Data Processing Addendum

This Data Processing Addendum (the "DPA") forms part of the Master SaaS Agreement, Master Hosted Software Subscription and Services Agreement, Master Software License and Services Agreement, and any agreement involvement the processing of personal data by PowerPlan, Inc. ("PowerPlan") on behalf of Client ("Agreement"). Client is the entity identified as such in the Agreement. Upon full execution of the Agreement (the "Addendum Effective Date"), this DPA will be incorporated into and become a part of the Agreement. In the event of a conflict between the DPA and Agreement, the terms and conditions of the DPA will prevail. PowerPlan and Client may collectively be referred to as the "Parties."

1. Definitions

Terms defined in the Agreement will, unless otherwise defined in this DPA, have the same meanings when used in this DPA. Further, the following capitalised terms used in this DPA will be defined as follows:

"Applicable Data Protection Law" refers to all laws and regulations applicable to PowerPlan's processing of Personal Data under the Agreement.

"Controller" means the Client when, alone or jointly with others, it determines the purpose and means of processing Personal Data.

"Client Account Data" means Personal Data that relates to Client's relationship with PowerPlan, including the names and contact information of the individuals authorized by Client to access Client's account and billing information of individuals that Client has associated with its Account. Client Account Data also includes any data PowerPlan may need to collect for the purpose of identity verification (e.g., providing multi-factor authentication services) or as part of its legal obligations to maintain records.

"Client Data" means any Client-provided, non-public or proprietary information exchanged as a result of using the Service form, including Personal Data processed by PowerPlan on behalf of Client in connection with the Services, as further described in Schedule 1. This includes the non-public or proprietary information (including Personal Data) of Client clients for whom Client acts as a processor.

"Data Subject" means a natural person who can be identified, directly or indirectly.

"Personal Data" means any information relating to a natural person who can be identified, directly or indirectly.

"process" or "processing" means any operation or set of operations which is performed upon Client Data whether or not by automated means.

"Processor" means the PowerPlan when the PowerPlan processes Personal Data on behalf of Client.

"Security Breach" means a breach of PowerPlan's security resulting in the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Client Data.

"Services" has the same meaning as defined in the Agreement, or if not defined in the Agreement, the processing of Client Data by the PowerPlan on behalf of the Client described in the Agreement.

"Subprocessor" means a processor appointed by the PowerPlan to process Client Data.

2. Instructions for Data Processing

2.1. *Generally*. The Agreement and this DPA will be the Client's instructions to PowerPlan for the processing of Client Data. PowerPlan will process Client Data solely for the purpose of providing the Services and will ensure that all individuals with access to the Client Data have a duty of confidentiality with respect to that Client Data. PowerPlan will not sell, share, disclose, retain, or otherwise use Client Data for any other purpose unless specifically instructed by Client in writing or as required by law.

2.2. *Regulatory and Legal Compliance*. PowerPlan will process Client Data in compliance with Applicable Data Protection Law. PowerPlan will provide reasonable assistance to Client in complying with its obligations under Applicable Data Protection Law. Unless prohibited by law, PowerPlan will notify Client promptly of any inquiries or complaints received about the processing of Personal Data from regulators or law enforcement authorities. PowerPlan will not respond to any such inquiries or complaints except on the documented instructions of Client or as required by law. If disclosure of Client Data is required by applicable law or a compulsory legal process, PowerPlan will, unless prohibited by applicable law: (i) notify Client promptly in writing before complying with any such disclosure request and provide Client an opportunity to intervene, if appropriate; and (ii) disclose only the minimum amount of Client Data necessary to comply with applicable law or a compulsory legal process.

2.3. *Data Subject Rights.* Unless prohibited by law, PowerPlan will promptly notify Client of any request from a data subject with respect to Personal Data contained in Client Data. PowerPlan will not respond to any data subject request without Client's prior written consent, except to confirm that the request relates to Client. PowerPlan will provide reasonable and timely assistance to Client in complying with its data protection obligations with respect to data subject rights under Applicable Data Protection Law.

