DATA PROCESSING ADDENDUM

This Data Processing Addendum (the **"Addendum"**) forms part of the Terms of Service entered into by and between ProjectToolBelt, LLC. having its place of business at 412 N Main St Suite 100 (**"Provider"**) and EasyGanttCharts_Customer (**"Client"**) dated **25 May, 2018** pursuant to which Provider provides services, including the use of the Provider's EasyGanttCharts Application and any other services purchased by Client from Provider (**"Services"**) to Client (the **"Agreement"**).

The terms used in this Addendum shall have the meanings set forth in this Addendum. Capitalized terms not defined herein shall have the meaning set forth in the Agreement. Except as modified below, the terms of the Agreement shall remain in full force and effect.

In consideration of the mutual obligations set out herein, the parties hereby agree that the terms and conditions set out below shall be added as an Addendum to the Agreement. Except where the context requires otherwise, references in this Addendum to the Agreement are to the Agreement as amended by, and including, this Addendum. Each reference to the Addendum in this Addendum means this Addendum including its Schedules and Appendices.

In the course of providing the Services to Client pursuant to the Agreement, Provider may Process Personal Data on behalf of Client and the parties agree to comply with the following provisions with respect to any Personal Data.

1. Effectiveness

1.1 **Legal Authority.** Client signatory represents to Provider that he or she has the legal authority to bind Client and is lawfully able to enter into contracts (e.g., is not a minor).

1.2 **Termination.** This Addendum will terminate upon the earliest of: (i) termination of the Agreement as permitted hereunder or by the Provider's Terms and Conditions (and without prejudice to the survival of accrued rights and liabilities of the parties and any obligations of the parties which either expressly or by implication survive termination); (ii) as earlier terminated pursuant to the terms of this Addendum or (iii) as agreed by the parties in writing.

2. Definitions

"Client Personal Data" means any Personal Data Processed by ProjectToolBelt, LLC (or a Sub-processor) on behalf of Client pursuant to or in connection with the Agreement;

"Data Protection Laws" means all laws and regulations, including laws and regulations of the European Union, the European Economic Area and their member states, and the GDPR, applicable to the Processing of Client Personal Data under the Agreement which are applicable to Client.

"GDPR" means the 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 (General Data Protection Regulation)

"Sub-processor" means any person (including any third party, but excluding an employee of Provider or any of its sub-contractors) appointed by or on behalf of Processor to Process Personal Data on behalf of Client under the Agreement

The terms, **"Commission"**, **"Controller"**, **"Data Subject"**, **"Member State"**, **"Personal Data"**, **"Personal Data Breach"**, **"Processing"**, **"Processor"**, and **"Supervisory Authority"** shall have the same meaning as in the GDPR, and shall be construed accordingly.

3. Processing of Personal Data

3.1 **Roles of the Parties.** The parties acknowledge and agree that with regard to the Processing of Personal Data, Client is the Data Controller, Provider is a Data Processor and that Provider will engage Sub-processors pursuant to the requirements set forth in Section 5 **"Sub-processors"** below.

3.2 **Client Authority.** Client represents and warrants that it is and will at all relevant times remain duly and effectively authorized to give the instruction set forth in Section 3.4 below on behalf of itself.

3.3 **Client's Processing of Personal Data.** Client shall, in its use of the Services, Process Personal Data in accordance with the requirements of Data Protection Laws. Client's instructions for the Processing of Personal Data shall comply with Data Protection Laws. In addition, Client shall have sole responsibility for the accuracy, quality, and legality of Personal Data and the means by which Client acquired Personal Data. Personal Data provided by the Client shall not contain information that reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric, data concerning health or data concerning an individual's sex life or sexual orientation ("Special Categories of Data").

