Exhibit A

Master Services Agreement

This Master Services Agreement ("**MSA**") is made between Impartner, Inc. ("**Impartner**") and the Customer identified on the Order Form ("**Customer**"). Impartner and Customer are referred to each as a **"Party"**, or collectively as the **"Parties"**. The Order Form and MSA, including any attachments or exhibits (**"Exhibits"**), which are hereby incorporated by reference, shall constitute the "**Agreement**" between the Parties. Capitalized terms not defined herein shall have the meaning assigned to them in the Order Form.

1. DEFINITIONS

"Affiliate" means any entity Controlling, Controlled by, or under common Control with a Party.

"**Control**" means direct or indirect ownership of more than fifty percent (50%) of the voting interests of an entity. An entity shall be deemed an Affiliate only for so long as such Control exists.

"**Appropriate Security Measures**" means commercially reasonable technical, physical, and procedural controls designed to (i) protect Customer Data against destruction, loss, alteration, unauthorized disclosure to third parties, and unauthorized access by employees or contractors employed by Impartner, and (ii) prevent the introduction of malicious code into the Licensed Services.

"Customer Data" means all electronic data, content, or information submitted by Portal Users to Impartner in connection with Impartner's provision of the Licensed Services or Support Services.

"DPA" means the data processing addendum attached hereto as Exhibit A, and is incorporated into the Agreement by reference herein.

"Documentation" means product descriptions found at https://impartner.com/packages-prm/, which may be updated from time to time by Impartner in its sole discretion. For clarity, as a SaaS provider with standard offerings, the Documentation is intended solely to provide objective criteria for the Parties to agree in advance what constitutes adequate delivery of the Licensed Services. Impartner's products and services may change over time as Impartner improves its products and services, and the Documentation is not intended to restrict Impartner from so improving its Licensed Services.

"Impartner Materials" means materials made available by Impartner to Customer via the Licensed Services, Support Services, or customer success portal, and includes, without limitation, how-to guides, training content, and FAQs.

"Implementation Services" means work performed by Impartner for initial installation and configuration of the Licensed Services in accordance with an Order Form.

"Licensed Services" means the online, cloud-based software applications, modules and associated content and materials (including Impartner Materials incorporated therein) provided by Impartner to Customer as set forth in an Order Form, as well as any updates, upgrades, improvements, enhancements, integrations or customizations which Impartner may develop and make available to Customer in its sole discretion, but excluding Third-Party Applications.

"Order Form" means the order form, order form amendment, or order form renewal signed by the Parties that sets forth the pricing, Services, Use Limits, applications and modules selected by Customer, along with any Support Services.

"Partners" means Customer's resellers, channel partners or other members of Customer's partner networks that provide services and/or sell products or services on behalf of Customer.

"Personal Information" has the meaning ascribed to it under the California Consumer Privacy Act of 2018 (the "**CCPA**"), and specifically includes "Personal Data," as defined by 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 (the "**GDPR**").

"Portal Users" means employees or agents of Customer or a Partner who are authorized to access and use the Licensed Services, and who have been supplied user identifications and login credentials by Customer (**"User Credentials"**).

"Premier Support" means additional support services that supplement the Standard Support Services, purchased on an annual basis, that may include a dedicated Technical Account Manager, as further described in an Order Form.

"Professional Services" means billable, professional services related to custom functionality, training after implementation, integration with or fixes related to use of the Licensed Services with Third-Party Applications, as outlined in an Order Form that delineates the specific scope of services.

"Standard Support Services" means Impartner's support ticketing and response system for the Licensed Services' standard product capabilities as further set forth in the service level agreement attached as Exhibit B (the **"Service Level Agreement"**). Standard Support Services are included as part of the Subscription Fees at no additional cost to Customer.

"Support Services" means all services offered to Customer other than the Licensed Services, and includes the Standard Support Services, Premiere Support, Implementation Services, and Professional Services.

"Third-Party Applications" means any services, software, products, applications, integrations and other features or offerings that are provided by Customer or obtained by Customer from a third party.

2. THE LICENSED SERVICES

2.1 Provision of the Licensed Services. Subject to Customer's compliance with the terms and conditions of the Agreement (including payment of the applicable Fees (as defined below)), Impartner shall make the Licensed Services available to Customer, Partners, and Portal Users for internal business purposes during the Term.

2.2 Affiliates. A Customer may enter into an Order Form on behalf of itself and its Affiliates, if expressly stated in the applicable Order, and subject to the following conditions: (i) Customer has the authority to enter into the Agrement on behalf of its Affiliates; (ii) Customer remains responsible for its Affiliates' compliance with the terms of the Agreement and any breach of the Agreement by a Customer Affiliate shall be deemed to be a breach by Customer; (iii) all use limits, as described in the Order Form, and other platform-related limitations of Customer arising from the Agreement shall be applied in the aggregate across Customer and all Customer Affiliates. Notwithstanding the foregoing, Customer is solely entitled to a single instance of the Licensed Services, unless expressly set forth in an Order Form. If additional instances are required, for any reason, including for an Affiliate to have unique functionality independent from the Customer's instance, additional implementation and/or subscription fees will apply, or the Affiliate may be required to enter into a separate Order Form.

2.3 Licensed Services Requirements. Impartner may make changes (including updates, updates, or other improvements) to the Licensed Services, on the condition that such changes do not materially diminish the features or functionality of the Licensed Services or the commitments set forth in the Service Level Agreement. Customer acknowledges, however, that its purchase of the Licensed Services is for the current version of the Licensed Services, and not contingent on the delivery of any future functionality or features, nor dependent on any oral or written comments made by Impartner or its personnel regarding future functionality or features.

2.4 Third-Party Applications. Impartner does not offer licenses to any Third-Party Applications. Customer is responsible for obtaining its own licenses to Third-Party Applications, and Customer agrees to comply with the applicable terms and conditions. Impartner does not make any warranties with respect to any Third-Party Applications. Except for Impartner's obligations related to Google Ads for Channel (if applicable) Customer maintains all obligations related to the implementation, customization, and exchange of data between Customer and any Third-Party Applications.

