RECENT UPDATES

- Updated throughout to remove reference to the Data Protection Act 1998 and to correctly reference the new General Data Protection Regulation (GDPR) legislation.
- **Customer's Responsibility** section updated to clarify the responsibility of the Data Controller in regard to Data Subjects.
- **Data Location** section updated to specify UK location of data and also to specify relocation within parameters of Data Processor responsibilities.
- **Security** section updated to reference ASPL's new Information Security Policy.

Cloud Service Agreement Attachment 3: Data Protection (2018-05-21)

This Data Protection attachment is only to be construed alongside the Cloud Service Agreement (CSA). It forms part of the CSA as per Section 1 of that document and runs concurrently with it. This Data Protection attachment specifically describes responsibilities in connection with ASPL's Cloud service.

DESIGNATION OF ASPL AS DATA PROCESSOR

The Customer designates ASPL as Data Processor with regard to Customer Personal Data within the scope of the CSA and ASPL agrees to act as Data Processor in accordance with the terms of the CSA and this Data Protection attachment. ASPL shall process Customer Personal Data solely for the purpose of the provision of the Services under the CSA.

ASPL may process certain personal data as a Data Controller as set out in the Privacy Policy, specifically in regard to the Customer, the Customer's employees and employed third parties (e.g. contractors).

CUSTOMER'S RESPONSIBILITY

The Customer qualifies as Data Controller of the set of Processing carried out by ASPL on the Customer's behalf and is fully responsible for abiding by Data Protection Laws and Regulations (such as the General Data Protection Regulation (GDPR)) and for compliance with its obligations, including ensuring the lawful basis for both the Customer's and ASPL's lawful processing of Customer Personal Data under the CSA, e.g. filing any required notifications or authorisation, providing notices to and obtaining consent (as applicable) from Data Subjects. As the Data Controller, it is the Customer's responsibility to ensure the individual rights of Data Subjects are upheld.

ASPL qualifies as Data Processor upon signature of the CSA and will remain as such as long as it (i) complies with the Customer's reasonable and legitimate instructions, including the instructions set out under this Attachment, (ii) provides adequate monitoring procedures regarding compliance with such instructions, (iii) does not go beyond the mandate given by the Customer by acquiring a relevant role in determining the purposes or the essential means of Processing.

TYPES AND CATEGORIES OF PERSONAL DATA

In order to execute the CSA and to perform the Services on behalf of the Customer, the Customer authorises and requests the Processor to Process the following Personal Data:

1. Categories of Personal Data: Personal Data may include, among other information, personal contact information such as name, home address, home telephone or mobile number, fax number, email address and passwords, financial details, etc.;
2. Categories of Data Subjects: Data Subjects include the Customer's clients.

DATA LOCATION

ASPL declares and warrants that for the provision of the Services it will use exclusively data centres located within the UK.

On occasion for maintenance purposes we will relocate customer databases in order to preserve the security, resilience and scalability of that database and its data, in order to continue legitimately fulfilling ASPL's responsibilities as Data Processor. This will not lead to databases being moved outside of the UK.

RIGHTS OF THE DATA SUBJECTS

To the extent legally permitted, ASPL agrees to promptly notify the Customer if it receives any requests, notices or other communication from Data Subjects for access to, correction, amendment, blocking, deletion of that Data Subject's Personal Data or objection to the processing of Personal Data of that Data Subject.

ASPL shall not respond to or act upon any such Data Subjects' request without the Customer's prior written consent, as ASPL is merely the Processor and not the Controller of the data.

SECURITY

ASPL shall implement and maintain appropriate technical and organisational measures to protect Personal Data against unauthorised or unlawful processing of personal data and against accidental loss, destruction or damage to Personal Data.

In the event that ASPL becomes aware of any confirmed security breaches (e.g. any accidental, unauthorised or unlawful destruction, loss, alteration, or disclosure of, or access to Customer Personal Data) or breaches of any provision of the GDPR, or in the event that ASPL is contacted by a supervisory authority for data protection violation (to the extent ASPL is permitted to notify under law), ASPL will promptly notify the Customer.

In the event of a security breach, ASPL shall cooperate with the Customer to identify and remediate the cause of such breach.

In addition, our Information Security Policy describes our approach to data security and our commitment to secure practices in general.

DATA RETENTION

Data uploaded to the service will be retained in accordance with Section 10 (Termination and Expiration) of the CSA.