3.4 **Provider's Processing of Personal Data.**

a. Provider shall only Process Client Personal Data for the purpose of the provision of the Services under the Agreement and in accordance with Client's documented instructions which are consistent with the terms of the Agreement, unless Processing is required by Data Protection Laws to which Provider (or the applicable sub-processor) is subject, in which case Provider shall to the extent permitted by the Data Protection Laws inform Client of that legal requirement before the relevant Processing of that Client Personal Data.

b. This Addendum, the Agreement and any Order Forms thereunder, are Client's complete and final instructions to Provider for the Processing of Client Personal Data. Any additional or alternate instructions must be agreed upon separately.

c. The following are deemed instructions of the Client to Provider: The processing of Client Personal Data (i) in accordance with the Agreement, this Addendum and any Order Forms under the Agreement, including without limitation with the transfer of Client Personal Data to any country or territory; and (ii) to comply with other documented instructions provided by Client where such instructions are consistent with the terms of the Agreement.

3.5 **Details of the Processing.** The subject-matter of Processing of Client Personal Data by Provider is the performance of the Services pursuant to the Agreement. The duration of the Processing, the nature and purpose of the Processing, the types of Client Personal Data and categories of Data Subjects Processed under this Addendum, as required by article 28(3) of the GDPR (and, possibly, equivalent requirements of other Data Protection Laws), are further specified in Exhibit A to this Addendum, as may be amended by the parties from time to time.

4. Provider Personnel

Throughout the term of this Addendum, Provider shall restrict its personnel from Processing Client Personal Data without authorization by Provider and shall limit the Processing to that which is needed for the specific individual's job duties in connection with Provider's provision of the Services under the Agreement. Provider will impose appropriate contractual obligations on its personnel, including relevant obligations regarding confidentiality, data protection and data security.

5. Sub-processors

5.1 **Appointment of Sub-processors.** For the purpose of the appointment of Sub-processors, Client acknowledges and agrees that Provider may engage third-party Sub-processors in connection with the provision of the Services, including without limitation the Processing of Client Personal Data.

5.2 **List of Current Sub-processors and Notification of New Sub- processors.** When requested by the Client, the Provider shall make available to Client an up-to-date list of all Sub-processors used for the processing of Client Personal Data.

5.3 **Objection Right for New Sub-processors.** Provider shall give Client prior written notice of the appointment of any new Sub-processor, including full details of the Processing to be undertaken by the Sub-processor. If, within 14 days of receipt of that notice, Client notifies Provider in writing of any objections (on reasonable grounds) to the proposed appointment, then (i) Provider shall work with Client in good faith to make available a commercially reasonable change in the provision of the Services which avoids the use of that proposed Sub-processor; and (ii) where such a change cannot be made within 14 days from Provider's receipt of Client's notice, notwithstanding anything in the Agreement, Client may by written notice to Provider with immediate effect terminate the Agreement to the extent that it relates to the Services which require the use of the proposed Sub-processor.

5.4 **Sub-processing Agreement; Liability.** Provider has or shall enter into a written agreement with each Sub-processor (the **"Sub-processing Agreement"**) containing data protection obligations not less protective than those in the Agreement and/or this Addendum with respect to the protection of Client Personal Data to the extent applicable to the nature of the Services provided by such Sub-processor. Provider shall be liable for the acts and omissions of its Sub-processors to the same extent Provider would be liable if performing the services of each Sub-processor directly under the terms of this Addendum.

5.5 **Copies of Sub-Processor Agreements.** Provider shall provide to Client for review copies of the Sub-processor agreements as Client may reasonably request from time to time. The parties agree that all commercial information may be removed by the Provider beforehand.

6. Security

6.1 **Adequate Measures.** Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Provider shall in relation to the Client Personal Data implement and maintain throughout the term of this Addendum, the technical and organizational measures set forth in Exhibit B (the **"Security Measures"**). Client acknowledges and agrees that it has reviewed and assessed the Security Measures and deems the appropriate for the protection of Client Personal Data.

