Airtable Data Processing Addendum

This Data Processing Addendum ("**DPA**") is made as of the date it is fully executed ("**Effective Date**") by and between Formagrid Inc dba Airtable ("**Airtable**") and the entity identified below ("**Customer**"). Airtable and Customer may each be referred to as a "**Party**" and collectively referred to as the "**Parties**" herein. This DPA is incorporated by reference into the agreement between Customer and Airtable that governs Customer's use of the Airtable Products ("**Agreement**"). All capitalized terms used but not defined in this DPA will have the meaning set forth in the Agreement.

This DPA sets out the terms that apply when Customer Personal Data is Processed by Airtable under the Agreement. The purpose of the DPA is to ensure such Processing is conducted in accordance with Applicable Law and respects the rights of individuals whose Personal Data is Processed under the Agreement.

This DPA has been pre-signed by Airtable. When Airtable receives a copy of this DPA that has been signed by Customer, which will occur automatically when the DPA is signed using DocuSign, Airtable's electronic signature provider, the DPA (if validly executed and applicable according to its terms) will become a legally-binding addendum to the Agreement.

1. Definitions

1.1 "**Affiliate**" means an entity that, directly or indirectly, controls, is controlled by, or is under common control with a party. As used herein, "control" means the power to direct the management or affairs of an entity and the beneficial ownership of fifty percent (50%) or more of the voting equity securities or other equivalent voting interests of an entity.

1.2 "**Applicable Law(s)**" means all US, UK, and EU laws, regulations, and other legal or regulatory requirements relating to privacy, data protection/security, or the Processing of Personal Data applicable to Airtable's performance of its services under the Agreement, including without limitation the California Consumer Privacy Act, Cal. Civ. Code § 1798.100 *et seq.* and its amendments and implementing regulations ("**CCPA**"), the United Kingdom Data Protection Act 2018, and the General Data Protection Regulation (Regulation (EU) 2016/679) ("**GDPR**"), and the United Kingdom GDPR ("**UK GDPR**"). For the avoidance of doubt, if Airtable's Processing activities involving Personal Data are not within the scope of an Applicable Law, such Applicable Law is not applicable for purposes of this DPA.

1.3 "**Airtable**" means Formagrid Inc and its worldwide affiliates and subsidiaries.

1.4 "**Airtable Products**" means the products and services provided by Airtable to Customer as specified in the Agreement.

1.5 "**Business Contact Data**" means business contact information and Airtable account log-in data of Customer's employees and Permitted Users of the Airtable Products.

1.6 "**Customer Personal Data**" means Customer Data, as defined in the Agreement, consisting of Personal Data, except for Business Contact Data.

1.7 "**EEA**" means, for purposes of this DPA, the European Economic Area (which is composed of the member states of the European Union), Norway, Iceland, Liechtenstein, and Switzerland.

1.8 "**EU SCCs**" means the Standard Contractual Clauses issued pursuant to the EU Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council, available at http://data.europa.eu/eli/dec_impl/2021/914/oj and completed as described in Section 9 (International Data Transfers).

1.9 "**Personal Data Breach**" means the accidental or unlawful destruction, loss, alteration, or unauthorized disclosure of or access to Customer Personal Data.

1.10 "**Personal Data**" includes "personal data," "personal information," and "personally identifiable information," each as defined by Applicable Law.

1.11 "**Process**" and "**Processing**" mean any operation or set of operations performed on Personal Data, or on sets of

Personal Data, whether or not by automated means, such as collecting, recording, organizing, creating, structuring, storing, adapting or altering, retrieving, consulting, using, disclosing (by transmission, dissemination or otherwise making such data available), aligning or combining, restricting, erasing, or destroying such Personal Data.

1.12 "**Standard Contractual Clauses**" means the EU SCCs or the UK SCCs, as applicable.

1.13 "**UK SCCs**" means the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses, available as of the Effective Date at https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-data-transfer-agreement-and-guidance/ and completed as described in Section 9 (International Data Transfers).

