Exhibit A

Data Processing Addendum

This **Data Processing Addendum ("DPA")**, is made pursuant to the order form to which it is attached (the "**Order Form**"), by and between Impartner, Inc. ("**Impartner**") and the customer indicated on page 1 of the Order Form ("**Customer**," or "**Data Controller**"). This DPA will govern the Order Form as well as any subsequent order forms, amendments, and/or renewals, unless otherwise expressly agreed in writing between the parties. The Order Form and any exhibits attached thereto, including this DPA, shall be referred to collectively herein as the "**Agreement**."

This DPA reflects the parties' agreement with regard to the Processing of Personal Data. All capitalized terms in this DPA have the meaning assigned to them in the Order Form, Subscription Agreement / Terms of Use, and any other exhibits attached thereto, unless expressly defined otherwise in this DPA. In the event of any conflict/s between the Order Form, Subscription Agreement / Terms of Use, and Data Processing Addendum, unless expressly indicated otherwise, the order of precedence shall be: (i) Data Processing Addendum, (ii) Order Form, (iii) Subscription Agreement. Any exhibits will be incorporated by reference and shall take the precedence of the document to which it has been addended.

In the course of providing the Service to Customer pursuant to the Agreement, Impartner may Process Personal Data on behalf of Customer and the parties agree to comply with the following provisions with respect to any Personal Data, each acting reasonably and in good faith.

Introduction

A. Customer is a Controller or Processor of certain Personal Data and wishes to appoint Impartner as a Processor or sub-processor to Process this Personal Data on Customer's behalf.

B. The parties have entered into this DPA to ensure that Impartner conducts such data Processing in accordance with Customer's instructions and Applicable Data Protection Law requirements, and with full respect for the fundamental data protection rights of the Data Subjects whose Personal Data will be Processed.

Definitions

In this DPA, the following terms shall have the following meanings. Other capitalized terms used in this DPA are defined in the context in which they are used or shall have the meanings given such terms in the Order Form or Subscription Agreement.

"**Applicable Data Protection Law**" shall mean: (i) Regulation 2016/679 of the European Parliament and of the Council 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 or "GDPR") and any data protection laws in any European Union Member State including laws implementing such Regulation, (ii) the California Consumer Privacy Act of 2018 ("CCPA"), including any regulations promulgated thereunder, as amended from time to time; (iii) the UK GDPR, and (iv) any other applicable data protection law.

"**Controller**" means the entity which determines the purposes and means of the Processing of Personal Data.

"**Data Subject**" means the identified or identifiable person to whom Personal Data relates.

"EU Standard Contractual Clauses" / "EU SCCs" means Module Two of the standard contractual clauses for the transfer of Personal Data, in accordance with Applicable Data Protection Law, to Controllers and Processors established in Third Countries, the approved version of which is in force at

the date of signature of this Agreement that are in the European Commission's Decision 2021/914 of 4 June 2021, as such standard contractual clauses are available at https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en, and as may be amended or replaced by the European Commission from time to time, and as further defined in clause 4 of this DPA.

"**Personal Data**" means any information relating to (i) an identified or identifiable natural person and, (ii) an identified oridentifiable legal entity (where such information is protected similarly as personal data or personally identifiable information under applicable Data Protection Laws and Regulations), where for each (i) or (ii), such data is CustomerData.

"**Processing**" (and "**Process**") means any operation or set of operations which is performed upon Personal Data, whether or not by automatic means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

"**Processor**" means the entity which Processes Personal Data on behalf of the Controller.

"Supervisory Authority(ies)" shall carry the meaning of that term in the GDPR.

"**UK Standard Contractual Clauses**" / "**UK SCCs**" means the standard contractual clauses for controllers to processors approved by the European Commission by way of Commission Decision C(2010)593, as amended by the UK Information Commissioner's Office for use in a UK context, available on the date of this Agreement at https://ico.org.uk/media/for-organisations/documents/2618973/uk-sccs-c-p-202012.docx, and as may be amended or replaced by the Information Commissioner's Office or/and Secretary of State from time to time.

Data Protection

1. *Relationship of the parties*. Customer appoints Impartner as a Processor, or service provider, to Process the Personal Data that is the subject matter of the Agreement (the "**Data**"). Accordingly, the parties acknowledge and agree that with regard to the Processing of Personal Data, Customer is the Controller and Impartner is the Processor. Each party shall comply with theobligations that apply to it under Applicable Data Protection Law. Customer hereby represents and warrants that Customer complies with the requirements in the Applicable Data Protection Law in collecting and transferring the data to Impartner and permitting Impartner to act as a processor of the Data. Customer agrees that it will not disclose any special categories of personal information to Impartner and Customer will indemnify Impartner from any third-party claims against Impartner as a result of such disclosure.

2. *Purpose limitation*. Customer hereby instructs Impartner to Process Personal Data and to transfer Personal Data to any country or territory as necessary for the provision of the Service and consistent with the Agreement. Customer's instructions for the Processing of Personal Data shall comply with Applicable Data Protection Law. Customer shall have sole responsibility for the accuracy, quality, and legality of the Data and the means by which Customer acquires the Data. Impartner shall Process the Data as a Processor only as necessary to perform its obligations under the Agreement, and in accordance with the documented instructions of Customer (the "**Permitted Purpose**"), except where otherwise required by any EU (or any EU Member State) law applicable to Impartner, in which case Impartner shall to the extent permitted by Applicable Data Protection Law inform Customer of that legal requirement before the relevant Processing of that Data. In no event shall Impartner Process the Data for its own purposes or those of any third party except as set forth in the Agreement. Impartner shall also inform Customer if in its opinion an instruction of Customer infringes or violates Applicable Data Protection Law. Impartner shall not sell the Data, nor process, retain, use, or disclose the Data (i) for any purposes other than the Permitted Purpose, or (ii) outside of the direct business relationship between Impartner and Customer.

3. *Details of the Processing*. Annex 1 to this DPA sets out certain information regarding Impartner's Processing of the Data as required by Article 28(3) of the GDPR. Either party may make reasonable amendments to Annex 1 by written notice to the other party from time to time as such party reasonably considers necessary

to meet those requirements. Nothing in Annex 1 (including as amended pursuant to this Section 3) confers any right or imposes any obligation on any party to this DPA.