6.2 **Personal Data Breach Risk.** In assessing the appropriate level of security, Provider shall take account of the risks that are presented by Processing, in particular from a Client Personal Data Breach

7. Data Subject Rights

7.1 **Correction, Blocking and Deletion.** Provider shall comply with any commercially reasonable request by Client to correct, amend, block or delete Client Personal Data, as required by Data Protection Laws, to the extent Provider is legally permitted to do so.

7.2 **Measures to assist with Data Subject Rights.** Taking into account the nature of the Processing, Provider shall assist Client by implementing appropriate technical and organizational measures, insofar as this is possible, for the fulfillment of the Client's obligations, as reasonably understood by Client, to respond to requests to exercise Data Subject rights under the Data Protection Laws. To the extent legally permitted, Client shall be responsible for any costs arising from Provider's provision of such assistance.

7.3 **Response to Requests:** Provider:

a. shall promptly notify Client if it or any Sub-processor receives a request from a Data Subject under any Data Protection Laws & Regulation in respect of Client Personal Data; and

b. shall not and shall ensure that no Sub-processor responds to that request except on the documented instructions of Client or as required by Data Protections Laws to which Provider or Sub- processor is subject, in which case Provider shall, to the extent permitted by such Data Protections Laws inform Client of that legal requirement before it or the applicable

Sub-processor responds to the request.

8. Personal Data Breach

8.1 **Notification of Data Breach.** Provider shall, to the extent permitted by law, notify Client without undue delay upon Provider or any Sub-processor becoming aware of a Personal Data Breach affecting Client Personal Data, providing Client with sufficient information to allow Client to meet any obligations to report or inform Data Subjects of the Personal Data Breach under the Data Protection Laws.

8.2 **Assistance to Client** Provider shall co-operate with Client and take such reasonable commercial steps as are directed by Client to assist in the investigation, mitigation and remediation of each such Personal Data Breach.

9. Data Protection Impact Assessment and Prior Consultation

Provider shall provide reasonable assistance to Client with any data protection impact assessments, and prior consultations with Supervising Authorities or other competent data privacy authorities, which Client reasonably considers to be required of it by Article 35 or 36 of the GDPR or equivalent provisions of any other Data Protection Law & Regulation, in each case solely in relation to Processing of Client Personal Data by, and taking into account the nature of the Processing and information available to, Provider or the Sub-processors

10. Return or Destruction of Personal Data.

10.1 **Return or Deletion.** Subject to the provisions of Section 10.2 below, at Client's election, made by written notice to Provider following 30 days of the date of cessation of any Services involving the Processing of Client Personal Data (the **"Cessation Date"**), Provider shall, and shall procure that all Sub-processors: (a) return a complete copy of all Client Personal Data to Client in such format and manner requested by Client and reasonably acceptable to Provider; and (b) delete and procure the deletion of all other copies of Client Personal Data Processed by Provider or any Sub-processor. Provider shall comply with any such written request within 30 days of the Cessation Date.

10.2 **Retention of Copies.** Provider and each Sub-processor may retain Client Personal Data to the extent required by applicable European Union law or the law of an EU Member State and only to the extent and for such period as required by such laws and always provided that Provider shall ensure the confidentiality of all such Client Personal Data and shall ensure that such Client Personal Data is only Processed as necessary for the purpose(s) specified in such law requiring its storage and for no other purpose.

11. Audit.

11.1 **Report on Compliance.** Subject to the provisions of Section 11.3 below, at Client's written request, Provider will provide Client all information necessary to demonstrate compliance with this Addendum. The information provided will constitute Provider Confidential Information under the confidentiality provisions of the Agreement or a non-disclosure agreement, as applicable.

11.2 **Audit.** Provider audits its compliance against data protection and information security standards on a regular basis. Such audits are conducted by Provider's internal audit team. The specific audits will necessarily vary depending upon the nature of the Services in question. Upon Client's written request, and subject to obligations of confidentiality, Provider will make available to Client a summary of its most recent relevant internal audit report and/or other documentation reasonably required by Customer which Provider makes generally available to its customers, so that Customer can verify Providers compliance with this DPA.