2. Relationship of the Parties

2.1 Customer is the Controller and Business as defined under the Data Protection Laws, and Customer determines the means and purposes for which Customer Personal Data is Processed by Airtable. To the extent Airtable Processes Customer Personal Data subject to the Data Protection Laws, Airtable is a Processor and Service Provider as defined under the Data Protection Laws, and Airtable will Process the Customer Personal Data according to the instructions set forth in this DPA, the Agreement, and as required under Data Protection Laws. Customer and Airtable are independent Controllers and Businesses, as defined under the Data Protection Laws, with respect to Business Contact Data. Either party may Process Business Contact Data as necessary for the purpose of (i) carrying out its obligations under the Agreement, (ii) applicable legal or regulatory requirements, (iii) requests and communications with the other party, (iv) administrative, business, and marketing purposes, and (v) to protect its respective rights in accordance with applicable law and, in the case of Airtable, maintaining the security and integrity of the Airtable Products.

2.2 Airtable hereby certifies that it understands the restrictions and obligations set forth in this DPA in relation to its role as a Processor and Service Provider, and that it will comply with them.

3. Customer's Instructions to Airtable

3.1 Purpose Limitation. Airtable will not (a) sell Customer Personal Data, (b) Process Customer Personal Data for any purpose other than for the specific purposes set forth in the Agreement, (c) retain, use, or disclose any such data outside of the direct business relationship between the Parties, or (d) otherwise engage in any Processing of Customer Personal Data beyond that in which a Processor may engage under the Applicable Law or in which a Service Provider may engage under the Applicable Law, unless obligated to do otherwise by Applicable Law. In such a case, Airtable will inform Customer of the applicable legal obligation before engaging in the Processing, unless legally prohibited from doing so. Further details regarding Airtable's Processing operations are set forth in Exhibit B.

3.2 Lawful Instructions. Customer will not instruct Airtable to Process Customer Personal Data in violation of Applicable Law. Airtable will without undue delay inform Customer if, in Airtable's opinion, an instruction from Customer infringes Applicable Law. The Agreement, including this DPA, constitutes Customer's complete and final instructions to Airtable regarding the Processing of Customer Personal Data, including for purposes of the Standard Contractual Clauses.

4. Limitations on Disclosure

Airtable will not disclose Customer Personal Data to any third party without first obtaining Customer's written consent, except as provided in Section 5 (Subcontracting), Section 7 (Responding to Individuals Exercising Their Rights Under Applicable Law) or Section 9 (Data Transfers), except as required by law. Airtable will require all employees, contractors, and agents who Process Customer Personal Data on Airtable's behalf to protect the confidentiality of the Customer Personal Data and to comply with the other relevant requirements of this DPA.

5. Subcontracting

5.1 Sub-Processors. Airtable may subcontract the collection or other Processing of Customer Personal Data only in compliance with Applicable Law and any additional conditions for subcontracting set forth in the Agreement. Customer acknowledges and agrees that Airtable's Affiliates and certain third parties may be retained as sub-

processors to Process Customer Personal Data on Airtable's behalf (under this DPA as well as under the Standard Contractual Clauses, if they apply) in order to provide the Airtable Products. Airtable's third-party sub-processors are listed at http://www.airtable.com/subprocessors (the "**Sub-processor List**"). Prior to a sub-processor's Processing of Customer Personal Data, Airtable will impose contractual obligations on the sub-processor substantially the same as those imposed on Airtable under this DPA to the extent applicable to the nature of the services provided by such sub-processor. Airtable remains liable for its sub-processors' performance under this DPA to the same extent Airtable is liable for its own performance.

5.2 Notification. Airtable will provide Customers with at least ten (10) days' written notice of new sub-processors before authorizing such sub-processor(s) to Process Customer Personal Data in connection with the provision of the Airtable Products. Airtable will notify Customer at the email address provided in the signature block of this DPA for purposes of this notification. The sub-processor agreements to be provided under Clause 5(j) of the EU SCCs may have all commercial information, or provisions unrelated to the EU SCCs, redacted prior to sharing with Customer, and Customer agrees that such copies will be provided only upon written request.