4. *International transfers*. Impartner shall not transfer any Personal Data of European Economic Area ("**EEA**") / UK Data Subjects (nor permit such Personal Data to be transferred) outside of the EEA / UK unless (i) it has first obtained Customer's prior written consent; and (ii) it takes such measures as are necessary to ensure the transfer is in compliance with Applicable Data Protection Law. Such measures may include (without limitation) transferring the Personal Data to a recipient in a country that the European Commission / UK authorities have decided provides adequate protection for Personal Data, or to a recipient that has achieved binding corporate rules authorization in accordance with Applicable Data Protection Law, or to a recipient that has executed the Standard Contractual Clauses adopted or approved by the European Commission / UK Secretary of State or the UK Information Commissioner (and approved by the UK Parliament). Partner hereby consents to the transfer of Personal Data to Impartner in the United States and the parties agree that the EU / UK Standard Contractual Clauses will apply to any such transfer, as appropriate.

    a. The EU SCCs shall be deemed incorporated in this Agreement as follows:
        - Clause 7 of the EU SCCs, the "Docking Clause (Optional)", shall be deemed incorporated;
        - in Clause 9 of the EU SCCs, the Parties choose Option 2, 'General Written Authorisation', with a time period of 10 days;
        - the optional wording in Clause 11 of the EU SCCs shall be deemed not incorporated;
        - in Clause 17 of the EU SCCs, the Data Exporter and Data Importer agree that the EU SCCs shall be governed by the laws of the Netherlands and choose Option 1 to this effect;
        - in Clause 18 of the EU SCCs, the Data Exporter and Data Importer agree that any disputes shall be resolved by the courts of the Netherlands;
        - Annexes I.A, I.B, I.C, II and III of the EU SCCs shall be deemed completed with the information set out in Annex 1, Annex 2 and Annex 3 to this DPA.

    b. Where the UK SCCs apply (i.e., for transfers from UK to countries, which were not recognized as providing adequate protections by UK authorities), they will be deemed incorporated in this Agreement as follows:
        - in Clause 9 of the UK SCCs, the Parties agree that UK SCCs shall be governed by the laws of the United Kingdom.
        - in Clause 12 of the UK SCCs, the Optional "Indemnification" and "Priority of standard contractual clauses" Clauses are deemed not incorporated;
        - Annex 1 and 2 of the UK SCCs shall be deemed completed with the information set out in Annex 1 and Annex 2 of this DPA; and
        - in light of the obligations of the parties under UK SCCs, read in light of the Schrems II judgment issued by the Court of Justice of the European Union on July 16, 2020 ("Schrems II"), in regard to the transfer of personal data by Data Exporter from the UK to Data Importer located outside the UK in countries, which were not granted an adequacy decision by the UK Secretary of State ("Third Country"), parties hereby warrant to honour the supplementary safe-guards, as outlined in Annex 4 to UK SCCs, which forms its integral part. For the avoidance of doubt, this clause shal be referred to as the Supplementary Safeguards clause. In case of conflict between this Supplementary Safeguards Clause, and the UK SCCs, the UK SCCs shall prevail.

5. *Confidentiality of Processing*. Impartner shall ensure that any person that it authorizes to Process the Data (including Impartner's staff, agents and subcontractors) (an "**Authorized Person**") shall be subject to a strict duty of confidentiality (whether a contractual duty or a statutory duty) and shall not permit any person to Process the Data who is not under such a duty of confidentiality. Impartner shall ensure that all Authorized Persons Process the Data only as necessary for the Permitted Purpose.

6. *Security*. Impartner shall implement appropriate technical and organizational measures to protect the Data (i) from accidental or unlawful destruction, and (ii) loss, alteration, unauthorized disclosure of, or access to the Data (a "Security Incident"). Such measures shall take into account the state of the art, the costs of implementation and the nature, scope, context and purpose of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons. Such measures may include those

listed in Appendix 2.

7. *Sub-processing*.

   7.1 Impartner may subcontract any processing of the Data to a third-party subcontractor ("**Sub-Processor**") in accordance with Applicable Data Protection Law. A list of Impartner's current authorized Sub-Processors (the "**List**") will be made available to Customer, either attached hereto, at a link provided to Customer, via email or through another means made available to Customer. Such List may be updated by Impartner from time to time. Impartner may provide a mechanism to subscribe to notifications of new authorized Sub-Processors and Customer agrees to subscribe to such notifications where available. At least ten (10) days before enabling any third party other than existing authorized Sub-Processors to access or participate in the processing of Personal Data, Impartner will add such third party to the List and notify Customer via email. Customer may object to such an engagement by informing Impartner within ten (10) days of receipt of the aforementioned notice by Customer, provided such objection is in writing and based on reasonable grounds relating to data protection. Customer acknowledges that certain sub-processors are essential to providing the Services and that objecting to the use of a sub-processor may prevent Impartner from offering the Services to Customer.

   7.2 If Customer reasonably objects to an engagement in accordance with Section 7.1, and Impartner cannot provide a commercially reasonable alternative within a reasonable period of time, Customer may discontinue the use of the affected Service by providing written notice to Impartner. Discontinuation shall not relieve Customer of any fees owed to Impartner under the Agreement.

   7.3 If Customer does not object to the engagement of a third party in accordance with Section 7.1 within ten (10) days of notice by Impartner, that third party will be deemed an authorized Sub-Processor for the purposes of this Addendum.

   7.4 Impartner will enter into a written agreement with the authorized Sub-Processor imposing on the Authorized Sub-Processor data protection obligations comparable to those imposed on Impartner under this Addendum with respect to the protection of Personal Data. In case an authorized Sub-Processor fails to fulfill its data protection obligations under such written agreement with Impartner, Impartner will remain liable to Customer for the performance of the authorized Sub-Processor's obligations under such agreement.

   7.5 If Customer and Impartner have entered into Standard Contractual Clauses, (i) the above authorizations will constitute Customer's prior written consent to the subcontracting by Impartner of the processing of Personal Data if such consent is required under the Standard Contractual Clauses, and (ii) the parties agree that the copies of the agreements with Authorized Sub-Processors that must be provided by Impartner to Customer pursuant to Clause 5(j) of the UK SCCs or Clause 9(c) of the EU SCCs may have commercial information, or information unrelated to the Standard Contractual Clauses or their equivalent, removed by Impartner beforehand, and that such copies will be provided by Impartner only upon request by Customer.