12. Transfer of Data.

12.1 **Standard Contractual Clauses.** Subject to the provisions of Section 12.2 below, to the extent Client Personal Data is transferred under this Addendum from the European Economic Area and/or its

Member States to countries which do not ensure an adequate level of data protection within the meaning of Data Protection Laws and Regulations, to the extent such transfers are subject to such Data Protection Laws and Regulations, the Client (as "data exporter") and ProjectToolBelt, LLC. (as "data importer") hereby enter into the contractual clauses set out in [Exhibit C] (the "Standard Contractual Clauses"), amended as indicated (in square brackets and italics) in such Exhibit and under Section 12.5 below in respect of the transfers.

12.2 **Applicability.** Section 12.1 shall not apply to a cross border transfer unless its effect, together with other reasonably practicable compliance steps (which, for the avoidance of doubt, do not include obtaining consents from Data Subjects), is to allow the relevant cross border to take place without breach of applicable Data Protection Law and Regulation (a "Restricted Transfer"). The Standard Contractual Clauses apply to (i) the legal entity that has executed the Standard Contractual Clauses as a Data Exporter and, (ii) all affiliates of Client, if any, established within the European Economic Area (EEA) and Switzerland that have purchased Services on the basis of an Order Form. For the purpose of the Standard Contractual Clauses and this Section 12, the Client and its affiliates shall be deemed to be "Data Exporters".

12.3 **Sub-processors.** Provider warrants and represents that, before the commencement of any Restricted Transfer to a Sub-processor, it shall ensure that one of the following is in place: (i) the Standard Contractual Clauses are at all relevant times incorporated into the agreement between Provider, or a relevant intermediate Sub-processor, on the one hand and Sub-processor on the other hand; (ii) that Sub-processor enters into an agreement incorporating the Standard Contractual Clauses with Client or that (iii) Provider's entry into the Standard Contractual Clauses under Section 12.1 above, or agreement to variations to those Standard Contractual Clauses made under Section 12.6 below, as agent for and on behalf of that Sub-processor, will have been duly and effectively authorized (or subsequently ratified) by that Sub-processor.

12.4 **Conflict.** In the event of any conflict or inconsistency between the body of this Addendum and the Standard Contractual Clauses, the Standard Contractual Clauses shall prevail.

12.5 **Changes to the Standard Contractual Clauses:** The parties agree that:

a. This Addendum, the Agreement and any Order Forms thereunder, are Client's complete and final instructions to Provider for the Processing of Client Personal Data. Any additional or alternate instructions must be agreed upon separately. For the purposes of Clause 5(a) of the Standard Contractual Clauses, the following is deemed an instruction by the Client to Provider to Process Client Personal Data:

   The processing of Client Personal Data (i) in accordance with the Agreement, this Addendum and any Order Forms under the Agreement, including without limitation the transfer of Client Personal Data to any country or territory; and (ii) to comply with other documented instructions provided by Client where such instructions are consistent with the terms of the Agreement.

b. Pursuant to the provisions of Clause 5(h) of the Standard Contractual Clauses, Client acknowledges and agrees that Provider may engage third- party Sub-processors in connection with the provision of the Services, including without limitation the Processing of Client Personal Data. Provider shall make available to Client an up-to-date list of all Sub-processors used for the processing of Client Personal Data in accordance with the provisions of Section 5.2 above.

c. Pursuant to Clause 5(h) of the Standard Contractual Clauses, Client acknowledges and expressly agrees that Provider may engage new Sub- processors in accordance with the provisions of Sections 5.2 and 5.3 above.