5.3 Right to Object. Customer may object to Airtable's use of a new sub-processor on reasonable grounds relating to the protection of Customer Personal Data by notifying Airtable promptly in writing at legal@airtable.com within ten (10) business days after receipt of Airtable's notice in accordance with the mechanism set out in Section 5.2. In its notification, Customer will explain its reasonable grounds for objection. In the event Customer objects to a new sub-processor, Airtable will use commercially reasonable efforts to make available to Customer a change in the Airtable Products or recommend a commercially reasonable change to Customer's configuration or use of the Airtable Products to avoid Processing of Customer Personal Data by the objected-to new sub-processor without unreasonably burdening Customer. If Airtable is unable to make available such change within a reasonable period of time, which will not exceed thirty (30) days, either Party may terminate without penalty the Processing of Customer Personal Data and/or the Agreement with respect only to those services which cannot be provided by Airtable without the use of the objected-to new sub-processor by providing written notice to the other Party.

6. Assistance & Cooperation

6.1 Security. Airtable will provide reasonable assistance to Customer regarding Customer's compliance with its security obligations under Applicable Law relevant to Airtable's role in Processing Customer Personal Data, taking into account the nature of Processing and the information available to Airtable, by implementing the technical and organizational measures set forth in Exhibit A, without prejudice to Airtable's right to make future replacements or updates to the measures that do not materially lower the level of protection of Customer Personal Data. Airtable will ensure that the persons Airtable authorizes to Process the Customer Personal Data are subject to written confidentiality agreements or are under an appropriate statutory obligation of confidentiality no less protective than the confidentiality obligations set forth in the Agreement.

6.2 Personal Data Breach Notification & Response. Airtable will comply with the Personal Data Breach-related obligations directly applicable to it under Applicable Law. Taking into account the nature of Processing and the information available to Airtable, Airtable will inform Customer of a substantiated Personal Data Breach without undue delay or within the time period required under Applicable Law, and in any event no later than seventy-two (72) hours following such substantiation. Airtable will notify Customer at the email address provided in the signature block of this DPA for purposes of Personal Data Breach notifications. Any such notification is not an acknowledgement of fault or responsibility. This notification will include Airtable's then-current assessment of the following information, to the extent available, which may be based on incomplete information:

(a) the nature of the Personal Data Breach, including, where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of Customer Personal Data records concerned;

(b) the likely consequences of the Personal Data Breach; and

(c) measures taken or proposed to be taken by Airtable to address the Personal Data Breach, including, where applicable, measures to mitigate its possible adverse effects.

Airtable will provide timely and periodic updates to Customer as additional information regarding the Personal Data Breach becomes available. Customer is solely responsible for complying with legal requirements for incident

notification applicable to Customer and fulfilling any third-party notification obligations related to any Personal Data Breach. Nothing in this DPA or in the Standard Contractual Clauses will be construed to require Airtable to violate, or delay compliance with, any legal obligation it may have with respect to a Personal Data Breach or other security incidents generally.

7. Data Subject Requests

To the extent legally permitted, Airtable will without undue delay notify Customer if Airtable receives any request from an individual seeking to exercise any right afforded to them under Applicable Law regarding their Customer Personal Data (a "**Data Subject Request**"). To the extent Customer, in its use of the Airtable Products, does not have the ability to address a Data Subject Request, Airtable will, upon Customer's request, take commercially reasonable efforts to assist Customer in responding to such Data Subject Request, to the extent Airtable is legally permitted to do so and the response to such Data Subject Request is required under Applicable Law.

8. DPIAs and Consultation with Supervisory Authorities or other Regulatory Authorities

Upon Customer's written request, Airtable will provide Customer with reasonable cooperation and assistance as needed and appropriate to fulfill Customer's obligations under Applicable Law to carry out a data protection impact assessment related to Customer's use of the Airtable Products. Airtable will provide reasonable assistance to Customer in the cooperation or prior consultation with the Supervisory Authority (as defined under the GDPR) in the performance of its tasks relating to the data protection impact assessment, and to the extent required under the Applicable Law.

9. International Data Transfers

9.1 Customer authorizes Airtable and its sub-processors to make international transfers of the Customer Personal Data in accordance with this DPA so long as Applicable Law for such transfers is respected.

9.2 With respect to Customer Personal Data transferred from the EEA, the EU SCCs will apply and form part of this DPA, unless the European Commission issues updates to the EU SCCs, in which case the updated EU SCCs will control. Undefined capitalized terms used in this provision will have the meanings given to them (or their functional equivalents) in the definitions in the EU SCCs. For purposes of the EU SCCs, they will be deemed completed as follows:

(a) Where Customer acts as a Controller and Airtable acts as Customer's Processor with respect to Customer Personal Data subject to the EU SCCs, Module 2 applies.