8. *Cooperation and Data Subjects' rights*. Impartner shall provide all reasonable and timely assistance (including by appropriate technical and organizational measures) to Customer to enable Customer to respond to: (i) any request from a Data Subject to exercise any of its rights under Applicable Data Protection Law (including its rights of access, correction, objection, erasure and data portability, as applicable); and (ii) any other correspondence, inquiry or complaint received from a Data Subject, regulator or other third party in connection with the Processing of the Data. In the event that any such request, correspondence, inquiry or complaint is made directly to Impartner, Impartner shall promptly inform Customer. To the extent legally permitted, Customer shall be responsible for any costs arising from Impartner's provision of the assistance described in this paragraph. Communications pertaining to the foregoing shall be sent to dataprocessing@impartner.com.

9. *Data Protection Impact Assessment*. If Impartner believes or becomes aware that its Processing of the Data is likely to result in a high risk to the data protection rights and freedoms of Data Subjects, it shall promptly inform Customer and provide Customer with all such reasonable and timely assistance as Customer may require in order to conduct a data protection impactassessment and, if necessary, consult with its relevant

data protection authority.

10. *Security incidents*. Upon becoming aware of a Security Incident, Impartner shall inform Customer without undue delay after becoming aware of the Security Incident, and shall provide all such timely information and cooperation as Customer may require in order for Customer to fulfil its data breach reporting obligations under (and in accordance with the timescales required by) Applicable Data Protection Law. Impartner shall further take all such measures and actions as are necessary to remedy or mitigate the effects of the Security Incident and shall keep Customer apprised of all developments in connection withthe Security Incident.

11. *Deletion or return of Data*. Upon termination or expiry of the Agreement, Impartner shall (at Customer's election) destroy or return to Customer all Data (including all copies of the Data) in its possession or control (including any Data subcontracted to athird party for Processing). This requirement shall not apply to the extent that Impartner is required by any EU (or any EU Member State) law to retain some or all of the Data.

12. *Audit*. Impartner will submit to audits and inspections in relation to the Processing of Data, at Customer's sole cost and expense, and will provide Customer with whatever information it needs to ensure that they are both meeting their obligations under Article 28 of GDPR. Customer agrees that its requests to audit Impartner may be satisfied by Impartner presenting up- to-date attestations, reports or extracts from independent bodies, including without limitation external or internal auditors, Impartner's data protection officer, data protection or quality auditors or other mutually agreed to third parties) or certification bya regulatory body by way of an IT security or data protection audit. Customer shall not exercise its audit rights under this DPA more than once per year, and no such audit may be exercised in a manner that (i) disrupts Impartner's normal business operations, or (ii) causes Impartner to breach any obligation of confidentiality to another customer or to any other third party, whether imposed by regulation or contract.

13. *Sub-processor Audits*. Customer may not audit Impartner's sub-processors without Impartner's and Impartner's sub- processor's prior agreement. Customer agrees that its requests to audit sub-processors may be satisfied by Impartner or Impartner's sub-processors presenting up-to-date attestations, reports or extracts from independent bodies, including without limitation external or internal auditors, Impartner's data protection officer, the IT security department, data protection or quality auditors or other mutually agreed to third parties) or certification by way of an IT security or data protection audit. Onsite audits at sub-processors premises may be performed by Impartner or a mutually agreed to auditor under a confidentiality agreement acting on behalf of Customer.

14. *Limitation of Liability*. Each party's liability arising out of or related to this DPA, whether in contract, tort or under any other theory of liability, is subject to the 'Limitation of Liability' section of the Agreement.

15. *Processing for Statistical Purposes*. Impartner may Process Data for statistical purposes following the termination or expiration of the Agreement. Any such Processing shall be subject to appropriate safeguards, as provided in Article 89 of the GDPR, for the rights and freedoms of the Data Subject. Those safeguards will ensure that technical and organizational measures are inplace in particular in order to ensure respect for the principal of data minimization. Those measures may include pseudonymization or that the Processing does not permit the identification of Data Subjects.

16. *Miscellaneous:*

    a. Headings. Headings in this DPA are for convenience of reference only and will not constitute a part of or otherwiseaffect the meaning or interpretation of this DPA.

    b. Entire Agreement. This DPA (including all schedules and appendices thereto) and the Agreement constitute the entire agreement between the parties relating to the subject matter of this DPA and supersede all prior agreements, understandings, negotiations and discussions of the parties in relation to the subject matter of this DPA.

    c. Severability. The provisions of this DPA are severable. If any phrase, clause or provision is invalid or unenforceablein whole or in part, such invalidity or unenforceability will affect only such phrase, clause or provision, and the rest ofthis DPA will remain in full force and effect.

    d. Notices. Any notice or other communication under this DPA given by either party to the other will be

deemed to be properly given if given in writing and delivered (i) in person, (ii) by electronic mail to the email addresses agreed to between the parties, or (iii) in accordance with the Notice provision of the Agreement. Either party may from time totime change its address for notices under this Section by giving the other party notice of the change in accordance with this Section.

e. Third-party Rights. The provisions of this DPA will endure to the benefit of and will be binding upon the parties andtheir respective successors and assigns.

f. Counterparts. This DPA may be executed in counterparts, each of which will be deemed an original, but all of whichtogether will constitute one and the same instrument. Execution of an Agreement incorporating the terms of this DPA shall be deemed to be execution of this DPA including all attachments.

g. Governing Law. This Addendum will be governed by and construed in accordance with the governing law of the Agreement, without regard to its conflict of laws principles, except to the extent that Applicable Data Protection Law(s) require otherwise, in which event this DPA will be governed in accordance with Applicable Data ProtectionLaw.

h. Signatures. This DPA has been signed on behalf of each of the parties by a duly authorized signatory.

[Remainder of Page Intentionally Blank]

Data Controller and Impartner have caused this Agreement to be executed by their duly authorized representatives as of the Effective Date.

