedures for permitting users to access terminals and servers. Each IgnitionOne employee has a unique user ID and pass-word. An appropriate user registration procedure is in place and new employees are assigned an auto-generated password that is required to be changed after the first login. Employees leaving the company are immediately de-registered. Devices containing client data are wiped before disposal.

IgnitionOne has established adequate procedures for identifying the users who have access to devices and servers and the data stored thereon. All IgnitionOne systems are secured via one of 2 systems: Microsoft Active Directory or RSA Mutual Key authentication. In both cases, access to individual devices and underlying data are restricted to the role of employee to ensure segregation of duties in compliance with ISO 27001 practices. Access to data is therefore strictly limited to those employees who need to have access to such data for the purpose of providing the services to the specific client. Security access logs are stored and validated to ensure access to systems is restricted to the proper audience.

3. **Transmission Control:**
IgnitionOne's follows strict secure, encrypted data transmission practices when communicating client data to any approved external entity. Internally, IgnitionOne uses secured VPN tunnels for any transmission or access to datasets across IgnitionOne facilities. A secure private network is used for processing client data within IgnitionOne datacenters.

4. **Input Control:**
Input of or editing data in the IgnitionOne systems is restricted to individual roles in the organization where it is required to perform duties. Input validation checks are used to validate data entered by system users. Internal administrators have elevated access to perform regular job duties such as testing and other maintenance oriented tasks.

5. **Audit Control:**
At all points, access logs for the systems are maintained to track actions within systems for auditing / investigation purposes. At all points, access logs for the systems are maintained to track actions within systems for auditing / investigation purposes. System access is granted on an individual basis so tying the system change with the specific user is possible within access logs.

6. **Availability Control:**
IgnitionOne has implemented routine back-up procedures to prevent accidental destruction or loss of data. IgnitionOne has implemented processes to immediately deploy services and data if/when necessary. Additionally, IgnitionOne has automatic failover redundancy through three replicated datacenters.

7. Data Storage:
IgnitionOne utilizes Transparent Data Encryption on its databases as well as file system encryption to protect data stored in both structured and unstructured formats while at rest.

8. Confidentiality Control:
All employees who have access to the client data have a confidentiality clause in their employment agreement and are made aware of the confidential and proprietary nature of data and the contents of this agreement. Employees are informed and trained on the obligations applicable to them with respect to data protection on a recurring annual basis.