Third Party Applications may offer Customer the ability to share Customer Data with Third-Party Applications (for example, through a marketplace, via application program interfaces (each an "**API**," or collectively, "**APIs**"), or otherwise). In the event Customer utilizes Third Party Applications to access or process Customer Data, Customer assumes all risk and liability with such access and processing. Impartner is not responsible for any disclosure, modification or deletion of Customer Data resulting from access by such Third Party Applications. Impartner may treat any requests to access Customer Data by Third Party Applications as written instructions by Customer to access Customer Data, so long as such access requires authentication to Impartner's platform using Customer's login credentials to the Licensed Services.

2.5 Google Ads for Channel. This Section applies if Customer purchases Impartner's Google Ads for Channel. Impartner will create a Google Ads account to establish and run Partners' advertising campaigns ("**Campaigns**") on the Partners' behalf. Portal Users will not have access to Google Ads accounts that Impartner creates. All campaigns that run through Google Ads for Channel must comply with, and are subject to, the Google Ads Terms & Conditions. Impartner will not commence a Campaign until Impartner has received payment in full for that Campaign. Any fees paid for Google Ads ad campaigns will not count towards the limits of liability delineated in this Agreement.

2.6 Rewards Services

2.6.1 General. This Section titled Rewards Services applies solely if Customer is buying Ignite Pro, MDF, Payment Processing Engine, Payments Manager, or Referral Automation Programs (collectively, "**Rewards Services**.") Customer will be responsible for providing all necessary information required for Impartner to provide the Rewards Services, such as reward amount(s) ("**Rewards**"), reward recipient ("**Rewards Recipient**"), and method of calculating and issuing the Rewards ("**Calculation Method**"). Impartner will calculate the amount of the Rewards to be paid to each Rewards Recipient based upon the most recent Calculation Method provided by Customer. The minimum amount for any individual Rewards to be paid to a Rewards Recipient is one hundred dollars ($100). If Customer approves Rewards less than one hundred dollars ($100), Impartner may, in its sole discretion, charge Customer a per/transaction fee of twenty five dollars ($25). Rewards will only be issued to Rewards Recipients after Customer approves such Rewards within the Licensed Service. Impartner will only process approved Rewards once it receives the funds necessary to pay such Rewards. Any unused, prefunded Rewards will be returned to Customer within thirty (30) days of the termination or expiration of this Agreement. If Rewards are paid to Rewards Recipients in a currency other than the currency in which the funds are paid to Impartner, exchange rates will be calculated using the prevailing rate of the Payment Processor applicable at the time Rewards payments are made.

2.6.2 Payment Processors. Impartner may utilize the services of one or more third-party payments processors (each a "**Payment Processor**") to process Rewards payments. Impartner shall have no liability for the acts or omissions of third-party Payment Processors, including any rejected payments or payment delays. Impartner reserves the right to charge Customer for any transaction fees associated with wire investigations, insufficient funds, return payments, generation or mailing of end-of-year Form 1099s or other tax statements. For clarity, unless expressly agreed otherwise in writing, Impartner does not issue Form 1099s for Customer or Rewards Recipients.

2.6.3 Rewards Indemnification. Customer agrees to indemnify, defend, and hold Impartner and its Payment Processors harmless from and against all losses, damages, liabilities, costs, and expenses resulting from any claims or actions arising out of any actual or alleged violation of Customer's obligation to report taxes associated with the Rewards. This obligation shall not be subject to any limitation of liability set forth elsewhere in the Agreement.

2.6.4 Rewards Compliance with Law. Customer is solely responsible for determining if a Reward payment or designated Rewards Recipient receiving a Reward would violate any provision of any present or future risk control program of the Federal Reserve, Office of Foreign Assets Control (OFAC) policy, Presidential Order, Financial Industry Regulatory Authority (FINRA) policy, any anti-money laundering (AML), anti-terror regulations, other applicable law, or the rules of the NACHA, Electronic Check Clearing House Organization, card associations, clearinghouses, networks and/or other associations which regulate Rewards transactions.

3. PERMITTED USE OF THE LICENSED SERVICES

3.1 Use of Licensed Services. Customer shall: (i) not make the Licensed Services available to anyone other than those authorized under this Agreement; (ii) not use the Licensed Services in any manner that exceeds the scope of the applicable Order Form; (iii) use commercially reasonable efforts to prevent unauthorized access to or use of the Licensed Services; (iv) promptly notify Impartner of any unauthorized access or use of the Licensed Services, passwords, authentication credentials, or any unauthorized use, access, or disclosure of Customer Data; (v) comply, and cause its Portal Users to comply, with the Agreement, and be solely responsible for its Portal Users' compliance with this Agreement; (vi) be solely responsible for all Customer Data, including the reliability, accuracy, completeness, timeliness, legality, and appropriateness of the Customer Data; (vii) secure and maintain any consents or permissions required to use the Customer Data as required by applicable law; (viii) ensure that the Customer Data does not infringe the rights of any third party, and is not otherwise obscene, threatening, defamatory, racially or ethically offensive, libelous, fraudulent or otherwise unlawful or tortious; (ix) not use the Licensed Services to send or store known viruses, worms, time bombs, Trojan horses, and other harmful, destructive, deceptive or malicious code, files, scripts, agents or programs; and (x) comply with all local, state, federal and foreign laws applicable to Customer's use of the Licensed Services. Customer may not provide user login credentials to any individuals or entities other than Third Party Applications. In the event Customer shares its login credentials, and/or Customer Data with one or more Third Party Applications, Customer shall be responsible for all actions performed by the Third Party Applications, including API calls to share Customer Data with Third Party Applications, and any such API calls will be considered actions performed by Customer.

3.2 Restrictions. Customer shall not at any time, directly or indirectly, and shall not permit any Portal User to: (i) copy, modify or create derivative works based on the Licensed Services; (ii) rent, lease, lend, sell, license, sublicense, publish, frame, mirror or otherwise distribute any part of the Licensed Services; (iii) reverse engineer, disassemble, decompile, decode, adapt, or otherwise attempt to derive or gain access to the source code of the Licensed Services, in whole or in part; (iv) intentionally disable, interfere with, or disrupt the integrity or performance of the Licensed Services; or (v) access or use the Licensed Services in order to build (or assist others in building) a competitive product or service or in any manner beyond the scope of the authorization granted herein.