(b) Where Customer acts as a Processor and Airtable acts as Customer's sub-processor with respect to Customer Personal Data subject to the EU SCCs, Module 3 applies.

(c) Clause 7 (the optional docking clause) is not included.

(d) Under Clause 9 (Use of sub-processors), the Parties select Option 2 (General written authorization). The initial list of sub-processors is set forth at http://www.airtable.com/subprocessors. Airtable will provide notice of updates to that list at least ten (10) business days in advance of any intended additions or replacements of sub-processors, in accordance with Section 5 of this DPA.

(e) Under Clause 11 (Redress), the optional requirement that data subjects be permitted to lodge a complaint with an independent dispute resolution body is inapplicable.

(f) Under Clause 17 (Governing law), the Parties select Option 1 (the law of an EU Member State that allows for third-party beneficiary rights). The Parties select the law of Ireland.

(g) Under Clause 18 (Choice of forum and jurisdiction), the Parties select the courts of Ireland.

(h) Annexes I and II of the EU SCCs are set forth in Exhibit B below.

(i) Annex III of the EU SCCs (List of sub-processors) is inapplicable.

(j) By entering into this DPA, the Parties are deemed to be signing the EU SCCs.

9.3 With respect to Customer Personal Data transferred from the United Kingdom for which the law of the United Kingdom (and not the law in any European Economic Area jurisdiction) governs the international nature of the

transfer, the UK SCCs form part of this DPA and take precedence over the rest of this DPA as set forth in the UK SCCs, unless the United Kingdom issues updates to the UK SCCs, in which case the updated UK SCCs will control. Undefined capitalized terms used in this provision will have the meanings given to them (or their functional equivalents) in the definitions in the UK SCCs. For purposes of the UK SCCs, they will be deemed completed as follows:

(a) Table 1 of the UK SCCs:

i. The Parties' details are the Parties and their affiliates to the extent any of them is involved in such transfer, including those set forth in Exhibit B.

ii. The Key Contacts are the contacts set forth in Exhibit B.

(b) Table 2 of the UK SCCs: The Approved EU SCCs referenced in Table 2 are the EU SCCs as executed by the Parties pursuant to this Addendum.

(c) Table 3 of the UK SCCs: Annex 1A, 1B, and II are set forth in Exhibit B.

(d) Table 4 of the UK SCCs: Either party may terminate this Addendum as set forth in Section 19 of the UK SCCs.

(e) By entering into this DPA, the Parties are deemed to be signing the UK SCCs and their applicable Tables and Appendix Information.

9.4 With respect to Customer Personal Data transferred from Switzerland for which Swiss law (and not the law in any European Economic Area jurisdiction) governs the international nature of the transfer, the EU SCCs will apply and will be deemed to have the following differences to the extent required by the Swiss Federal Act on Data Protection ("**FADP**"):

(a) References to the GDPR in the EU SCCs are to be understood as references to the FADP insofar as the data transfers are subject exclusively to the FADP and not to the GDPR.

(b) The term "**member state**" in the EU SCCs will not be interpreted in such a way as to exclude data subjects in Switzerland from the possibility of suing for their rights in their place of habitual residence (Switzerland) in accordance with Clause 18(c) of the EU SCCs.

(c) References to Personal Data in the EU SCCs also refer to data about identifiable legal entities until the entry into force of revisions to the FADP that eliminate this broader scope.

(d) Under Annex I(C) of the EU SCCs (Competent supervisory authority): where the transfer is subject exclusively to the FADP and not the GDPR, the supervisory authority is the Swiss Federal Data Protection and Information Commissioner, and where the transfer is subject to both the FADP and the GDPR, the supervisory authority is the Swiss Federal Data Protection and Information Commissioner insofar as the transfer is governed by the FADP, and the supervisory authority is as set forth in the EU SCCs insofar as the transfer is governed by the GDPR.