For Data Processor (Impartner, Inc.):		**For Data Controller:**	
Signature:	_____	Signature:	_____
Name (Print):	_____	Name (Print):	_____
Title:	_____	Title:	_____
Signature Date:	_____	Signature Date:	_____

[Remainder of Page Intentionally Blank]

ANNEX 1: DETAILS OF PROCESSING OF PERSONAL DATA

A. LIST OF PARTIES

1. Data exporter(s):

Name: Party identified as Customer in the DPA

Address: The address listed on page 1 of the Order Form

Contact Person's name, position and contact details: Listed on page 1 of the Order Form

Activities relevant to the data transferred under EU/UK SCCs: Primary business point of contact for relationship with Data Importer.

Signature and date: Reflected in DPA

Role (controller/processor): Controller

2. Data importer:

Name: Impartner, Inc.

Address: 10619 South Jordan Gateway Suite 200, South Jordan, UT 84095

Contact Person's name, position and contact details: Zachary R. Burd, Senior Director, Legal and Business Affairs, dataprocessing@impartner.com

Activities relevant to the data transferred under EU/UK SCCs: Responsible for Data Importer's data privacy program

Signature and date: Reflected in DPA

Role (controller/processor): Processor

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose Personal Data is transferred:

Customer may provide Impartner, or allow Impartner access to, Personal Data associated with the following categories of Data Subjects:

- Employees, agents, advisors, subcontractors or contact persons of Customer;
- Customer's clients, channel partners, prospects, business partners, and vendors (who are natural persons);
- Other authorized users of the Services.

Categories of Personal Data transferred:

The personal data transferred concern the following categories of data:

- Personal details, names, user names, passwords, email addresses of users
- Personal data within emails which identifies or may be reasonably linked or linkable to an individual
- Data Subjects' metadata including sent, to, from, date, time, subject which may be considered Personal Data
- File attachments sent by Data Exporter or Data Exporter's partners which may contain Personal Data

- Personal Data sent by users of their own accord in free text fields or in files uploaded
- Personal Data Information offered by users as part of support enquiries
- Technical operational data including without limitation IP addresses, logins, search queries; which may include Personal Data
- Other data added by Controller from time to time

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 specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

Data Exporter agrees that it will not disclose any special categories of Personal Data or Personal Data classified as "sensitive" (or similar classification) to Data Importer.

The frequency of the transfer

Data Exporter transfers Personal Data as often as necessary to adequately provide Services outlined in the Agreement. This may involve transfers in multiple instances, e.g., to update recipient lists at which Services are aimed.

Nature and purpose of the processing

Data Importer is engaged to provide the Services to Data Exporter which involve the Processing of Personal Data. The scope of the Services is set out in the Agreement, and the Personal Data will be Processed by Data Importer to deliver those Services and to comply with the terms of the Agreement and this DPA.

The period for which the personal data will be retained

The Personal Data will be retained per the requirements of the Subscription Agreement and this DPA, and shall be as long as necessary to perform the Services.

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

Subject matter and nature of transfers to sub-processors are outlined in Annex 3 of the DPA, for each relevant sub-processor. Duration of transfers is same as the duration of transfers to the Data Importer.

C. COMPETENT SUPERVISORY AUTHORITY

For purposes of the EU SCCs, the competent supervisory authority is the Dutch Data Protection Authority, unless expressly agreed otherwise in the DPA.

[Remainder of Page Intentionally Blank]

ANNEX 2

Technical and Organizational Measures Including
Technical and Organizational Measures to Ensure the Security of the Data

This Annex 2 ("**Annex**") forms part of the DPA and EU/UK SCCs and must be completed by the parties.

The below includes description of the technical and organizational security measures implemented by the Data Importer in accordance with UK SCCs Clauses 4(d) and 5(c) (or document/legislation attached):

Overview
This document serves as an overall listing of the controls in place at Impartner to maintain the security of our office and data. Impartner follows the COSO framework for organizational controls. These controls are always in force and audited for compliance at least annually by a certified public accounting firm. They form the backbone of our SOC 2 processes.

Management

Impartner management is ultimately responsible for overseeing these controls. On a semi-annual basis each control owner is required to review the controls under their jurisdiction. Management observes the controls in action over the course of the year to ensure functionality and to recommend changes where needed.

Definitions

- **Company** – Company is defined as Impartner, Inc.
- **Customer** – Customer is defined as the customer indicated on page 1 of the order form to which this Annex 2 attaches.

Integrity and ethical values

Control Description
The Company's views on personal and corporate integrity and ethical values, along with guidelines for employee conduct are contained within the Code of Conduct. The Code of Conduct provides a framework for how employees conduct business and perform their duties.
The Company maintains a Contractor Agreement, which outlines the Company's associated standards of conduct. Third-party contractors working on behalf of the Company are required to read, accept, and abide by the Agreement before commencing work.
Background checks are performed on all new employees using a third-party service. The results are reviewed by HR for appropriateness and appropriate action is taken, as deemed necessary.
According to the Code of Conduct, Company personnel witnessing any improper behavior should report such incidents promptly to management and/or HR.
On an annual basis, all relevant employees are subject to a formal performance review to assess the employee's performance in their current roles and to identify opportunities for growth and job performance improvement.
The Code of Conduct reiterates that employees who violate company policies are subject to appropriate disciplinary action up to and including termination.

Board oversite and development of controls

Control Description
The Company is managed by a Board comprised of key investors who are independent of day-to-day management of the Company and the founders/executives. The Board is governed by a charter, meets in executive session on a quarterly basis, and retains full and free access to officers, employees, and the books and records of the Company. The Board and its committees have authority to hire independent legal, financial, or other advisors as deemed necessary or appropriate in the discharge of their duties, including oversight of the development and performance of internal control.
Quarterly, the Board meets with members of executive management to discuss operational and financial results and significant matters, risks, and issues facing the Company.

