**PlanGrid Data Processing Addendum**

This Data Processing Addendum ("**DPA**") forms part of the Master Subscription Agreement or other written or electronic agreement between the Service Provider ("**Supplier**") and PlanGrid, Inc. (collectively with its affiliates and subsidiaries worldwide, "**PlanGrid**"). This DPA applies to and takes precedence over any conflicting provisions contained in the Underlying Agreement or in any related contractual document between the parties, such as an order form, statement of work, data security agreement, or data processing addendum thereunder (the Underlying Agreement and any such related documentation, collectively, the "**Main Agreement**")

For good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged, Supplier and PlanGrid agree as follows:

1. For purposes of this DPA:

    a. "**PlanGrid Data**" means Personal Data or Confidential Information that Supplier receives from PlanGrid, or otherwise Processes for or on behalf of PlanGrid, in connection with the Main Agreement.

    b. "**PlanGrid Systems**" means any hardware, software, networks or other information technology resources owned or operated by PlanGrid, other than any that are owned by Supplier or its Sub processors.

    c. "**Confidential Information**" means any information that (i) is marked "Confidential," "Privileged," "Proprietary" or "Trade Secret" or (ii) a reasonable business person would understand to be confidential, privileged, proprietary or a trade secret, such as pricing data, financial data, sales data, business techniques, know-how, concepts, development tools and processes, computer programs, design drawings and manuals, patents, copyrights or other intellectual property of any kind or nature, business plans and strategies.

    d. "**Data Protection Laws**" means all laws, regulations and other legal requirements of any jurisdiction relating to privacy, data security, communications secrecy, Personal Data Breach notification, or the Processing of Personal Data, such as, to the extent applicable, the General Data Protection Regulation (Regulation (EU) 2016/679) ("**GDPR**").

    e. "**Personal Data**" means any information of PlanGrid or its customers relating to an identified or identifiable individual, within the meaning of the GDPR (regardless of whether the GDPR applies).

    f. "**Security Breach**" means the accidental, unauthorized or unlawful destruction, loss, alteration or disclosure of, or access to, PlanGrid Data.

    g. "**Process**" and "**Processing**" mean any operation or set of operations performed on PlanGrid Data or on sets of PlanGrid Data, whether or not by automated means, such as collection, recording, organization, creating, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

h. "**Sub processor**" means any Supplier affiliate or subcontractor Processing PlanGrid Data or accessing PlanGrid Systems for Supplier.

2. This DPA applies to all PlanGrid Data and all Supplier access to PlanGrid Systems in connection with the Main Agreement. Appendix 1 of Annex A of this DPA provides background on the subject matter, nature and purpose of the Processing, and additional detail.

3. Supplier will Process PlanGrid Data only to lawfully provide services to PlanGrid under the Main Agreement unless a legal requirement obligates Supplier to engage in different Processing of the data. In such case, Supplier shall inform PlanGrid of that legal requirement before commencing the different Processing, unless that legal requirement prohibits providing such information on important grounds of public interest, and, in the case of a legal obligation to provide the Personal Data to a third party, Supplier will provide PlanGrid a reasonable opportunity to contest the legal obligation or to seek protection for the disclosure.

4. Supplier will access PlanGrid Systems only with PlanGrid's written authorization and only to lawfully provide services to PlanGrid under the Main Agreement. PlanGrid may deny or revoke access to PlanGrid Systems for security concerns in its sole discretion.

5. Supplier shall promptly inform PlanGrid if, in Supplier's opinion, an instruction from PlanGrid regarding Personal Data infringes applicable Data Protection Law.

6. Supplier will ensure that the persons Supplier authorizes to Process PlanGrid Data are subject to a written confidentiality agreement covering such data or are under an applicable statutory obligation of confidentiality.

7. Taking into account the nature of the Processing, Supplier will provide reasonable assistance to PlanGrid for the fulfilment of PlanGrid's obligation to honor requests by individuals (or their representatives) to exercise their rights under the GDPR and other applicable Data Protection Law (such as rights to access their Personal Data).

8. Supplier shall implement appropriate technical and organizational measures to ensure a level of security for the PlanGrid Data appropriate to the risk. Such security measures must comply with Annex B and applicable Data Protection Laws. This is without prejudice to Supplier's right to make future updates to the security measures that do not lower the level of protection required by this DPA.