3.3 Two Factor Authentication. The Licensed Services support access using two-factor authentication ("**2FA**"), which is known to reduce the risk of unauthorized use of or access to the Licensed Services. Impartner strongly encourages Customer to use, and cause its Partners and Portal Users to use 2FA. Impartner disclaims all responsibility for any damages, losses or liability to Customer, Partners, Portal Users, or any other affected individuals, where such damages, losses, or liability could have been prevented by the use of 2FA.

3.4 Service Suspension. Notwithstanding anything to the contrary in the Agreement, Impartner may suspend Customer's and/or any Portal User's access to any portion or all of the Licensed Services if: (i) any charge owing by Customer is thirty (30) days or more overdue, until such amounts are paid in full; (ii) Impartner reasonably determines that: (A) Customer's or any Portal User's use of the Licensed Services disrupts or poses a security risk to Impartner or to any other customer or vendor of Impartner; or (B) Customer, or any Portal User, is using the Licensed Services in breach of the Agreement or in violation of applicable law; (iii) Customer ceases to do business in the ordinary course, becomes insolvent or unable to pay debts as they become due, makes an assignment for the benefit of creditors or similar disposition of its assets, or becomes the subject of any bankruptcy, reorganization, liquidation, dissolution, or similar proceeding (each, a "**Bankrupty Event**"); (iv) any vendor of Customer, or Google Ads (if Customer is buying Google Ads for Channel), has denied Impartner's access to, or use of, any Third-Party Applications needed to enable Customer's access to or use of the Licensed Services; or (v) Impartner's provision of the Licensed Services to Customer is or becomes prohibited by applicable law. Any suspension described in subclause (i)-(v) is a "**Service Suspension**." Impartner shall use commercially reasonable efforts to promptly provide written notice of any Service Suspension to Customer and to provide updates regarding resumption of access to the Licensed Services following any Service Suspension. Impartner shall use commercially reasonable efforts to resume providing access to the Licensed Services as soon as reasonably possible

after the event giving rise to the Service Suspension is cured. Impartner will have no liability for any damage, liabilities, losses (including any loss of data or profits) that Customer may incur as a result of a Service Suspension. Customer's sole remedy for any Service Suspension made pursuant to 3 shall be a *pro rata* refund of any pre-paid Fees.

4. SUPPORT SERVICES

4.1 General. All Support Services other than Standard Support must be listed in an Order Form.

4.2 Impartner's Obligations. Impartner shall perform Support Services in a professional and workmanlike manner. Impartner shall be entitled, in its sole discretion, to determine the method and means for performing the Support Services.

4.3 Customer Obligations. Customer acknowledges and agrees that timely performance and delivery of Support Services is dependent upon information and responses provided by Customer. Accordingly, in addition to any specific responsibilities set out in the Order Form, Customer shall: (i) provide the appropriate and necessary resources, and timely and accurate information and documentation, as reasonably requested by Impartner, to allow Impartner to perform the Support Services; (ii) timely review and respond to requests for approval and information; and (iii) make available personnel familiar with Customer's requirements and with the expertise necessary to permit Impartner to undertake and complete the Support Services. Customer acknowledges that any delay on its part in the performance of its obligations may have an impact on Impartner's performance of its activities under the Order Form, and Impartner shall not be liable for any delay to the extent caused by Customer's failure to fulfill any of its obligations under the Agreement or any Order Form.

4.4 Expenses. If applicable, Customer shall reimburse Impartner for all expenses that have been pre-approved in writing by Customer and incurred by Impartner in connection with Support Services, including, but not limited to, transportation expenses, meals, rental cars, lodging, and disbursements to third parties, such as third-party professional and programming service providers. Records of reimbursable expenses including statements and receipts shall be provided to Customer upon request.

5. FEES AND PAYMENT

5.1 Fees. Customer shall pay all fees specified in the applicable Order Form ("**Fees**"). Except as otherwise set forth herein or in an Order Form, Fees are quoted and payable in United States dollars. If Customer requires a Purchase Order to process an invoice, it is responsible for taking all necessary steps to ensure timely payments are made under this Agreement. Failure to make timely payment shall not be excused due to delays caused by Customer's Purchase Order process.

5.2 Payment Disputes. Customer may dispute part or the entirety of an invoice by: (i) providing written notice to Impartner of such dispute within ten (10) days of invoice receipt; (ii) providing a reasonably detailed description of the dispute, at least sufficient to allow Impartner to analyze the dispute, as part of the written notice; (iii) only submitting such dispute in good faith; (iv) paying all undisputed amounts when due; and (v) paying all disputed amounts promptly after resolution of such dispute. If any undisputed amounts invoiced pursuant to an Order Form are not received by Impartner by the due date, then such amounts shall accrue interest at the rate of 1.5% of the outstanding balance per month, or the maximum rate permitted by law, whichever is lower, from the date such payment was due until the date paid. Notwithstanding anything to the contrary in the Agreement, and without limiting any remedies available to Impartner, Customer shall be liable to Impartner for all reasonable expenses, including but not limited to collections and legal fees, associated with Impartner's efforts to collect on undisputed, overdue Fees. In addition, if Customer fails to make timely payment of undisputed, overdue Fees, in addition to any other remedies set forth in the Agreement, any payment terms which deviate from the following will automatically revert to: (i) Fees being due thirty (30) days from the invoice date, and (ii) Fees being invoiced annually in advance.

5.3 Taxes. Fees do not include any taxes, levies, duties, or similar governmental assessments of any nature, including, but not limited to, value-added, sales, use, or withholding taxes, assessable by any local, state, provincial, federal or foreign jurisdiction (collectively, "**Taxes**"). Customer is responsible for paying all Taxes associated with purchases under this Agreement, which shall be included as a separate line item on each invoice. If applicable, Customer will provide Impartner with a certificate of exemption or similar

documentation required to exempt any transaction under this Agreement from sales and use tax or other tax liability.