Management reporting lines & responsibility over objectives

Control Description
HR maintains formal organizational charts to clearly identify positions of authority and the lines of communication and escalation.
Employee duties and responsibilities are defined and communicated through job descriptions and policies and procedures. Job descriptions exist for common positions and are periodically reviewed by HR and management for accuracy and updated as needed.
The Company maintains an internal control policy which outlines management's responsibility regarding internal controls, frameworks, audit observations (from internal and external sources), and remediation of findings. The policy is reviewed and approved by the Audit and Risk Committee on an annual basis.
The responsibility and accountability for designing, developing, implementing, operating, maintaining, monitoring, and approving relevant system controls is assigned to appropriate personnel with authority to perform their related duties.
The Company maintains a third-party (vendor) risk management policy, which outlines the policies, procedures, and responsibilities associated with onboarding new vendors and monitoring existing vendors who will have access to Company's Customers' personal information, including their implementation and execution of applicable internal controls. The policy is reviewed and approved by a member of InfoSec on an annual basis.
On a periodic basis, control owners sign an acknowledgement form, certifying that they have read applicable SOC control descriptions and, as needed, narratives, and understand their related process and control responsibilities. Desired updates, if any, are communicated to applicable internal and external (auditors) personnel to update appropriate documentation.

Employee recruitment, retention, and training

Control Description
Internal policy and procedure documents relating to security and availability are maintained and made available on the Company's box.com site. The policies are reviewed and approved by a member of IT management on an annual basis.
The Company maintains policies related to computer usage and security awareness, which reflect its commitment to provide training to its employees on guarding against, detecting, and reporting malicious software that poses a risk to the Company's information systems. In accordance with the policies and the annual security awareness training, Company personnel are trained on appropriate computer usage and security awareness. Company personnel are instructed to notify IT immediately of any abnormal system behavior or suspicion of a threat.
Job requirements are documented in formal job descriptions. Prior to fulfilling positions within the Company, management evaluates a candidate's abilities and background (experience, education, training, etc.) to meet the requirements of the position.
IT provides company-wide security awareness training to all new employees upon hire, and to all company personnel at least once per calendar year, to help employees understand their obligations and responsibilities to comply with the Company's security and confidentiality policies and procedures, including the identification and reporting of incidents.
The Company provides on-the-job training and/or external training of new hires and/or existing employees, as deemed necessary, to empower them with the skills needed to carry out job responsibilities, as they relate to security and availability.
As part of its ongoing efforts in business planning, budgeting, and risk assessments, senior management evaluates the need for additional tools and resources in order to achieve its business objectives.

Before the Company engages or otherwise works with relevant vendors/third parties (e.g., colocation facilities), the Company requests and reviews relevant supporting documentation and information (e.g. business licenses, entity standing, industry standard assurance/attestation reports, inquiries, completed questionnaires) before engaging in a business relationship. Entities found to be lacking in or non-compliant with relevant commitments and requirements (e.g., security, availability) and other relevant policies and procedures are refused.
Formal agreements are in place with relevant vendors and third parties. The agreements establish, as applicable, the commitments and requirements of the vendor or partner, such as the scope of services and product specifications, roles and responsibilities, compliance and control requirements (e.g., security, availability), and service level expectations. These agreements require the vendors to notify Company personnel should a security incident occur involving PRM data and/or services.
The Company evaluates relevant service providers (e.g., colocation facility, cloud providers) annually in accordance with its vendor management process. Relevant supporting documentation and information (e.g. industry standard assurance/attestation reports (e.g., SOC 2), inquiries, completed questionnaires) are obtained and assessed to (a) re-evaluate the services provided and identify any new risks arising from the relationship, b) evaluate the appropriateness and effectiveness of relevant vendor controls and the impact of control exceptions, if known, and c) validate the Company is adhering to relevant complementary user-entity control considerations, if any. Results of the evaluations are included in threat/risk analysis discussions for planning and possible mitigation, where deemed necessary.

Generation & use of quality information

Control Description
The Company has a dedicated technology support team, consisting of development, IT, and Quality Assurance personnel, which is focused on maintaining the quality of internal information systems.
In support of Company initiatives (e.g., SOC), the Company has designed, documented, and implemented IT General Controls (change management; logical and physical access and security; and computer operations) over its relevant information systems to support automated control activities and the quality of information captured, generated, processed, and/or stored therein.
The Company maintains a master list of all relevant spreadsheets and system-generated reports/information from internal and external sources used in support of the performance of internal control (IT-dependent manual controls) related to the PRM Application System. The master list is updated as needed, but formally reviewed by applicable department management on an annual basis to ensure completeness and accuracy. On the list, management also specifies how it obtains reasonable assurance that the information being used is sufficiently reliable (e.g., completeness, accuracy, level of detail, change-control) for its intended purpose.

Internal communication of objectives & responsibilities

Control Description
The Company maintains an information security incident management policy. The policy defines the protocols for identifying, reporting, investigating, responding to, mitigating, communicating, and documenting suspected or known security incidents and is made available to relevant internal users in the Company's Box.com site.
The Company maintains documentation of system and service descriptions outlining relevant aspects of the design and operation of the system, its boundaries, and components. Documentation is available to relevant internal and/or external users through PRM support pages, the Company's box.com site, master IT system asset listings, and system/network diagrams.
Changes that may affect the Company's security and/or availability commitments and requirements and/or the related responsibilities of internal or external users are communicated directly to the relevant users (via means such as PRM messages, support pages, and user guides; broadcast emails; direct outreach by Project Managers; department meetings; and/or educational events).

For user story requests, authorization is given by the Product Owner or management to ensure they meet user needs and the PRM design vision. For reported bugs, authorization occurs once the bugs are verified by internal personnel or automation processes.

External communication of internal controls

Control Description
The Company communicates its security and availability commitments regarding the system to external users via the Subscription Agreement (Terms of Use) and Privacy Policy, which are posted on the Company's website.
External user roles and responsibilities are communicated via several mediums, including the Subscription Agreement (Terms of Use) and Privacy Policy, which are posted on the Company's website.
Support contact information is readily available to Customer through the Company's website and other Company-provided documentation (e.g., training documentation, Subscription Agreement (Terms of Use)). Customers and/or associated users are encouraged to contact appropriate Company personnel if they become aware of items such as operational or security failures, incidents, system problems, concerns, or other complaints.

Identification and assessment of risks

Control Description
The Executive Team maintains a strategic plan, which includes department objectives and goals for the coming year. Consideration is given to operational, reporting (external financial, external non-financial, and internal), and compliance objectives. At least quarterly, the Executive Team meets to monitor progress against the Company objectives/goals and to discuss specific business developments, department results, and various risks and opportunities facing the Company.
Management communicates business objectives and goals to all team members through various means, including quarterly Company-wide meetings, Company-wide emails, and other messaging systems, as appropriate.
The Company has established a Security Council, consisting of members of the IT Operations, Development, Dev/Ops, and Security teams. The Security Council meets regularly to evaluate whether the Company's security initiatives are aligned with operational risks, objectives, and goals.