10. Audits

Airtable will allow for and contribute to audits, including inspections, conducted by Customer or another auditor mandated by Customer subject to the following conditions: so long as the Agreement remains in effect, Customer may request that Airtable provide it with Airtable's most recent SOC II Type II and ISO 27001 reports ("**Records**") no more than once annually relating to Airtable's compliance with this DPA (an "**Audit**"). To the extent Customer uses a third-party representative at Customer's sole expense to conduct the Audit, Customer will ensure that such third-party representative is bound by obligations of confidentiality no less protective than those contained in the Agreement. Customer will provide Airtable with ninety (90) business days prior written notice of its intention to conduct an Audit. Customer will conduct the Audit in a manner that will result in minimal disruption to Airtable's business operations and such Audit will take no longer than two (2) business days. Further, Customer will not be entitled to receive data or information of other customers of Airtable or any other Confidential Information of Airtable that is not directly relevant for the authorized purposes of the Audit.

11. Legal Process

If Airtable is legally compelled by a court or other government authority to disclose Customer Personal Data, then to the extent permitted by law, Airtable will promptly provide Customer with sufficient notice of all available details of the legal requirement and reasonably cooperate with Customer's efforts to challenge the disclosure, seek an appropriate protective order, or pursue such

other legal action, as Airtable deems appropriate.

12. Destruction of Personal Data

Upon termination of the Agreement and written request from Customer, Airtable will delete or anonymize Customer Personal Data, unless prohibited by Applicable Law. Notwithstanding the foregoing, nothing will oblige Airtable to delete or anonymize Customer Personal Data from files created for security, backup and business continuity purposes sooner than required by Airtable's data retention processes.

13. Applicability and Order of Precedence

This DPA replaces any existing data processing addendum the Parties may have previously entered into in connection with the Agreement. In the event of a conflict between the terms of the Agreement and this DPA, the terms of the DPA will apply. In the event of a conflict between this DPA and the applicable Standard Contractual Clauses, the Standard Contractual Clauses will apply.

This DPA is signed by duly authorized representatives of the Parties and is effective as of the Effective Date:

alberto villa VIA TRIPOLITANIA 195 ROMA ROMA (RM) 00199 ITALIA	**FORMAGRID INC** 799 Market St., 8th Floor San Francisco, California 94103
DocuSigned by: Alberto Villa 50388ABD9C554EC... Signature ALBERTO VILLA Name PRESIDENTE Title 9/4/2023 Date Signed Email: alberto.villa@kronosroma.it	Yoel Gluck Signature Yoel Gluck Name Head of Security Title Date Signed: September 21, 2022 Email: legal@airtable.com

Exhibit A
Information Security Addendum

This Information Security Addendum ("**Addendum**") describes the technical and organizational measures implemented by Airtable to ensure an appropriate level of security and supplements and forms part of the Master Subscription Agreement, Terms of Service, Data Processing Addendum or other written or electronic agreement between Airtable and Customer governing the use of Airtable's products and services ("**Agreement**"). In the event of a conflict between the terms of the Agreement and this Addendum, the terms of the Agreement will apply. Capitalized terms used but not defined herein will have the meaning set forth in the Agreement.

1. ACCESS CONTROLS

a. Control Measures. Airtable has implemented reasonable system access controls and physical access controls designed to limit access based on authorization and prevent personnel and others who should not have access from obtaining access to Airtable systems housing Customer Personal Data.

b. System Access Controls. Airtable's system access control measures include the following:

i. Restricting unauthorized users from accessing information not needed for their roles through role-based user access and using least privileged principles.
ii. Unique user accounts identifiable to individual users, password requirements, and two-factor authentication.
iii. Provisioning and removal of employee access to Customer Personal Data when access is no longer required.
iv. Periodic access reviews to ensure that only Airtable personnel who still require access to Customer Personal Data have it.

c. Physical Access Controls. Airtable utilizes cloud hosting infrastructure, currently Amazon Web Services ("**AWS**") hosting infrastructure, with regard to the Airtable Products. All physical security controls are managed by the cloud hosting provider. Annually, Airtable reviews the applicable security and compliance reports of its cloud hosting provider to ensure appropriate physical security controls, including:

i. Use of data centers with physical and environmental controls appropriate to the risk for Customer Personal Data and for the equipment, assets, or facilities used to hold and Process such Customer Personal Data (e.g. use of key card access controls and security guard monitoring).
ii. Use of data centers with 24/7 security protection, automatic fire detection and suppression, fully redundant power systems, and other reasonable environmental controls.