6. PROPRIETARY RIGHTS

6.1 Impartner Reservation of Rights. Impartner is and will remain the exclusive owner of all rights, title, and interest, in the Licensed Services, Documentation, and Support Services, any and all improvements or enhancements to the same, and all intellectual property rights embodied therein ("**Impartner Property**"). Unless expressly stated otherwise in an Order Form, all intellectual property rights in any work arising from or created, produced, developed, or delivered by Impartner, whether alone or jointly with others, in the course of this Agreement will immediately upon creation or performance, vest absolutely in and will be and remain the property of Impartner, and Customer will not acquire any right, title or interest therein, other than the rights and licenses granted under the Agreement. Except for the rights and licenses specified in the Agreement, all other rights are reserved by Impartner.

6.2 Feedback. Impartner encourages Customer to provide suggestions, proposals, ideas, recommendations, or other feedback regarding the Licensed Services, Support Services, and related resources ("**Feedback**"). Impartner shall own all right, title, and interest to all Feedback, including all intellectual property rights embodied therein. To the extent Customer provides Feedback, Customer agrees to assign, and hereby does assign to Impartner all worldwide right and title to the Feedback, including the right to sue for any past, present, or future infringement; provided that (i) this assignment does not grant rights under any issued patents owned by Customer; and (ii) the Feedback is provided "as is" without any warranties, whether express, implied, or statutory. Customer agrees to cooperate with Impartner and execute such documents (at Impartner's cost) as may be necessary for Imparter to register, record, enforce, or defend its rights in any Feedback.

6.3 Customer Data. As between the Parties, Customer owns all rights, title and interest in and to all Customer Data and all intellectual property rights embodied therein. Impartner may use Customer Data to provide the Licensed Services during the Term (as defined below) of the Agreement. To the extent Customer Data is combined with data derived or obtained from public sources, the portion of data derived or obtained from such public sources will not be considered Customer Data. Impartner may create and use Usage Data. "**Usage Data**" means data derived from or compiled through Customer's or its Portal Users' use of the Licensed Services, such as statistics indicating frequency of use of the Licensed Services. Usage Data may be derived from Customer Confidential Information, but will not include Personal Information. Usage Data that is not linked or linkable to any individual or to Customer shall be owned by Impartner and may be used by Impartner for any lawful purpose.

7. CONFIDENTIALITY

7.1 Confidential Information. As used herein "**Confidential Information"** shall mean all confidential or proprietary information disclosed orally or in writing by one Party to the other that is identified as confidential or whose confidential nature is reasonably apparent under the circumstances. Customer Confidential Information includes Customer Data; Impartner Confidential Information includes the Licensed Services and Documentation; and Confidential Information of each Party shall include the terms and conditions of the Agreement and all Order Forms, as well as business and marketing plans, technology and technical information, product plans and designs, and business processes disclosed by such Party. Confidential Information shall not include information which: (a) is or becomes a part of the public domain through no fault of the receiving Party; (b) was in the receiving Party's lawful possession prior to the disclosure; (c) is lawfully disclosed to the receiving Party by a third party without restriction on disclosure or any breach of confidence; or (d) is independently developed by the receiving Party.

7.2 Protection of Confidential Information. Each Party agrees to (i) hold the other's Confidential Information in confidence, (ii) use the same degree of care that it uses to protect the confidentiality of its own confidential information of like kind (but in no event less than reasonable care), and (iii) not use or disclose such Confidential Information other than in connection with the performance of its obligations hereunder or as otherwise authorized by the Agreement. Notwithstanding the foregoing, either Party may disclose any of the other Party's Confidential Information to its, and its Affiliates' and Partners' employees, contractors, consultants, attorneys, accountants, and other advisors ("**Representatives**") that have a need

to know such Confidential Information in connection with such Party's performance under the Agreement and that have agreed to be bound by confidentiality obligations similar to those in this Confidentiality section. Each Party shall be liable to the other under the Agreement for any breach of this Confidentiality section by its Representatives. A Party shall notify the disclosing Party in writing of any loss or unauthorized or inadvertent use or disclosure of or access to the disclosing Party's Confidential Information promptly following the receiving Party's discovery of such loss, use, disclosure, or access, and shall promptly take measures to minimize the effect of such loss, use, disclosure, or access and to prevent its recurrence.

7.3 Sensitive Personal Information. Customer agrees not to use the Licensed Services to collect, process, or store any Sensitive Personal Information. Customer agrees not to transmit, disclose, or make available Sensitive Personal Information to Impartner, or to Impartner's third-party service providers pursuant to its relationship with Impartner. For purposes of this provision, Sensitive Personal Information shall have the definition ascribed to it under the California Privacy Rights Act of 2020 (the "**CPRA**") and shall include "special categories of personal data" as defined by the GDPR.

7.4 Term. These confidentiality obligations will remain in effect for the duration of the Agreement plus two (2) years following its termination; provided, however, that all obligations under this Agreement relating to (i) trade secrets will survive for so long as any such Confidential Information remains a trade secret under applicable law, and (ii) financial information will survive for a period of five (5) years following termination of this Agreement.

7.5 Protection of Customer Data. Without limiting the above, Impartner shall maintain appropriate administrative, physical, and technical safeguards for protection of the security, confidentiality and integrity of Customer Data, and if the Parties have entered into a DPA, in accordance with Annex II of said DPA. Impartner shall not (a) modify Customer Data; (b) disclose Customer Data except to provide the Licensed Services to Customer, as compelled by law in accordance with the section herein titled Compelled Disclosure, or as otherwise expressly permitted in writing by Customer; or (c) access Customer Data except to provide the Licensed Services and prevent or address service or technical problems, or at Customer's request in connection with customer support matters.

7.6 Compelled Disclosure. The receiving Party may disclose the Confidential Information of the disclosing Party if it is compelled by law to do so, provided the receiving Party gives the disclosing Party prior notice of such compelled disclosure (to the extent legally permitted) and reasonable assistance, at the disclosing Party's cost, if the disclosing Party wishes to contest the disclosure.