Risk analysis and management

Control Description
The Company maintains master lists of IT system components (e.g., servers, software, network devices) supporting PRM. The lists are reviewed and updated as needed, but at least annually, for completeness and accuracy.
At least annually, the Company performs a formal risk assessment, which includes the identification of relevant internal and external threats (including those arising from Customer and the use of vendors/third parties) to system components, an analysis of the risks associated with the identified threats, the determination of appropriate risk mitigation strategies (including procedures over assessing and monitoring vendors/third parties), and the development or modification and deployment of controls consistent with the risk mitigation strategy.

Fraud assessment

Control Description
As part of the Company's formal risk assessment, management identifies fraud risks and assesses the likelihood of occurrence and potential impact on the Company's operational, reporting, and compliance objectives.

Identification of changes that impact the system

Control Description
Several mediums, such as the formal risk assessment process, quarterly Board of Directors meetings, weekly Executive management team meetings, industry (including security) news feeds/resources, and Customer security questionnaires (in RFPs), assist Company personnel in identifying relevant changes (e.g., environmental, regulatory, technology) that could impact business objectives; commitments and requirements to security and availability; and internal and external operations. In response to relevant changes, the risk assessment and related mitigation strategies are updated where deemed necessary.

Evaluation of the effectiveness of controls

Control Description
As part of the risk assessment and mitigation processes, the Company identifies, designs, develops, and implements key controls where deemed necessary. The Company uses several mediums, including Customer feedback, application / system security and performance monitoring, and internal performance reviews, to monitor the overall effectiveness of its underlying control environment. Identified discrepancies are appropriately investigated and, where needed, resolved. The resolution of such discrepancies may include updating the risk assessment and related mitigation strategies.
The Company employs host and network-based intrusion detection/intrusion prevention (IDS/IPS) systems and logging and monitoring software to a) collect data from PRM application and supporting infrastructure components (e.g., servers, databases, network devices) and endpoint systems, b) monitor the related systems for security and operational matters (e.g., latency, throughput, uptime, utilization), and c) detect unusual system activity. Based on configured events, the software systems automatically generate email, console, and/or MS Teams alerts to IT support personnel for further investigation and, if needed, resolution.
On an annual basis, IT personnel review production servers and network devices to ensure relevant configuration settings are maintained in accordance with the current hardening policy and procedure document and out-of-compliance configurations are appropriately corrected.
Quarterly vulnerability scans and annual third-party penetration tests are performed on Impartner’s core applications to identify vulnerabilities and variances from Company standards. Results are evaluated by appropriate personnel and remediation actions are performed, where deemed appropriate.

Internal communication of control deficiencies

Control Description
The Company uses a Third-party service to actively forward relevant system alerts to on-call personnel. At any given time, there are three individuals on call: a primary contact, a backup contact, and an escalation contact. The on-call rotation includes at least one member of the Operations team at all times.

Protection of information assets

Control Description
The Company maintains a Hardening Policy, which establishes internal standards for asset hardening and configuration (e.g., access and service restrictions, logging and monitoring mechanisms (including host-based agents), patching). The Policy is reviewed and approved by a member of IT management on an annual basis.
Firewalls are implemented at external points of connectivity and network segment boundaries (DMZ, internal) and are configured (e.g., access control lists, rules) to protect against unauthorized external access. Firewall rules are restrictive by default, and are configured to restrict connectivity and data flow to pre-approved network destinations and ports.

Traffic flowing to PRM also passes through a web application firewall designed to inspect traffic for malicious content and mitigate or prevent denial-of-service attacks.
Customers do not have direct access to the PRM database. Customers authenticate to PRM which connects to the production database via a restricted private connection.
A unique user ID and password are required to access PRM. PRM provides Customers the ability to set their own password policies within PRM, including Expiration, History, Minimum Length, Complexity, Login attempts and Lockout duration.
In order to remotely access relevant production network devices and PRM systems (web, database, and support services servers; and the database), users must pass through several layers of authentication. First, users must connect to the corporate network through a local physical connection, corporate WiFi via LDAP authentication, or VPN via a username and two factors of authentication. Next, users authenticate at the system or device layer using a separate username and password. Password parameters are configured according to the Company's password policy and include, where system functionality permits, settings such as minimum length, complexity, expiration, history, and lockout.
Internal user account passwords for PRM web, database, and support services servers are stored in an encrypted hash.
Customers' PRM account passwords are hashed and salted in accordance with industry standards.
External access to PRM is restricted through the use of user authentication and a minimum of TLS encryption. TLS is used during Customer logins and throughout Customer sessions, providing encryption of data transmissions between Customer browsers and PRM application servers. In addition, VPN, TLS, SSH, and/or other encryption-based technologies are required for communications between other remotely accessible endpoints and the systems and users connecting to them.
The Company uses a combination of private circuit technologies (IPsec and a private leased layer 2 connection) in order to protect data transmitted between its facilities (corporate office, colocation facilities).
The PRM database is encrypted at rest using full-disk encryption.
Database and file backups are encrypted at rest and access to the backups is restricted to appropriate IT personnel.
PRM supports the use of role-based security, allowing Customer account administrators the capability to assign pre-defined access levels (roles) and associated permissions to applicable users, based on job functions.
Administrative access to the production network domain, network devices, PRM super user functionality, and PRM supporting systems (web, database, and support services servers; database; SparkPost; and cloud storage) is restricted via logical access rights to appropriate IT administrators / support personnel and required system accounts. Access is granted on a minimum necessary basis in order for Company personnel to effectively carry out job functions and responsibilities.
Company access to view or manage Customer instances of PRM is restricted via logical access rights to appropriate support personnel.

Control of access to the system and supporting services

Control Description
Requests for new or modified access to the production network domain, network devices, PRM super user functionality, and PRM supporting systems (web, database, and support services servers; the database; SparkPost; and cloud storage) are approved by an appropriate supervisor before access is granted. System administrators provision access rights that are in accordance with the request and/or are commensurate with the user's job responsibilities.