d. The copies of the Sub-processor agreements that must be sent by the Supplier to the Client pursuant to Clause 5(j) of the Standard Contractual Clauses may have all commercial information, or provisions unrelated to the Standard Contractual Clauses or their equivalent, removed by the Supplier beforehand; and, that such copies will be provided by Provider only

upon reasonable request by Client.

e. That Section 13 below shall apply without prejudice to clauses 7 (Mediation and Jurisdiction) and 9 (Governing Law) of the Standard Contractual Clauses.

f. The certification of deletion of Personal Data that is described in Clause 12(1) of the Standard Contractual Clauses shall be provided by Provider to the Client only upon Client's request.

g. Section 14 below shall be deemed to apply to any violation of the Standard Contractual Clauses.

13. Jurisdiction and Governing Law.

13.1 **Law.** This Addendum and all non-contractual or other obligations arising out of or in connection with it are governed by the laws of the United Kingdom.

13.2 **Jurisdiction.** With respect to any disputes or claims howsoever arising under this Addendum, including disputes regarding its existence, validity or termination or the consequences of its nullity the parties submit to the jurisdiction of the competent courts of London, United Kingdom.

14. Indemnification; Limitation of Liability

If one party is held liable for a violation of this Addendum or, if applicable, any provision of the Standard Contractual Clauses, committed by the other party, the latter will, to the extent to which it is liable, indemnify the first party for any cost, charge, damages, expenses or loss it has incurred in accordance with the provisions of the "Indemnification" Section of the Agreement. Each party's liability, taken together in the aggregate, arising out of or related to this Addendum and/or the Standard Contractual Clauses, whether in contract, tort or under any other theory of liability, is subject to the 'Limitation of Liability' section of the Agreement. For the avoidance of doubt, Provider's total liability for all claims from the Client or any third party arising out of or related to the Agreement and this Addendum shall apply in the aggregate for all claims under both the Agreement and this Addendum.

[Remainder of Page Intentionally Left Blank; Signature Pages to Follow]

EXECUTED by and on behalf of:
Provider

Name: Sathish Kumar Srinivasan
Role: Co-Founder
Date: 22 Jun, 2018

EXECUTED by and on behalf of:

EasyGanttCharts_Customer

Name:
Role:
Date:

EXHIBIT A TO DATA PROCESSING ADDENDUM: DETAILS OF PROCESSING

- **Duration of the Processing:** The duration of data processing shall be for the term agreed between data exporter and Provider in the Agreement or an applicable Order Form.

- **Nature and purpose of the Processing: The scope** and purpose of processing of the data subjects' personal data is to facilitate the provision of Provider's Services.

- **Types of Client Personal Data:** The personal data transferred includes e-mail, documents and other data in an electronic form provided in the context of Provider's Services, which shall not include any Special Categories of Data.

- **Categories of Data Subjects:** Data subjects include the Client's representatives and end-users including employees, contractors, collaborators, and Client's customers. Data subjects may also include individuals attempting to communicate or transfer personal information to users of Provider's Services. The data subjects exclusively determine the content of data submitted to Provider.

EXHIBIT B TO DATA PROCESSING ADDENDUM: SECURITY MEASURES

1. Personnel. Data Importer's personnel will not process customer data without authorization. Personnel are obligated to maintain the confidentiality of any customer data and this obligation continues even after their engagement ends.

2. Data Privacy Contact

ProjectToolBelt, LLC
4212 N Main St Suite 100
Buffalo, Wyoming 82834

3. Technical and Organization Measures. The Data Importer has implemented and will maintain appropriate technical and organizational measures, internal controls, and information security routines intended to protect customer data against accidental loss, destruction, or alteration; unauthorized disclosure or access; or unlawful destruction as follows:

3.1 Organization of Information Security.

a. *Security Roles and Responsibilities.* The Data Importer has appointed Sathish Kumar Srinivasan as the security officer responsible for coordinating and monitoring the security rules and procedures.

b. *Duty of Confidentiality.* The Data Importer's personnel with access to customer data are subject to confidentiality obligations.