7.7 Obligations on Termination. Upon expiration or termination of the Agreement, each Party will: (a) immediately cease all use of the other Party's Confidential Information; and (b) upon request, within ten (10) calendar days, unless otherwise specified in the Agreement, confirm in writing to the other Party that it has permanently erased from computer memory, destroyed or returned to the other Party the other Party's Confidential Information, as well as any copies thereof on any media or in any form. Notwithstanding the foregoing, Impartner may retain Customer Data as required by applicable laws, regulations, court orders, subpoenas or other legal process. Any failure of Impartner to return or destroy electronic copies of Customer Data that are automatically generated through data backup and/or archiving systems shall not be deemed to violate the provisions of this Section 7.7, provided that (i) Impartner shall not use such back-ups or archived copies of Customer Data for any purpose; (ii) such copies shall be subject to the confidentiality obligations set forth herein, and (iii) such Customer Data is deleted in Impartner's due course and within a commercially reasonable timeframe.

7.8 Remedies. Each Party agrees that the other Party may have no adequate remedy at law if there is a breach or threatened breach of the confidentiality provisions herein and, accordingly, that either Party is entitled (in addition to any legal or equitable remedies available to such Party) to seek injunctive or other equitable relief without the necessity of proof of actual damages to prevent or remedy such breach.

8. WARRANTIES, REMEDIES, AND DISCLAIMERS

8.1 Limited Service Warranty. Upon completion of Implementation Services and for the remainder of the Term, Impartner warrants that the Licensed Services will operate without a Documented Defect (the "**Performance Warranty**"). "**Documented Defect**" means a material deviation between the then-current, general release version of the Licensed Services and Documentation. Customer shall promptly notify

Impartner of a Documented Defect, and Impartner will use commercially reasonable efforts to promptly repair the Documented Defect. In the event a Documented Defect cannot be repaired within thirty (30) days from the receipt of notice through no fault of Customer, then Customer may terminate those specific services upon notice to Impartner and receive a *pro rata* refund for the specific Licensed Services that are affected. For clarity, "fault," as used in the preceding sentence, shall include any unreasonably delayed response/s by Customer to any reasonable implementation-related requests from Impartner. The remedy in this Section 8.1 shall be Customers exclusive remedy for breaches of the Performance Warranty.

8.2 Malicious Code. Impartner warrants that it has taken commercially reasonable steps to prevent the introduction of any malicious code or any other internal components, devices or mechanisms designed to disrupt, disable, harm, or otherwise impair in any material respect the normal and authorized operation of the Licensed Services, including viruses, worms, time bombs, and Trojan horses.

8.3 Disclaimer. EXCEPT AS EXPRESSLY PROVIDED HEREIN, THE LICENSED SERVICES ARE PROVIDED ON AN AS-IS BASIS WITHOUT WARRANTY OF ANY KIND, WHETHER EXPRESS, IMPLIED, STATUTORY OR OTHERWISE, AND EACH PARTY SPECIFICALLY DISCLAIMS ALL IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT, AND FITNESS FOR A PARTICULAR PURPOSE, TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW. IMPARTNER DOES NOT WARRANT THAT THE LICENSED SERVICES WILL SATISFY CUSTOMER'S REQUIREMENTS OR (WITHOUT LIMITING THE PERFORMANCE WARRANTY ABOVE) THAT IT IS WITHOUT DEFECT OR ERROR OR THAT CUSTOMER'S ACCESS THERETO WILL BE UNINTERRUPTED. IN ADDITION, EACH PARTY AGREES THAT IT HAS NOT RELIED UPON ANY REPRESENTATION OR WARRANTY OR ANY OTHER INFORMATION OF ANY KIND MADE BY OR PROVIDED BY THE OTHER PARTY, OR ANY OTHER PERSON ON SUCH PARTY'S BEHALF.

9. INDEMNIFICATION; LIMITATION OF LIABILITY

9.1 Indemnification. Each Party (an "**Indemnifying Party**") agrees to defend the other Party, its directors, officers, employees, and agents (collectively, the "**Indemnified Party**") against any claims, demands, suits, or proceedings (each, a "**Claim**") made or brought against the Indemnified Party by a third party and indemnify the Indemnified Party from any damages finally awarded by a court of competent jurisdiction against the Indemnified Party or amounts agreed to in settlement in connection with any such Claim, to the extent the Claim arises out of or results from: (a) an allegation, in the case of Customer as the Indemnified Party, that the Licensed Services infringe or misappropriate the intellectual property rights, publicity rights, or privacy rights of such third party; or (b) an allegation, in the case of Impartner as the Indemnified Party, that the Customer Data or any other information provided by Customer to Impartner for use in connection with the Licensed Services, infringes or violates the intellectual property rights or privacy rights of a third party, or violates the electronic mail requirements in Section 12. In no event will Impartner have any obligation or liability under subsection (a) for any Claim that is caused by, or results from: (i) Customer's combination, operation or use of the Licensed Services with software or other materials not supplied by Impartner, including Third-Party Applications; (ii) any alteration or modification of the Licensed Services by Customer; (iii) Customer's continued allegedly infringing activity after being notified thereof or after being provided modifications that would have avoided the alleged infringement; or (iv) the actions or omissions of any person or entity other than Impartner. In no event will Customer have any obligation or liability under subsection (b) for any Claim that is caused by, or results from: (i) Impartner's continued allegedly infringing activity after being notified thereof or after being provided modifications that would have avoided the alleged infringement; or (ii) the actions or omissions of any person or entity other than Customer or its Portal Users.

9.2 Remedy for Infringement. Should Customer's right to use the Licensed Services pursuant to the Agreement be subject to a Claim of infringement, or if Impartner reasonably believes such a Claim of infringement (collectively, "**IP Claims**") may arise, Impartner may, at its option and in its sole discretion: (i) procure for Customer the right to continue to access and use the Licensed Services; (ii) modify the Licensed Services to render them non-infringing but substantially functionally equivalent to the Licensed Services prior to such modification; or (iii) if the alternatives described in clauses (i) and (ii) of this paragraph are not commercially practicable, then Impartner may terminate the Agreement and refund to Customer any amounts pre-paid by Customer for the Licensed Services for the unused portion of the subscription term.