As part of the onboarding process for PRM, an administrator account is created for the Customer's primary contact, enabling him/her to manage all Customer user accounts going forward. In order to log in, the user must change the initial password, thus preventing Company personnel from using that password to access the Customer's application instance.
The Privacy Policy, which is posted on the Company's website, instructs external users to maintain the secrecy of their PRM passwords and account information. Additionally, account sharing of end-user-based accounts on internal systems is prohibited (unless exempted by management) by internal policies. The policies also state that violators may be subject to appropriate disciplinary action
In accordance with the Company's Hardening Policy, only system/service accounts that serve a valid business purpose are enabled on production servers, databases, and network devices, and default (built-in) passwords have been changed where applicable.
HR personnel notify IT system administrators of employee terminations. Upon notification, system administrators proceed to disable/delete the employee's access to applicable systems, including the production network domain, network devices, PRM super user functionality, and PRM supporting systems (web, database, and support services servers; the database; SparkPost; and cloud storage). A checklist listing relevant Company systems is utilized in the process to ensure that access rights are checked and, where applicable, disabled/deleted.
Passwords to sensitive built-in administrator and other master-level accounts are changed in a timely manner when an employee with knowledge of them departs or changes roles and no longer needs such access. A checklist listing all relevant systems, utilities, and colocation facilities is utilized in the process to ensure all accounts are appropriately updated.
All production network domain accounts that are inactive for 90 days are automatically disabled. If the accounts are still inactive after 180 days, notification is sent to IT management for review.
On an annual basis, a user account audit of the production network domain, network devices, PRM super users, and PRM supporting systems (web, database, and support services servers; the database; SparkPost; and cloud storage) is performed by a member of IT management to validate the ongoing appropriateness of all internal accounts and related access levels.

Physical access

Control Description
All new requests for access to the colocation facilities must be approved by a member of IT senior management.
Upon notification of an applicable employee termination, the Sr. Director of IT or other authorized Company account administrator updates the master access list at the colocation facilities to disable the employees associated physical access rights.
On a semi-annual basis, the list of personnel with physical access rights to the colocation facilities are reviewed by a member of IT senior management to validate the ongoing appropriateness of access.

Asset management

Control Description
The Information Security team maintains an End of Life Policy, which outlines the policies governing the disposition of obsolete or unwanted IT assets and any accompanying software and data stored therein.
IT maintains a master list of relevant IT hardware assets. As IT assets containing sensitive software and/or data are deemed end-of-life and ready for sale or disposal, the storage media is removed and securely wiped. The master list is updated to reflect the actions taken on disposed assets.

Logical access

Control Description
The Sr. Director of IT reviews configured firewall rules on a semi-annual basis for appropriateness and adherence to Company standards. Requests for changes, if any, are documented and submitted to appropriate network personnel for implementation.

Data movement

Control Description
The Company maintains policies relating to data transmission and storage, which prohibit the transmission of sensitive information over the Internet or other public communication paths (for example, e-mail), unless it is encrypted. In addition, these policies prohibit the storage of Customer information on removable media, mobile devices, or other unencrypted end-user storage media.

Unauthorized or malicious software

Control Description
Endpoint security software has been implemented to assist Company personnel in preventing, detecting, and analyzing security-related events, including the introduction of potentially malicious software, on end-user systems and production servers. Endpoints are configured to receive updated threat and virus signatures from the vendor continuously. The software sends a consolidated report to IT at least daily outlining threats detected on relevant endpoints, action taken, etc. Relevant issues are appropriately investigated and, if needed, resolved.

Patch management

Control Description
The Company maintains a patch management policy, which establishes internal standards for identifying, evaluating, and implementing patches to remediate relevant vulnerabilities. The policy is reviewed and approved by the Sr. Director of IT on an annual basis.
IT monitors the availability of patches to network devices and PRM supporting systems (web, database, and support services servers) on a daily basis. Relevant patches are applied in a timely manner, in a phased approach starting with non-production network devices and servers to assess the potential for service disruptions before application to the production servers.

Incident management

Control Description
For security events deemed to be an "incident," as defined in the Incident Response Policy, the Security Incident Response Team is activated and executes the incident response program, which includes analysis, containment, eradication, recovery, communication to affected parties (internal and external), and post-incident activity, as appropriate. Details of key information gathered and actions performed relating to the incident and associated response are documented in an Incident ticket.
The Company’s IT team performs periodic tabletop incident response simulations to test the Company’s Security Incident Response Plan, taking into account the threat, likelihood, magnitude, business impact analysis, availability, etc. The Security Incident Response Plan and related policies / processes / systems are revised, as needed, based on the test results.
At least annually, the Company tests its ability to failover PRM to the disaster recover colocation facility.

Change management

Control Description
The Company maintains a formal application change management policy, which outlines considerations for planning, design, testing, implementation, and maintenance of changes.
For each change, automated application regression tests are performed to identify common issues.
Application-related changes are appropriately tested by Quality Assurance (QA) personnel prior to implementation in production.
Changes are approved by appropriate personnel, as defined in the application change management policy, prior to implementation in production.
For PRM and its related database, separate development, test, and production environments exist in support of the Company's application change management process.
PRM changes are deployed to production servers by appropriate personnel, who are separate from the development function.
PRM code can be rolled back as needed during and after deployment.
The Company maintains a formal infrastructure change management policy, which defines the relevant types of changes that can be made to the Company's infrastructure and sets forth the procedures for the associated testing, approval, and documentation. The policy is reviewed and approved on an annual basis by a member of IT for ongoing appropriateness.
During the ongoing risk assessment processes and the periodic planning and budgeting processes, infrastructure, data, software, and procedures are evaluated for needed changes. Change requests are created where appropriate.
When relevant system deficiencies are identified, change requests are generated, analyzed, prioritized, assigned, authorized, tested, approved, and implemented in accordance with the Company’s change management procedures.