3.2 Risk Management.

The Data Importer conducts regular testing and monitoring of the effectiveness of its safeguards, controls, systems, including conducting penetration testing. The Data Importer implements measures, as needed, to address vulnerabilities discovered in a timely manner.

3.3 Storage.

The Data Importer's database servers are hosted in a data center operated by a third party vendor, that has been qualified per the Data Importer's vendor management procedure. The Data Importer maintains complete administrative control over the virtual servers, and no third-party vendors have logical access to customer data.

3.4 Asset Management.

a. *Asset Inventory.* The Data Importer maintains an inventory of all media on which customer data is stored. Access to the inventories of such media is restricted to authorized personnel.

b. *Asset Handling.*

i. The Data Importer imposes restrictions on printing customer data and has procedures for disposing of printed materials that contain customer data.

ii. The Data Importer's personnel must obtain authorization prior to storing customer data on portable devices, remotely accessing customer data, or processing customer data outside the Data Importer's facilities.

3.5 Software Development and Acquisition: For the software developed by Data Importer, Data Importer follows secure coding standards and procedures set out in its standard operating procedures.

3.6 Change Management: Data Importer implements documented change management procedures that provide a consistent approach for controlling, implementing, and documenting changes (including emergency changes) for the Data Importer's software, information systems or network architecture. These change management procedures include appropriate segregation of duties.

3.7 Third Party Provider Management: In selecting third party providers who may gain access to, store, transmit or use customer data, Data Importer conducts a quality and security assessment pursuant to the provisions of its standard operating procedures.

3.8 Human Resources Security. The Data Importer informs its personnel about relevant security procedures and their respective roles, as well as of possible consequences of breaching the security rules and procedures. Such consequences include disciplinary and/or legal action.

3.9 Physical and Environmental Security.

a. *Physical Access to Facilities.* The Data Importer limits access to facilities where information systems that process customer data are located to identified authorized individuals who require such access for the performance of their job function. Data Importer terminates the physical access of individuals promptly following the date of the termination of their employment or services or their transfer to a role no longer requiring access to customer data.

b. *Protection from Disruptions.* The Data Importer uses commercially reasonable systems and measures to protect against loss of data due to power supply failure or line interference.

c. *Component Disposal.* The Data Importer uses commercially reasonable processes to delete customer data when it is no longer needed.

3.10 Communications and Operations Management.

a. *Security Documents.* The Data Importer maintains security documents describing its security measures and the relevant procedures and responsibilities of its personnel.

b. *Data Recovery Procedures.*

i. On an ongoing basis, the Data Importer maintains multiple copies of customer data from which it can be recovered.

ii. The Data Importer stores copies of customer data and a data recovery procedures in a different place from where the primary computer equipment processing the customer data is located.

iii. The Data Importer has procedures in place governing access to copies of customer data.

iv. The Data Importer has anti-malware controls to help avoid malicious software gaining unauthorized access to customer data.

c. *Encryption; Mobile Media.* The Data Importer uses HTTPS encryption on all data connections. The Data Importer restricts access to customer data in media leaving its facilities. The Data Importer further has a destruction policy for hardware in the data center that stores customer data.

d. *Event Logging.* The Data Importer logs the use of our data-processing systems. We maintain logs for at least 20 days.