2.4. *Additional Costs*. If any of the Client's instructions require processing Client Data in a manner that falls outside the scope of the Services, the PowerPlan may either (a) make the performance of any such instructions subject to the payment by the Client of any costs and expenses incurred by the PowerPlan or such additional charges as the PowerPlan may reasonably determine; or (b) terminate the Agreement and the Services.

3. Client Warranties and Undertakings

The Client represents and warrants that: (a) it has provided all applicable notices and obtained all required consents required for the lawful processing of Client Data; and (b) it has reviewed the security measures set out in Schedule 2 and agrees that the security measures are appropriate based on the nature and sensitivity of the Client Data.

4. Subprocessors

4.1. *Conditional Authorization.* Client provides a general authorization for PowerPlan to engage downstream Subprocessors that is conditioned on the following requirements:

(a) PowerPlan will impose contractual data protection obligations on any Subprocessor it appoints to process Client Data to meet the standards required by Applicable Data Protection Law and this DPA; and

(b) PowerPlan will remain liable for any breach of this Addendum that is caused by an act, error, or omission of its Subprocessors.

4.2. *Current Subprocessors and Notification of Changes*. Client authorizes PowerPlan to engage Subprocessors to process Client Data. PowerPlan will provide a list of Subprocessors upon written request. PowerPlan will notify Client of changes to its Subprocessors. Client may object to PowerPlan's appointment or replacement of a Subprocessor within 14 days of the notification, provided such objection is in writing and based on reasonable grounds relating to data protection. In such an event, the parties agree to discuss commercially reasonable alternative solutions in good faith. If the parties cannot reach a resolution within 90 days from the date of PowerPlan's receipt of Client's written objection, Client may discontinue the use of the affected Services by providing written notice to PowerPlan. Such discontinuation will be without prejudice to any fees incurred by Client prior to the discontinuation of the affected Services. If no objection has been raised prior to PowerPlan replacing or appointing a new Subprocessor, PowerPlan will be deemed to have authorized the new Sub-processor.

5. Security Measures and Audits

5.1. *Security Measures.* PowerPlan will implement reasonable physical, organizational, and technical measures to protect against any unauthorized or unlawful access, processing, loss, destruction, theft, damage, use or disclosure of Client Data or systems (collectively, "Appropriate Safeguards"), including, at a minimum, the security measures set forth as Schedule 2. These Appropriate Safeguards will be appropriate to the harm that might result from any risks to Client Data or systems and having regard to the nature of the Client Data or system which is to be protected and will take into consideration the state of the art, the costs of implementation and the nature, scope, context and purpose of the processing and the risks to the rights and freedoms of the Personal Data subjects.

5.2. *Variation of Measures*. The PowerPlan may, by written notice to the Client, vary the security measures set out in Schedule 2, including (where applicable) following review by the PowerPlan of such measures, provided that such variation does not reduce the overall level of protection afforded to the Client Data by the PowerPlan under this DPA.

5.3. *Compliance Review.* PowerPlan will cooperate with reasonable assessments by Client as to its compliance with this DPA and Applicable Data Protection Law but all such assessments must be conducted (i) on reasonable written notice to the PowerPlan; (ii) only during the PowerPlan's normal business hours; (iii) in a manner that does not disrupt the PowerPlan's business; (iv) subject to a confidentially agreement in a form such as PowerPlan may reasonably request; (v) in compliance with relevant policies for individuals visiting PowerPlan's or sub-vendors premises; and (vi) at Client's expense. Notwithstanding anything to the contrary, the assessment right provided in this Section 5.3 may be satisfied by the provision of a successful assessment result performed by an experienced, qualified independent auditor within the last 24 months.

6. Security Breach and Response

6.1. *Breach Notification.* PowerPlan will promptly notify Client without undue delay and no later than 72 hours upon PowerPlan becoming aware of a Security Breach. PowerPlan should notify Client via email to PowerPlan's primary business contact or other email address provided by Client for such notifications if it has knowledge that there is, or reasonably believes that there has been, an actual or potential Security Breach. To the extent known, notice must include the following: (a) the nature of the Security Breach, (b) the categories and numbers of data subjects concerned, and the categories and numbers of records concerned; (c) the name and contact details of PowerPlan's DPO or other relevant contact from whom more information may be obtained; (d) the likely consequences of the Security Breach; and (e) the measures taken or proposed to be taken to address the Security Breach.