2. OPERATIONS MANAGEMENT AND NETWORK SECURITY

a. Airtable establishes and maintains reasonable operations management and network security measures, including the following:

i. Network segmentation based on the label or classification level of the information stored.
ii. Protection of servers and web applications using restrictive firewalls.
iii. Regular review, testing, and installation of security updates and patches to servers.

3. CHANGE MANAGEMENT

a. Airtable maintains a formal change and release management policy and procedure for software, system, and configuration changes. Such policies and procedures include:

i. A process for testing, and approving promotion of changes to production.
ii. A process for performing security assessments of changes into production.

b. Airtable follows secure application development policies, procedures, and standards that are aligned to industry-

standard practices, such as the OWASP Top 10.

i. Airtable provides secure code development training based on role for secure application development, configuration, testing, and deployment.

4. DATA ENCRYPTION AND DELETION

a. Airtable encrypts Customer Personal Data while at rest using industry best practice encryption standards and methods.

b. Airtable encrypts Customer Personal Data while in transit using industry standard encryption methods designed to encrypt communications between its server(s) and customer browser(s).

c. Airtable uses cryptographic controls and approved algorithms for information protection within the service environment based on Airtable's company policies and standards.

d. Airtable encrypts employee workstations with full disk encryption, strong passwords, and screen lockout.

e. Airtable maintains policies and procedures regarding the deletion of Customer Personal Data in accordance with applicable laws and NIST guidance. Customer Personal Data is deleted upon customer request and removed off our cloud hosting provider servers.

5. SUB-PROCESSORS

a. Airtable uses certain sub-processors to assist Airtable in providing the Airtable platform and associated services. Prior to engaging any sub-processor who has or potentially will have access to or Processes Customer Personal Data, Airtable conducts an assessment of the security and privacy practices of the sub-processor to ensure they are commensurate with the level of data access the sub-processor will have and the scope of the services it will provide. Airtable then enters into a written agreement with the sub-processor containing privacy, data protection, and data security obligations that ensure a level of protection appropriate to the sub-processor's Processing activities.

b. Airtable performs annual reviews of its sub-processors ensuring that compliance and security standards are maintained and material changes to processes are reviewed.

6. SYSTEM MONITORING AND VULNERABILITY MANAGEMENT

a. Airtable regularly monitors its production environment Processing Customer Personal Data for unauthorized intrusions, vulnerabilities, etc. Airtable's system monitoring measures include the following:

i. Use of intrusion detection measures to prevent and identify potential security attacks from users outside the boundaries of the system.
ii. Automated application and infrastructure vulnerability scans are performed to identify vulnerabilities. Airtable classifies its vulnerabilities using industry standards and remediates its vulnerabilities based on severity level.
iii. Annual third-party penetration testing. An executive summary can be provided upon request.
iv. Annual risk assessments and continuous monitoring of Airtable's risk register.
v. Periodic third-party security audits, such as SOC 2 Type 2 and ISO27001 audits.
vi. Monitoring, logging, and reporting on critical/suspicious activities with regard to network devices, including retention of logs for forensic-related analysis. Airtable maintains audit logs that record and examine activity within Airtable's production environment. Logs are backed up in real time and Airtable has implemented controls in place to prevent modification or tampering of logs.
vii. Operation of a "bug bounty" program to identify potential security vulnerabilities.
viii. Deployment of anti-virus & malware tools to detect and remediate harmful code or programs that can negatively impact the Airtable Products.

7. PERSONNEL CONTROLS

a. Airtable uses reasonable efforts to ensure the continued reliability of employees who have access to Customer Personal Data by implementing the following measures:

i. Conducting background checks, subject to applicable laws, on all Airtable employees who may access Customer Personal Data.
ii. Requiring employees to acknowledge Airtable's information security policies, including but not limited to Airtable's Code of Conduct and Acceptable Use Policy, upon hire and complete new-hire security training.
iii. Requiring employees to complete annual privacy and security training covering topics that address their obligations to protecting Customer Personal Data and privacy and security best practices.
iv. Instructing them to report potential Personal Data Breaches to the security team.
v. Imposing sanctions for material violations of Airtable's information security policy.

8. BACKUPS, BUSINESS CONTINUITY AND DISASTER RECOVERY

a. Backups. Airtable maintains a policy and procedure for performing backups of Customer Personal Data.

b. Business Continuity Program. Airtable maintains a reasonable business continuity program, including a disaster recovery plan, designed to minimize disruption to the Airtable Products. The plans are tested annually and the process is amended, as needed.