9. Supplier will provide reasonable assistance to PlanGrid in ensuring PlanGrid's compliance with the security obligations of the GDPR and other applicable Data Protection Law, as relevant to Supplier's role in Processing the Personal Data, taking into account the nature of Processing and the information available to Supplier.

10. Security Breach: Supplier will comply with the Security Breach-related obligations directly applicable to it under the GDPR and other Data Protection Law. Taking into account the nature of Processing and the information available to Supplier, Supplier will provide reasonable assistance to PlanGrid in complying with those applicable to PlanGrid. Without limiting the foregoing, Supplier will:

    a. Within 48 hours of determining that a Security Breach likely occurred, inform

PlanGrid of the Security Breach by sending an email to security@plangrid.com the "**Breach Notification Contact Point**"); and

b. Within such time period, and without undue delay as the information becomes available after that (and in any event at least once each day that there is new material information), inform PlanGrid (via the Breach Notification Contact Point) of:

- The nature of the Security Breach, including, where possible, the categories and approximate number of data subjects concerned, and the categories and approximate number of Personal Data records concerned;
- The likely consequences of the Security Breach; and
- Measures taken or proposed to be taken by Supplier to address the Security Breach, including, where appropriate, measures to mitigate its possible adverse effects;

c. Promptly provide PlanGrid with other information and records sufficient to document PlanGrid's and Supplier's compliance with the Personal Data Breach-related requirements of applicable Data Protection Law;

d. Provide reasonable assistance to, and cooperation with, PlanGrid to take measures that in PlanGrid's reasonable determination (a) reduce the risk to individuals whose Personal Data was involved, or (b) otherwise help PlanGrid qualify for an exemption from a legal requirement to notify an individual or a supervisory authority of the Security Breach; and

e. Assume responsibility for all reasonable costs associated with investigating, mitigating, and remediating any Security Breach, including by reimbursing PlanGrid for costs in connection with providing legally required notifications of such Security Breach and remediation services PlanGrid reasonably deems necessary, such as credit monitoring or identity theft protection services.

11. Supplier will, at the choice of PlanGrid, return to PlanGrid and/or securely destroy all PlanGrid Data upon the end of the services relating to the Processing or at PlanGrid's earlier request, except to the extent that applicable legal requirements require storage of the PlanGrid Data, in which case Supplier will (a) to the extent legally permitted, inform PlanGrid of the legal requirement and of the particular PlanGrid Data records that Supplier intends to retain and (b) at the choice of PlanGrid, return to PlanGrid and/or securely destroy such PlanGrid Data as soon as practicable.

12. Taking into account the nature of the Processing and the information available to Supplier, Supplier will provide reasonable assistance to and cooperation with PlanGrid for PlanGrid's performance of any legally required (a) data protection impact assessment of the Processing or proposed Processing of the Personal Data involving Supplier and (b) related consultation with supervisory authorities.

13. Supplier may subcontract the Processing of PlanGrid Data or access to PlanGrid Systems only in compliance with applicable Data Protection Laws, any conditions for

subcontracting set forth in the Agreement, and the following:

a. Prior to the Sub processor's Processing of PlanGrid Data or receipt of access (or access credentials) to PlanGrid Systems, Supplier will impose contractual obligations on the Sub processor that are at least as protective as those imposed on Supplier under this DPA.

b. 30 days prior to the Sub processor's Processing of PlanGrid Data or receipt of access (or access credentials) to PlanGrid Systems, Supplier must notify PlanGrid of the identity of the proposed Sub processor by email to privacy@plangrid.com.

c. If PlanGrid objects to a Sub processor due to a reasonable belief that the Sub processor cannot provide the level of protection required under this DPA, Supplier will either (i) promptly provide PlanGrid with records or information that provide reasonable assurance that the Sub processor will provide such level of protection or (ii) promptly notify PlanGrid of any available alternatives to change the services or receive the services from an alternate Sub processor. If Supplier cannot promptly do either (i) or (ii) in a manner reasonably acceptable to PlanGrid, PlanGrid may terminate the contract for the services involving the Sub processor and receive a prorated refund for the remaining unused period. This is without prejudice to any other rights or remedies that PlanGrid may have by reason of any breach of this DPA or the Main Agreement.

14. Supplier remains responsible for its Sub processors and liable for their acts and omissions as for its own acts and omissions.

15. Supplier will provide at least the same level of protection for the Personal Data as is required under the EU-U.S. and Swiss-U.S. Privacy Shield, though this DPA does not require Supplier to join such programs. If Supplier determines that it can no longer provide this level of protection, Supplier will promptly notify PlanGrid of this determination.