3.11 Access Control.

a. *Records of Access Rights.* The Data Importer maintains a record of security privileges of individuals having access to customer data.

b. *Access Authorization.*

i. The Data Importer maintains and updates a record of personnel authorized to access systems that contain customer data.

ii. The Data Importer deactivates authentication credentials of employees or contract workers immediately upon the termination of their employment or services as well as such authentication credentials that have not been used for a period of time not to exceed six months.

iii. The Data Importer identifies those personnel who may grant, alter or cancel authorized access to data and resources.

c. *Least Privilege.*

i. Technical support personnel are only permitted to have access to customer data when needed for the performance of their job function.

ii. The Data Importer restricts access to customer data to only those individuals who require such access to perform their job function.

d. *Integrity and Confidentiality.*

i. The Data Importer instructs its personnel to disable administrative sessions when leaving the Data Importer's premises or when computers are unattended.

ii. The Data Importer stores passwords in a way that makes them unintelligible while they are in force.

e. *Authentication.*

i. The Data Importer uses commercially reasonable practices to identify and authenticate users who attempt to access information systems.

ii. Where authentication mechanisms are based on passwords, the Data Importer requires that the passwords are renewed regularly.
iii. Where authentication mechanisms are based on passwords, the Data Importer requires the password to be at least eight characters long.

iv. The Data Importer ensures that de-activated or expired identifiers are not granted to other individuals.

v. The Data Importer maintains commercially reasonable procedures to deactivate passwords that have been corrupted or inadvertently disclosed or pursuant to a number of failed login attempts.

vi. The Data Importer uses commercially reasonable password protection practices, including practices designed to maintain the confidentiality and integrity of passwords when they are assigned and distributed, and during storage.

f. *Network Design.* The Data Importer has controls to avoid individuals assuming access rights they have not been assigned to gain access to customer data they are not authorized to access.

3.12 Network Security.

a. *Network Security Controls.* Data Importer's information systems have security controls designed to detect and mitigate attacks by using logs and alerting.

b. *Antivirus.* Data Importer implements endpoint protection on its hosting environments, including antivirus; which are continuously updated with critical patches or security releases in accordance with Data Importer's server change control procedures.

3.13 Information Security Incident Management.

a. *Record of Breaches.* The Data Importer maintains a record of security breaches with a description of the breach, the time period, the consequences of the breach, the name of the reporter, and to whom the breach was reported, and the procedure for recovering data.

b. *Record of Disclosure.* The Data Importer tracks disclosures of customer data, including what data has been disclosed, to whom, and at what time.

3.14 Business Continuity Management. The Data Importer employs redundant storage and its procedures for recovering data are designed to attempt to reconstruct customer data in its original state from before the time it was lost or destroyed.

Exhibit C – Model Contractual Clauses

Commission Decision C(2010)593 Standard Contractual Clauses (processors)

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection

Name of the data exporting organisation: EasyGanttCharts_Customer		
Address:		
Tel:	Fax:	E-mail:
Other information needed to identify the organisation:		

(the data **exporter**)

And

Name of the data importing organisation: ProjectToolBelt, LLC		
Address: 412 N Main St Suite 100, Buffalo, Wyoming 82834		
Tel: 13106224434	Fax:	E-mail: privacy@ProjectToolBelt.com
Other information needed to identify the organisation: Not Applicable		

(the data **importer**)
each a "party"; together "the parties",

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

Clause 1
Definitions

For the purposes of the Clauses:

a. *'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject'* and *'supervisory authority'* shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [Parties may reproduce definitions and meanings contained in Directive 95/46/EC within this Clause if they considered it better for the contract to stand alone.];

b. *'the data exporter'* means the controller who transfers the personal data;

c. *'the data importer'* means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

d. *'the subprocessor'* means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

e. *'the applicable data protection law'* means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

f. *'technical and organisational security measures'* means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2

Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

Clause 3

Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

3. The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

a. that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

b. that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

c. that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;

d. that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

e. that it will ensure compliance with the security measures;

f. that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

g. to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

h. to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

i. that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and j. that it will ensure compliance with Clause 4(a) to (i).