6.2. *Cooperation and Remediation.* PowerPlan will (i) cooperate with Client in the manner reasonably requested by Client and in accordance with law to investigate and resolve the Security Breach and to mitigate any harmful effects of the Security Breach; (ii) promptly implement any necessary remedial measures to ensure the protection of Client Data; and (iii) document responsive actions taken related to any Security Breach.

6.3. *Information to Third Parties.* Except as required by applicable law or regulation, PowerPlan will not inform any third party of any Security Breach without first obtaining Client's prior written consent, other than to inform a complainant that Client will be informed of the Security Breach. Client will have the sole right to determine whether notice of the Security Breach is to be provided to any individuals, Supervisory Authorities, regulators, law enforcement agencies, consumer reporting agencies, or others and the contents of any such notice.

7. Duration and Termination

7.1. *Return/Deletion of Client Data.* The PowerPlan will, within 30 days of the date of termination or expiry of the Agreement:

(a) if requested by the Client within that period, return a complete copy of all Client Data by secure file transfer in such a format as reasonably agreed to by the Client to the PowerPlan; and

(b) other than any Client Data retained by the PowerPlan after termination of the Agreement as expressly permitted by this DPA or as required by the Standard Contractual Clauses, delete, and use all reasonable efforts to procure the deletion of all other copies of Client Data processed by the PowerPlan or any sub-processors.

7.2. *Certification.* Upon Client's request, PowerPlan must promptly certify in writing to Client that it has destroyed or returned all Client Data. In the event that PowerPlan is unable to return or destroy all Client Data, PowerPlan will retain Client Data only to the extent and for such period as required by applicable laws, maintain the security and confidentiality of all such retained Client Data in accordance with the protections of this DPA, and ensure that such Client Data is only processed as necessary for the purposes specified in the applicable laws preventing its deletion and for no other purposes.

7.3. *Compliance with this DPA.* If PowerPlan determines that it can no longer meet its obligations under this DPA or Applicable Data Protection Law, PowerPlan will notify Client of that determination within 5 business days and work with Client to take reasonable and appropriate steps to stop and remediate the unauthorized use of Client Data.

8. Law and Jurisdiction

The Parties agree that the laws, jurisdictions, and venues set forth in the Agreement will also govern this DPA.

SCHEDULE 1

Details of processing

1. **Categories of data subjects**

The categories of data subjects whose Personal Data are transferred: Client employees who have access rights to the PowerPlan software and other Data Subjects whose Personal Data is included in the contracts that may be uploaded to the PowerPlan software (e.g., Data Subjects who countersign Client leases).

2. **Categories of Personal Data**

The transferred categories of Personal Data are: Personal Data required to log-in to, or otherwise utilize, the PowerPlan software (e.g., name, company email address, IP address), other business contact information such as title, employer name, phone number, and Personal Data included in the contracts that may be uploaded to the PowerPlan software (e.g., name and title of lease signatories).

3. **Special categories of Personal Data (if applicable)**

The transferred Personal Data includes the following special categories of data: No sensitive or special categories of personal data are transferred save where it is contained within government issued identity documents which are required to be shared for legal and/or regulatory purposes (in which case it shall be protected in line with applicable law and these clauses).

4. **Frequency of the transfer**

The frequency of the transfer is: continuous during the term of the Agreement.

5. **Subject matter / Purpose of the processing**

The subject matter of the processing is: providing of use of cloud-deployed software or SaaS to Client.

6. **Nature of the processing**

The nature of the processing is: collection, organisation, structuring, and storage, use, erasure, and destruction

7. **Purpose(s) of the data transfer and further processing**

The purpose of the data transfer and further processing is: providing cloud-accessible software or SaaS to Client.

8. **Duration**

The period for which the Personal Data will be retained, or, if that is not possible, the criteria used to determine that period: as set out in Section 7 of the DPA.

SCHEDULE 2

Technical and Organisational Measures

Description of the technical and organisational security measures implemented by the data importer / PowerPlan (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, as well as the risks for the rights and freedoms of natural persons.