9. DATA BREACH MANAGEMENT

a. Personal Data Breach Notification. Airtable will notify Customer promptly and without undue delay after confirming a Personal Data Breach, and promptly take reasonable steps to minimize harm and secure Customer Personal Data.

b. Details of the Personal Data Breach. Airtable's notification of a Personal Data Breach will describe, to the extent possible, the nature of the Personal Data Breach, the measures taken to mitigate the potential risks, and any measures Airtable recommends Customer take to address the Personal Data Breach.

10. SECURITY REVIEW

a. Certification Audit. Upon Customer's written request (email to suffice), Airtable will provide to Customer for review a copy of Airtable's most recent annual SOC II Type II audit results, and a copy of its then-current ISO 27001 certificate.

11. MODIFICATIONS

a. Modifications to Security Procedures. Customer acknowledges and agrees that from time to time Airtable will modify its systems and security procedures. Airtable will notify Customer before making any modifications to its systems and security procedures that materially reduce the level of security required under this Addendum.

Exhibit B
Annexes I and II of the EU SCCs

ANNEX I

A. LIST OF PARTIES

MODULE TWO: Transfer Controller to Processor

MODULE THREE: Transfer Processor to Processor

Data exporter(s):

Name: The exporter is the Customer specified in the Agreement.

Address: specified in the Agreement.

Contact person's name, position and contact details: specified in the Agreement.

Activities relevant to the data transferred under these Clauses: Obtaining the Airtable Products from data importer.

Role (Controller/Processor): Controller

Data importer(s):

Name: Formagrid Inc dba Airtable

Address: 799 Market Street, 8th Floor, San Francisco, CA 94103

Contact person's name, position and contact details: Legal Department, legal@airtable.com

Activities relevant to the data transferred under these Clauses: Providing the Airtable Products to data exporter.

Role (Controller/Processor): Processor

B. DESCRIPTION OF TRANSFER

MODULE TWO: Transfer Controller to Processor

MODULE THREE: Transfer Processor to Processor

Categories of data subjects whose personal data is transferred

Data subjects whose Personal Data is uploaded by data exporter to, or otherwise received directly or indirectly from data exporter (including from a Permitted User on data exporter's behalf) by or through, the Airtable Products, or provided by data exporter to Airtable to input into the Airtable Products.

Categories of personal data transferred

The data exporter may transfer Personal Data to Airtable, the extent of which is determined and controlled by the data exporter in its sole discretion. Such Personal Data may include any category of Personal Data the data exporter or its Permitted Users may enter into the Airtable Products.

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialized training), keeping a record of access to the data, restrictions for onward transfers or additional

security measures.

None anticipated.

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).

Continuously, for the length of the Agreement between the Parties.

Nature of the processing

Customer Personal Data transferred will be processed to (i) provide the Airtable Products to the data exporter and fulfill the data importer's obligations under the Agreement; and (ii) comply with applicable law.

Purpose(s) of the data transfer and further processing

Customer Personal Data transferred will be processed to (i) provide the Airtable Products to the data exporter and fulfill the data importer's obligations under the Agreement; and (ii) comply with applicable law.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

Customer Personal Data will be retained for the length of time necessary to provide Airtable Products under the Agreement and in accordance with Airtable's data retention processes and as otherwise required by applicable law.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

Airtable's sub-processors will process Customer Personal Data to assist Airtable in providing the Airtable Products pursuant to the Agreement, for as long as needed for Airtable to provide the Airtable Products.

C. COMPETENT SUPERVISORY AUTHORITY

MODULE TWO: Transfer Controller to Processor

MODULE THREE: Transfer Processor to Processor

Identify the competent supervisory authority/ies in accordance with Clause 13.

The Parties will follow the rules for identifying such authority under Clause 13 and, to the extent legally permissible, select the Irish Data Protection Commission.

ANNEX II - TECHNICAL AND ORGANIZATIONAL MEASURES INCLUDING TECHNICAL AND ORGANIZATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

MODULE TWO: Transfer Controller to Processor

MODULE THREE: Transfer Processor to Processor

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

Please see Exhibit A of the DPA, which describes the technical and organizational security measures implemented by Airtable.