Clause 5

Obligations of the data importer [Mandatory requirements of the national legislation applicable to the data importer which do not go beyond what is necessary in a democratic society on the basis of one of the interests listed in Article 13(1) of Directive 95/46/EC, that is, if they constitute a necessary measure to safeguard national security, defence, public security, the prevention, investigation, detection and prosecution of criminal offences or of breaches of ethics for the regulated professions, an important economic or financial interest of the State or the protection of the data subject or the rights and freedoms of others, are not in contradiction with the standard contractual clauses. Some examples of such mandatory requirements which do not go beyond what is necessary in a democratic society are, inter alia, internationally recognised sanctions, tax-reporting requirements or anti-money- laundering reporting requirements.]

The data importer agrees and warrants:

a. to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

b. that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

c. that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;

d. that it will promptly notify the data exporter about:

i. any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,

ii. any accidental or unauthorised access, and

iii. any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

e. to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

f. at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

g. to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to

obtain a copy from the data exporter;

h. that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;

i. that the processing services by the subprocessor will be carried out in accordance with Clause 11;

j. to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter.

Clause 6

Liability

1. The parties agree that a ny data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or subprocessor is entitled to receive compensation from the data exporter for the damage suffered.

2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity. The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the subprocessor agrees that the data subject may issue a claim against the data subprocessor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the subprocessor shall be limited to its own processing operations under the Clauses.

Clause 7

Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

   a. to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

   b. to refer the dispute to the courts in the Member State in which the data exporter is established.

2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8

Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

Clause 9

Governing Law

The Clauses shall be governed by the law of the Member State in which the data exporter is established, namely **United States**

Clause 10

Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11

Subprocessing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses [This requirement may be satisfied by the subprocessor co-signing the contract entered into between the data exporter and the data importer under this Decision.]. Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.

2. The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

3. The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established, namely **United States**

4. The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12

Obligation after the termination of personal data processing services

1. The parties agree that on the termination of the provision of data processing services, the data importer and the subprocessor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

2. The data importer and the subprocessor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

On behalf of the data exporter:

Name (written out in full):	Position
Address	
Other information necessary in order for the contract to be binding (if any):	
Signature	

(stamp of organisation)

On behalf of the data importer:

Name (written out in full): Sathish Kumar Srinivasan	Position Co-founder
Address 412 N Main St, Suite 100, Buffalo, Wyoming 82834.	
Other information necessary in order for the contract to be binding (if any):	
Signature 	

(stamp of organisation)

APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed by the parties. The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix.

Data exporter

The data exporter is **EasyGanttCharts_Customer**

Data importer

The data importer is ProjectToolBelt, LLC. ProjectToolBelt, LLC offers services that allow organizations to manage Employee leave records, TimeSheet records and other HR processes.

Data subjects

Data subjects include the data exporter's customer's representatives and end-users including employees, contractors, collaborators, and customers of the data exporter. Data subjects may also include individuals attempting to communicate or transfer personal information to users of the services provided by data importer. The data subjects exclusively determine the content of data submitted to the Company.

Categories of data

The personal data transferred includes e-mail, documents and other data in an electronic form in the context of the services being provided by ProjectToolBelt, LLC (the "Services").

Processing operations

The personal data transferred will be subject to the following basic processing activities:

A. **Duration and Object of Data Processing.** The duration of data processing shall be for the term agreed between data exporter and ProjectToolBelt, LLC. The objective of the data processing is the performance of the Services.

B. **Scope and Purpose of Data Processing.** The scope and purpose of processing personal data is to facilitate provision of the Services.

C. **Customer Data Access.** For the agreed term ProjectToolBelt, LLC will at its election and as necessary under applicable law implementing Article 12(b) of the EU Data Protection Directive, either: (1) provide data exporter with the ability to correct, delete, or block customer data, or (2) make such corrections, deletions, or blockages on its behalf.

D. **Data Exporter's Instructions.** For the Services, ProjectToolBelt, LLC will only act upon data exporter's instructions.

E. **Customer Data Deletion or Return.** Upon expiration or termination of data exporter's use of the Services, ProjectToolBelt LLC will delete data exporter's customer data within 30 days of the account termination.

APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES

See Exhibit B to Addendum above.