1. Pseudonymisation and Encryption

Pseudonymisation contains measures that enable one to process Personal Data in such a manner that the Personal Data can no longer be attributed to a specific data subject without the use of additional information, provided that this additional information is stored separately, and is subject to appropriate technical and organisational measures. Encryption contains measures that enable one to convert clearly legible information into an illegible string by means of a cryptographic process.

- Stored data is encrypted where appropriate, including any backup copies of the data.

2. The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services

Confidentiality and integrity are ensured by the secure processing of Personal Data, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage.

a. Confidentiality

(i) Physical access control

Measures that prevent unauthorised persons from gaining access to data processing systems with which Personal Data are processed or used.

- Physical access control systems
- Definition of authorises persons and Management and documentation of individual authorisations
- Regulation of Visitors and external staff
- Use of monitored data centres (monitoring performed by the infrastructure service providers)
- Logging of physical access

(ii) System/Electronic access control

Measures that prevent data processing systems from being used without authorisation.

- User Authentication by simple authentication methods (using username/password)
- Secure transmission of credentials using networks (using TSL and SSL)
- Automatic account locking
- Guidelines for Handling of passwords
- Definition of authorised persons
- Managing means of authentication
- Access control to infrastructure that is hosted by cloud service provider

(iii) Internal Access Control

Measures that ensure that persons entitled to use a data processing system have access only to the data to which they have a right of access, and that Personal Data cannot be read, copied, modified, or removed without authorisation in the course of processing or use and after storage.

- Automatic and manual locking
- Access right management
- Access right management including authorisation concept, implementation of access restrictions, implementation of the "need-to-know" principle, managing of individual access rights.

(iv) Isolation/Separation Control

Measures to ensure that data collected for different purposes can be processed (storage, amendment, deletion, transmission) separately.

- Network separation

- Segregation of responsibilities and duties
- Document procedures and applications for the separation

(v) Job Control

Measures that ensure that, in the case of commissioned processing of Personal Data, the data are processed strictly corresponding the instructions of the principal.

- Training and confidentiality agreements for internal staff and external staff

b. Integrity

(i) Data transmission control

Measures ensure that Personal Data cannot be read, copied, modified, or removed without authorisation during electronic transmission or transport, and that it is possible to check and establish to which bodies the transfer of Personal Data by means of data transmission facilities is envisaged.

- Secure transmission between client and server and to external systems by using industry-standard encryption
- Secure network interconnections ensured by Firewalls etc.
- Logging of transmissions of data from IT system that stores or processes Personal Data

(ii) Data input control

Measures that ensure that it is possible to check and establish whether and by whom have been input into data processing systems, modified, or removed.

- Logging authentication and monitored logical system access
- Logging of data access including, but not limited to access, modification, entry, and deletion of data
- Documentation of data entry rights and partially logging security related entries.

c. Availability and Resilience of Processing Systems and Services

Availability includes measures that ensure that personal data is protected from accidental destruction or loss due to internal or external influences. Resilience of processing systems and services includes measures that ensure the ability to withstand attacks or to quickly restore systems to working order after an attack.

- Implementation of transport policies
- Backup Concept
- Protection of stored backup media

3. The ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident

Organisational measures that ensure the possibility to quickly restore the system or data in the event of a physical or technical incident.

- Continuity planning (Recovery Time Objective & Recovery Point Objective)
- Documented and timed quarterly disaster recovery exercises

4. A process for regularly testing, assessing, and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing

Organisational measures that ensure the regular review and assessment of technical and organisational measures.

- Documentation of interfaces and Personal Data fields
- Internal assessments

5. Additional technical and organisational measures

The following additional technical and organisational measures will be implemented:

- Measures for certification/assurance of processes and products
- Measures for ensuring data minimisation
- Measures for ensuring data quality
- Measures for ensuring limited data retention
- Measures for ensuring accountability
- Measures for allowing data portability and ensuring erasure

6. For transfers to (sub-) processors, technical and organisational measures to be taken by the (sub-) processor to assist to the data exporter

For transfers to (sub-) processors, the technical and organisational measures to be taken by the (sub-) processor to be able to provide assistance to the data importer / Client are as summarised in clause 2 above.