9.3 Sole Remedy. CUSTOMER HEREBY AGREES THAT THIS SECTION 9.1(a) AND 9.2 TOGETHER SET FORTH IMPARTNER'S SOLE AND EXCLUSIVE LIABILITY AND CUSTOMER'S SOLE AND EXCLUSIVE REMEDY FOR IP CLAIMS.

9.4 Indemnification Process. In connection with any Claim, (a) the Indemnified Party shall promptly notify the Indemnifying Party in writing of such Claim, provided the Indemnified Party's failure to provide written notice to the Indemnifying Party shall not affect the Indemnifying Party's indemnification obligations except to the extent the Indemnifying Party is materially prejudiced thereby; (b) the Indemnifying Party shall control the defense and all related settlement negotiations relating to the Claim, provided, however, that the settlement of such Claim shall not be made without the advance written permission of the Indemnified Party, which shall not be unreasonably withheld; and (c) the Indemnified Party shall provide the Indemnifying Party with the assistance, information and authority reasonably necessary to perform the foregoing.

9.5 Limitation of Liability.

9.5.1 IN NO EVENT SHALL EITHER PARTY HAVE ANY LIABILITY TO THE OTHER FOR ANY LOST PROFITS OR REVENUES OR FOR ANY INDIRECT, SPECIAL, INCIDENTAL, CONSEQUENTIAL, COVER OR PUNITIVE DAMAGES, HOWEVER CAUSED, WHETHER IN CONTRACT, TORT OR UNDER ANY OTHER THEORY OF LIABILITY, AND WHETHER OR NOT THE PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

9.5.2 EXCEPT FOR THEIR OBLIGATIONS UNDER SECTION 3.1 (USE OF SERVICES), SECTION 3.2 (RESTRICTIONS), SECTION 5 (FEES AND PAYMENT), SECTION 7 (CONFIDENTIALITY), SECTION 9 (INDEMNIFICATION), AND ANY DATA PROCESSING ADDENDUM INCLUDED IN THE AGREEMENT, IN NO EVENT SHALL EITHER PARTY'S LIABILITY TO THE OTHER PARTY FOR DAMAGES UNDER THIS AGREEMENT FOR ANY CAUSE WHATSOEVER, AND REGARDLESS OF THE FORM OF THE ACTION, EXCEED THE FEES PAID BY CUSTOMER FOR THE APPLICABLE LICENSED SERVICES DURING THE 12-MONTH PERIOD IMMEDIATELY PRECEDING THE INCIDENT UNDER THE APPLICABLE ORDER FORM (THE "**BASE CAP**").

9.5.3 WITH RESPECT TO THEIR OBLIGATIONS UNDER SECTION 7 (CONFIDENTIALITY), SECTION 9 (INDEMNIFICATION), AND ANY DATA PROCESSING ADDENDUM INCLUDED IN THE AGREEMENT, IN NO EVENT SHALL EITHER PARTY'S LIABILITY TO THE OTHER FOR DAMAGES UNDER THIS AGREEMENT FOR ANY CAUSE WHATSOEVER, AND REGARDLESS OF THE FORM OF THE ACTION, EXCEED FIVE TIMES (5X) THE BASE CAP.

10. Insurance. Impartner shall maintain during the term of this Agreement the following insurance coverages:

10.1 Workers compensation. Worker's compensation as prescribed by applicable law, and employers' liability insurance in an amount of no less than $1,000,000 per accident;

10.2 Commercial liability. Commercial general liability insurance, the limits of which shall not be less than $1,000,000 per occurrence and $2,000,000 annual aggregate;

10.3 Automobile. Automobile bodily injury and property damage liability insurance, the limit of which shall not be less than $1,000,000 per occurrence;

10.4 Umbrella. Umbrella or excess liability insurance, the limits of which insurance shall not be less than $6,000,000; and

10.5 Tech errors and omissions/Cyber. Tech errors and omissions/Cyber insurance the limits which shall not be less than $5,000,000.

11. TERM AND TERMINATION

11.1 Term of Agreement. Unless otherwise terminated earlier under Section 8.1 (Limited Service Warranty) or 11.2 (Termination for Cause), the Agreement commences on the Effective Date (as defined in the Order Form) and continues until the expiration of any of the term(s) specified in an Order Form ("**Term**").

11.2 Termination for Cause. A Party may terminate the Agreement for cause (i) upon thirty (30) days' written notice to the other Party of a material breach if such breach remains uncured at the expiration of such period, or (ii) immediately upon a Bankruptcy Event of either Party.

11.3 Refund or Payment upon Termination. Upon any termination for cause by Customer under Section 11.2 (Termination for Cause), Impartner shall refund Customer any prepaid Fees covering the unused portion of the Term. Upon any termination for cause by Impartner, without limiting any other remedies available to Impartner, Customer shall pay any unpaid Fees covering the remainder of the Term within thirty (30) days after the effective date of termination. Except as provided in this Section, in no event shall any termination relieve Customer of its obligation to pay any Fees payable to Impartner for any period prior to the effective date of termination.

11.4 Surviving Provisions. All provisions which, by their nature, are intended to survive the termination or expiration of the Agreement shall survive.

12. COMPLIANCE WITH LAW. The Parties shall comply with all applicable laws, rules, regulations in connection the Licensed Services. For clarity, for emails sent to U.S. residents by Customer via the Licensed Services, Customer shall comply with all requirements of the federal Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (the "**CAN SPAM Act**"), all rules and official guidance promulgated by the Federal Trade Commission ("**FTC**") pursuant to the CAN SPAM Act, the Federal Communications Commission's ("**FCC**") rules and orders regulating the transmission of commercial e-mail to wireless devices, and all other applicable U.S. federal, state and local laws and regulations.