16. Supplier will make readily available to PlanGrid all information reasonably necessary to demonstrate compliance with this DPA and will allow for and contribute to audits, including inspections, conducted by PlanGrid or another auditor designated by PlanGrid in its sole discretion.

17. PlanGrid may provide this Addendum and a copy of the relevant privacy and security provisions of the Main Agreement to a regulator or PlanGrid customer if required by applicable law, the Accountability for Onward Transfer Principle of the Privacy Shield programs, or by contract provisions that PlanGrid entered into with its customer to legitimize the transfer of the Personal Data from the customer to PlanGrid under applicable law.

18. The provisions of this DPA survive the termination or expiration of the Main Agreement for so long as Supplier or its Sub processors Process PlanGrid Data or have access to PlanGrid Systems, except that Section 10 (Security Breach) survives indefinitely.

19. The Standard Contractual Clauses attached hereto as Annex A form part of this DPA

and take precedence over the rest of this DPA to the extent of any conflict.

| **_____ (Supplier Name)** | **PlanGrid, Inc. for itself and on behalf of its affiliates and subsidiaries worldwide** |
|---|---|
| Signature: _____ | Signature: _____ |
| Print Name: _____ | Print Name: _____ |
| Title: _____ | Title: _____ |
| Date: _____ | Date: _____ |

## Annex A

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

Name and contact information of the data exporting organisations:

PlanGrid, Inc.
2111 Mission St #404
San Francisco, CA 94110
United States of America
(415) 963-4088
privacy@plangrid.com

PlanGrid UK Limited
Floor 11
Whitefriars, Lewins Mead,
Bristol UK, BS1 2NT
+44 (0)20 3695 0292
privacy@plangrid.com

……
(collectively, the data **exporter**)

And

Name of the data importing organisation:

Address:

Tel.:

e-mail:

Other information needed to identify the organization:

……

(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;

(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 Sub processor'* means any processor engaged by the data importer or by any other Sub processor of the data importer who agrees to receive from the data importer or from any other Sub processor 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 Sub processor 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 Sub processor 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 Sub processor 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 Sub processor 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*[1]**

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

[1] 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.

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 Sub processor will be carried out in accordance with Clause 11;

(j) to send promptly a copy of any Sub processor agreement it concludes under the Clauses to the data exporter.

*Clause 6*

***Liability***

1. The parties agree that any 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 Sub processor 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 Sub processor 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 Sub processor 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 Sub processor 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 Sub processor agrees that the data subject may issue a claim against the data Sub processor 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 Sub processor 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 Sub processor, 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 Sub processor preventing the conduct of an audit of the data importer, or any Sub processor, 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 the United Kingdom.

*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 Sub processor which imposes the same obligations on the Sub processor as are imposed on the data importer under the Clauses[2]. Where the Sub processor 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 Sub processor's obligations under such agreement.

2. The prior written contract between the data importer and the Sub processor 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 Sub processor 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 the United Kingdom.

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 Sub processor 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

[2] This requirement may be satisfied by the Sub processor co-signing the contract entered into between the data exporter and the data importer under this Decision.

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 Sub processor 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.

By signing below, the parties also are signing Appendix 1 and Appendix 2 hereto.

**On behalf of the data exporter:**

On behalf of PlanGrid:

Name (written out in full):

Position:

Address: 2111 Mission St #40, San Francisco, CA 94110, USA

Signature…….

**On behalf of the data importer:**

Name (written out in full):

Position:

Address:

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. By signing the Clauses, the parties also are signing this Appendix 1. 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 (please specify briefly activities relevant to the transfer):

*PlanGrid, Inc. - A provider of technology and related services.*

**Data importer**

The data importer is (please specify briefly activities relevant to the transfer):

*The data importer is a service provider who collects or processes personal data upon the instruction of the data exporter in accordance with the terms of the Agreement.*

**Data subjects**

The personal data transferred concern the following categories of data subjects (please specify):

*PlanGrid's customers or end users or employees whose personal data is collected or processed by the service provider.*

**Categories of data**

The personal data transferred concern the following categories of data (please specify):

*All categories of personal data.*

**Processing operations**

The personal data transferred will be subject to the following basic processing activities (please specify):

*The objective behind Processing of Personal Data by the data exporter is in accordance with the services pursuant to the Agreement.*

**Anticipated duration of processing:** For the term of the Main Agreement or until scope of processing changes.

## Appendix 2 to the Standard Contractual Clauses

This Appendix forms part of the Clauses. By signing the Clauses, the parties also are signing this Appendix 2.

**Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached):**

See Annex C to the DPA, which is below.

## Annex B
## Security Requirements

Supplier will comply in all respects with the data security requirements set forth below (the "**Data Security Policy**"), during the term of the Agreement. All terms not defined in this schedule shall have the definitions as set forth in the Data Processing Addendum duly executed by the Parties (**the "Agreement**").

**1. Service Data –** Protection and Non-Disclosure. Supplier shall safeguard Service Data in accordance with this Data Security Policy (and the confidentiality obligations set forth in the Agreement), and will not disclose, transfer or use any such information for any purpose other than to perform its obligations under this Agreement.

**2. System Protection & Recovery -** Supplier will protect its servers hosting Service Data against outages using standard SaaS industry methods designed to prevent outages and minimize impacts during any unavoidable service interruptions, including ensuring (a) its computer system is UPS protected, backed up automatically, and protected by fire suppression systems, and (b) it has implemented and regularly tests a disaster recovery or business continuity plan for its facilities where Service Data is stored.

**3. Data Security** - Supplier will maintain the following basic security requirements during the term of the Agreement: (i) install and maintain a working network firewall to protect data accessible via the Internet; (ii) encrypt all data sent across open networks; (iii) keep security patches up-to-date; (iv) ensure up-to-date anti-virus software is used on all employee laptops; (v) ensure no manufacturer-supplied defaults for system passwords and other security parameters are used; (vi) mandate the use of "strong passwords" for all Supplier employees accessing Service Data in production environments; (vii) regularly test security systems and processes; (viii) maintain a policy that addresses information security for Supplier employees and its suppliers; (ix) restrict physical access to systems containing Service Data; (x) restrict remote access to the entire network and employ remote access controls to verify the identity of users connecting; (xi) protect on-site and off-site backups from unauthorized access during transit and storage; and (xii) no less rigorous than those maintained by PlanGrid for its own Information of a similar nature; (xiii) no less rigorous than generally accepted industry standards, including ISO 27001 and 27002; and (xiv) required by all applicable federal and state laws, rules and regulations relating to privacy, the protection of personal Information and data protection laws and regulations (including without limitation applicable security breach notification laws) (collectively "**Data Privacy Laws"**).

**4. Secure Data Transmission -** Supplier will use the following mechanisms for the protection of Service Data transmission:

(i) XML/HTTP over SSL, with certificate-based authentication utilizing a 2048-bit (or larger) RSA public key, and 128-bit (or stronger) symmetric encryption;

(ii) digitally signed and encrypted S/MIME messages over HTTP or SMTP, using certificates with a 2048-bit (or larger) RSA public key, and 128-bit (or stronger) symmetric encryption;

(iii) digitally signed and encrypted PGP (Pretty Good Privacy) or GPG (Gnu Privacy Guard) messages over a variety of transports, with 2048-bit (or larger) RSA or DH/DSS public keys, and 128-bit (or stronger) symmetric encryption;

(iv) For all message-based encryption schemes employing digital signatures (including PGP and S/MIME), Supplier will verify the digital signature of the message and reject messages with invalid signatures; and

(v) For all encryption schemes employing public key cryptography, Supplier will maintain the confidentiality of the private component of the public-private key pair and will promptly notify Customer in the event that the private key is compromised.

**5. Security Incidents.**

**5.1. Security Incident Notification -** Supplier will inform Customer within 48 hours of detecting any unauthorized access, collection, acquisition, use, transmission, disclosure, corruption or loss of Service Data, or breach of any environment (i) containing Service Data, or (ii) managed by Supplier with controls substantially similar to those protecting Service Data (each, a "**Security Incident**").

**5.2. Remediation -** Supplier will remedy any Security Incident in a timely manner and provide Customer written details regarding Supplier's internal investigation regarding any Security Incident.

**5.3. Formal Notification -** Other than as required by applicable law, Supplier agrees not to notify any regulatory authority, nor any customer, on behalf of Customer unless Customer specifically requests in writing that Supplier does so, and Customer reserves the right to review and approve the form and content of any notification before it is provided to any party. Supplier will cooperate and work together with Customer to formulate and execute a plan to rectify all confirmed Security Incidents.