Risk mitigation

Control Description
The Company maintains a Disaster Recovery policy, which outlines tasks and procedures to be executed for disaster recovery, to minimize the amount of downtime caused by a disaster.
The Company maintains a formal Backup Policy, which is reviewed and approved by the Sr. Director of IT on an annual basis.
PRM production runs in a redundant environment with clusters of servers, enabling load balancing and continued operation in the event of a logical or hardware failure of any given server.
The Company currently contracts with Flexential, utilizing two geographically distinct colocation facilities. The Company mirrors production technology and functionality (e.g., software, systems, data) between the facilities to permit the resumption of PRM operations in the event of a disaster at the production facility.
On a daily basis, incremental and/or full backups of production network device configurations and PRM data and locally-stored Customer files are generated, stored locally to disk, and subsequently copied to tape. IT monitors the backup and copy processes for completion using log files and/or automated email alerts. Issues are appropriately investigated and, if needed, resolved.
PRM production databases and website content reside at the production Flexential colocation facility (in Las Vegas) or the Azure IaaS and are replicated, in real-time, to redundant hardware sets both locally and at either the disaster recovery Flexential colocation facility (in SLC), or multi-zone Azure IaaS facilities. Email alerts are automatically sent out by monitoring utilities in the event of a replication issue or noteworthy lag. Issues are appropriately investigated and, if needed, resolved by IT and/or database personnel.
The Company tests its ability to restore PRM database data quarterly, and Customer files semi-annually, from backup data.

The Company has established an Insurance Committee headed by the CFO which meets at least annually with a broker to review the insurance coverage of the business, taking into account risks that may threaten achievement of applicable Company objectives. The Insurance Committee makes appropriate changes to the insurance coverage, as deemed necessary.

Capacity management

Control Description
Monitoring software is used to track processing, storage, memory, and other system performance metrics and demands in PRM and compare them to historical trends on an ongoing basis. Based on pre-defined capacity thresholds, the software automatically generates email and logged alerts to IT support personnel for further investigation. Significant events (e.g., increasing trend in usage) are further discussed in the weekly Engineering meeting. Change requests are initiated as needed to maintain or improve the system.
The Company maintains a master list of PRM system components at its production and disaster recovery locations. The list includes information about hardware assignment and redundancy.

[Remainder of Page Intentionally Blank]

ANNEX 3

Vendor's Sub-Processors

Flexential: Located in Salt Lake City, Ut and Las Vegas, NV
Colocation services with no logical access to data
Partner portals are hosted at these sites

Azure: Located in US-West-2 availability zone (Portland OR)
Hosts main database and PRM admin portal with PRM microservices
No logical data access

Amazon Web Services (AWS):
US-West zone
Hosting microservices
No logical data access.

Auth0: Located in multiple AWS US zones
Provides Identity Provider services with logical access to usernames

Wasabi: Located in Azure US-west zone
Provides offsite backup data storage

Google Analytics:
Processes data at numerous Google data centers in the U.S.
Provides web analytics for Impartner's customers to analyze portal activity

New Relic:
Colocation services in Chicago, IL and Multiple AWS US zones
Provides aggregate performance metrics for Impartner engineers to identify and troubleshoot tech issues
No logical data access

Linode: Located in London, UK
Provides Internet as a Service (IaaS) for News on Demand and Social on Demand
no logical data access

Otava: Located in Ann Arbor, MI
Provides IaaS for Impartner Referral
no logical data access.

SolarWinds Papertrail:
Numerous data centers in the U.S.
Log aggregation and alerting to detect anomalies and debug technical issues

Vertical Response:
Located in San Francisco, CA
Provides email services for TCMA email marketing functionality
Has access to Partners' client lists provided by Partners either directly to Vertical Response or via Impartner

Mailgun Technologies Inc.,
Headquartered in San Antonio, TX; Configured to processes EU Data solely in the EU.
Provides email services for Impartner's News On Demand and Social On Demand products
Has access to Customer's partner lists if Customers utilize Impartner's News on Demand or Social On Demand products

[Remainder of Page Intentionally Blank]

ANNEX 4

Supplementary Safeguards

This Annex is integrated into the UK SCCs (hereinafter “Clauses”) by reference.

Pursuant to the Supplementary Safeguards Clause, parties to UK SCCs hereby warrant the following:

1. In the event that Data Importer receives a request from any law enforcement authority of a Third Country for disclosure of personal data processed under these Clauses in such Third Country, it will use every reasonable effort to redirect such authority to request data directly from the relevant Data Exporter.

2. In the event that Data Importer is served with legally binding requests by any law enforcement authority in Third Country for disclosure of personal data in such Third Country, it will notify the relevant Data Exporter without undue delay. Such notification shall include information available to Data Importer.

3. In the event that the Data Importer in Third Country becomes aware of any direct access by local public authorities regarding such personal data, it will notify the relevant Data Exporter without undue delay. Such notification shall include relevant information available to Data Importer.

4. If Data Importer is prohibited from notifying the relevant Data Exporter, it agrees to seek a waiver of the prohibition. Data importer agrees to document its efforts to seek such waiver in order to be able to demonstrate them upon reasonable request of Data Exporter.

5. In case of any legally binding request as referred to in point 2 above, Data Importer will review the legality of the request for disclosure under laws of the relevant Third Country, notably whether such request remains within the powers granted to the requesting public authority, and to exhaust available remedies to challenge the request if it concludes that there are grounds under such laws to do so. When challenging a request, Data Importer shall seek interim measures with a view to suspend the effects of the request until the court has decided on the merits. Data importer shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are notwithstanding the obligations of Data Importer under the Clauses.

6. In any case, Data Importer will provide the minimum amount of personal data permissible if responding to a request for disclosure, based on a reasonable interpretation of the request.

7. Data importer will immediately notify relevant Data Exporter if, after having committed to these supplementary safeguards, and for the duration of the Clauses, Data Importer has a reason to believe that it has become subject to new/amended Third Country laws or a change in national enforcement practices that do not allow Data Importer to meet its obligations under the Clauses.

8. Data importer has implemented appropriate technical and organisational measures to ensure compliance with the level of protection required under UK data protection laws in the context of a transfer of Personal Data to Third Countries under the Clauses to ensure a level of security appropriate to the risk, as outlined in Annex 2 to these Clauses.

9. Data importer further certifies that:

    a. it has not and for the duration of the Clauses will not purposefully create back doors or similar programming that could be used to access its system holding Personal Data processed under the Clauses, or purposefully create or change its business processes in a manner that facilitates undue access to such Personal Data or systems, and

    b. local laws of the relevant Third Country of the Data Importer do not require it to create or maintain such back doors or business processes as outlined in the provision immediately above

[Remainder of Page Intentionally Blank]