13. GENERAL PROVISIONS

13.1 Export Compliance; Sanctioned Countries. Each Party shall comply with the export laws and regulations of the United States and other applicable jurisdictions in providing and using the Licensed Services. Without limiting the foregoing, each Party represents that it is not named on any U.S. government list of persons or entities prohibited from receiving exports, and Customer shall not permit Portal Users to access or use the Licensed Services in violation of any U.S. export embargo, prohibition or restriction. Furthermore, Customer represents and warrants that (i) all Portal Users are prohibited from residing in, or operating from, any country that is sanctioned by either the U.S. Treasury Department's Office of Foreign Assets Control (OFAC) or the United Nations Security Council ("**Prohibited Countries**"), and (ii) it will not knowingly permit any data pertaining to residents of any Prohibited Countries be processed by the Licensed Services, including by prohibiting Portal Users from processing any such data via the Licensed Services.

13.2 Force Majeure. Except with respect to the payment of Fees hereunder, neither Party shall be liable to the other Party for a failure or delay in performing any obligation hereunder that is directly caused by conditions beyond that Party's reasonable control, including acts of God, Pandemic (as defined below), war, terrorism, civil commotion, strikes, labor disputes and governmental actions or restriction ("**Force Majeure Event**"), provided the Party seeking to be excused from performance promptly notified the other Party of the Force Majeure Event, takes commercial reasonably action to mitigate the effects of the Force Majeure Event, and promptly resumes performance when the Force Majeure Event has subsided. When a Party's delay or non-performance continues for a period of thirty (30) days or more, the other Party may terminate the Agreement without penalty. Any prepaid amounts shall be refunded on a prorated basis. "**Pandemic**" shall mean a global transmissible health emergency as declared by the World Health Organization that results in specific governmental restrictions that makes the performance of a party's obligations under this Agreement illegal or impossible. The parties expressly agree that the novel coronavirus Covid-19 pandemic, ongoing as of the date of the execution of this Agreement, is not a Force Majeure Event.

13.3 Relationship of the Parties. The Parties are independent contractors. The Agreement does not create a partnership, franchise, joint venture, agency, fiduciary or employment relationship between them.

13.4 No Third-Party Beneficiaries. There are no third-party beneficiaries to the Agreement.

13.5 Notices. Except as otherwise specified in the Agreement, all notices, permissions and approvals hereunder shall be in writing and delivered to the addresses set forth on the first page of the Agreement and shall be deemed to have been given upon: (i) personal delivery, (ii) the second business day after

overnight delivery, or (iii) receipt of acknowledgment by recipient if sent by email. Any legal notices sent to Impartner by email must additionally be sent to legal.notice@impartner.com, and any notices sent by email related to invoices or billing must additionally be sent to accounts.receivable@impartner.com.

13.6 Waiver and Cumulative Remedies. No failure or delay by either Party in exercising any right under the Agreement shall constitute a waiver of that right. Other than as expressly stated herein, the remedies provided herein are in addition to, and not exclusive of, any other remedies of a Party at law or in equity.

13.7 Severability. If any provision of the Agreement is held by a court of competent jurisdiction to be contrary to law, the provision shall be modified by the court and interpreted so as best to accomplish the objectives of the original provision to the fullest extent permitted by law, and the remaining provisions of the Agreement shall remain in effect.

13.8 Assignment. Neither Party may assign its rights or obligations under this Agreement without the other Party's prior written consent. Notwithstanding the foregoing, either Party may assign its rights and obligations under this Agreement to an Affiliate as part of a reorganization, or to a purchaser of its business entity or substantially all of its assets or business to which rights and obligations pertain without the other Party's consent, provided that: (a) the purchaser is not insolvent or otherwise unable to pay its debts as they become due; (b) the purchaser is not a competitor of the other Party; and (c) any assignee is bound hereby. Other than the foregoing, any attempt by either Party to transfer its rights or obligations under this Agreement will be void.

13.9 Governing Law; Venue. The Agreement, and any disputes arising out of or related hereto, shall be governed exclusively by the internal laws of the State of Utah, without regard to its conflicts of laws rules. The state and federal courts located in Salt Lake City, Utah shall have exclusive jurisdiction to adjudicate any dispute arising out of or relating to the Agreement. Each Party hereby consents to the exclusive jurisdiction of such courts.

13.10 Entire Agreement. The Agreement, including all Exhibits, constitutes the entire agreement between the Parties and supersedes all prior and contemporaneous agreements, proposals or representations, written or oral, concerning its subject matter. In the event of conflict between the Order Form, the order of precedence shall be: (i) DPA, if applicable, (ii) other Exhibits, (iii) Order Form, and then (iii) the MSA. No modification, amendment, or waiver of any provision of the Agreement shall be effective unless in writing that specifically references the Agreement and is signed by the Party against whom the modification, amendment or waiver is to be asserted. Notwithstanding any language to the contrary therein, no terms or conditions stated in any Customer purchase order or in any other Customer order documentation shall be incorporated into or form any part of the Agreement, and all such terms or conditions shall be null and void.

[Remainder of Page Intentionally Blank]

Appendix 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, Master Services Agreement, and any other exhibits attached thereto, unless expressly defined otherwise in this DPA. In the event of any conflict/s between the Order Form, Master Services Agreement, and Data Processing Addendum, unless expressly indicated otherwise, the order of precedence shall be: (i) Data Processing Addendum, (ii) Order Form, and (iii) Master Services 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 Services 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 Master Services 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, as amended by the California Privacy Rights Act of 2020, including any regulations promulgated thereunder, as amended from time to time (together, "CCPA"); (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 or identifiable legal entity (where such information is protected similarly as personal data or personally identifiable information under Applicable Data Protection Law), where for each (i) or (ii), such data is Customer Data.

"**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 UK Government, which at the date of this DPA is the UK International Data Transfer Agreement available at https://ico.org.uk/media/for-organisations/documents/4019538/international-data-transfer-agreement.pdf or the UK Addendum to the EU SCCs available at https://ico.org.uk/media/for-organisations/documents/4019539/international-data-transfer-addendum.pdf, as each may be amended or replaced by the Information Commissioner's Office and/or UK Government 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 the obligations that apply to it under Applicable Data Protection Law. Impartner shall notify Customer within a reasonable period of time after it makes a determination that it can no longer meet its obligations under Applicable Data Protection Laws and this Addendum. 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.

   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, in accordance with the documented instructions of Customer, and for the business purposes in Annex I (the "**Permitted Purpose**"), except where otherwise permitted by Applicable Data Protection Law, 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. Vendor is prohibited from selling or sharing Personal Information. Impartner shall not process, retain, use, or disclose the Data (i) for any purposes other than the Permitted Purpose, (ii) for any commercial purpose other than the Permitted Purpose, or (iii) outside of the direct business relationship between Impartner and Customer. Impartner is prohibited from combining or updating the Personal Information that it collects under the Agreement and this DPA with Personal Data that it receives from another source or collects from its own interaction with the Data Subject, unless expressly permitted under Applicable Data Protection Laws.

2. *Details of the Processing*. Annex I 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 I by written notice to the other party from time to time as such party reasonably considers necessary to meet those requirements. Nothing in Annex I (including as amended pursuant to this Section 3) confers any right or imposes any obligation on any party to this DPA.

3. *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 or UK Government. Customer 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 I, Annex II and Annex III 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 accordance with Annex IV to this DPA.

4. *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.

5. *Security*. Impartner shall implement appropriate technical and organizational measures to protect the Data from (i) 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 Annex II to this DPA.

6. *Sub-processing*.

    6.1 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.

6.2 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.

6.3 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 DPA.

6.4 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.

6.5 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.

7. *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.

8. *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.

9. *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.

10. *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 a third party for Processing). This requirement shall not apply to the extent that Impartner is required by any Applicable Data Protection Law to retain some or all of the Data.

11. *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 Applicable Data Protection Law. 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 by a 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. Customer may take reasonable and appropriate steps, upon reasonable notice, to stop and remediate Impartner's unauthorized use of Customer's Personal Data.

12. *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.

13. *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.

14. *Miscellaneous:*

    a. Headings. Headings in this DPA are for convenience of reference only and will not constitute a part of or otherwise affect 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 unenforceable in whole or in part, such invalidity or unenforceability will affect only such phrase, clause or provision, and the rest of this 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 to time 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 and their respective successors and assigns.

    f. Counterparts. This DPA may be executed in counterparts, each of which will be deemed an original, but all of which together 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 DPA 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 Protection Law.

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 I: 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 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: 10897 S River Front Parkway, Ste #500, South Jordan, UT 84095

Contact Person's name, position and contact details: Shane Walters, Privacy Officer, dataprocessing@impartner.com

Activities relevant to the data transferred under EU 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.

Business purposes of the processing

Data Importer will process the Personal Data for the following business purposes:

1. Helping to ensure security and integrity to the extent the use of the consumer's personal information is reasonably necessary and proportionate for these purposes.

2. Debugging to identify and repair errors that impair existing intended functionality.

3. Performing services on behalf of the business, including maintaining or servicing accounts, providing customer service, processing or fulfilling orders and transactions, verifying customer information, processing payments, providing financing, providing analytic services, providing storage, or providing similar services on behalf of the business.

4. Undertaking internal research for technological development and demonstration.

5. Undertaking activities to verify or maintain the quality or safety of a service or device that is owned, manufactured, manufactured for, or controlled by the business, and to improve, upgrade, or enhance the service or device that is owned, manufactured, manufactured for, or controlled by the business.

The period for which the personal data will be retained

The Personal Data will be retained per the requirements of the Master Services 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 III 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 II

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

This Annex II 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:

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.
- **Client** – Client is defined as any user of Impartner systems.

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 customers 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 customers 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 III – LIST OF SUB-PROCESSORS

The controller has authorised the use of the following sub-processors:

Name Address	Contact person's name, position and contact details	Description of processing (including a clear delimitation of responsibilities in case several sub-processors are authorised)
Flexential Corp. 600 Forest Point Circle Suite 100 Charlotte, NC 28273	Jeff Goodrich, Account Executive, Jeff.Goodrich@flexential.com 801-617-2975	Colocation services with no logical access to data. Partner portals are hosted at these sites.
Google LLC (Google Analytics) The Googleplex 1600 Amphitheatre Parkway, Mountain View, CA 94043	Keith Enright, Chief Privacy Officer office@google.com	Provides data at numerous Google data centers in the US, and web analytics for Impartner's customers to analyze portal activity.
Global Process Manager, Inc. 17th Floor Times Plaza, United Nations Avenue corner Taft Avenue, Ermita, Manila, 1000	Erik M. Nielsen, President, Connect@gpm.com.ph +632-7759-7105 to 07 ext 123	Receives and fulfills customer requests for technical assistance and support, including in relation to PRM partner portals.
Intuition Machines Inc. (hCaptcha) 1065 SW 8th St #704 Miami, FL 33130	privacy@intuitionmachines.com	Provides bot detection for Impartner Customers who opt-in to service.
Linode, LLC (Akamai Technologies, Inc.) 249 Arch St Philadelphia, PA 19106	James Ackley, Data Privacy Officer Privacy@linode.com	Provides IaaS for News On Demand and Social On Demand. No logical data access.
Mailgun Technologies, Inc. 112 E Pecan St Ste 1100 San Antonio, TX 78205	Darine Fayed, DPO Privacy@mailgun.com	Configured to process 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.
Message Systems, Inc. dba SparkPost 9160 Guilford Rd Columbia, MD 21046	support@sparkpost.com	Provides email service for operational notifications.
Microsoft Corporation (Azure) 5010 NE 36th St. Redmond, WA 98052	Tony Stein, Account Manager Tony.Stein@microsoft.com	Hosts main database and PRM admin portal with PRM microservices. No logical data access.
MongoDB, Inc. 1633 Broadway 38th Floor New York, NY 10019	Mindy Lieberman Chief Information Officer (844) 666-4632 mindy.lieberman@mongodb.com	Provides NoSQL database as a service (Atlas) for microservice backends.
New Relic, Inc. 188 Spear Street San Francisco, CA 94105	Stephanie Blake, Data Privacy Officer Privacy@newrelic.com	Provides aggregate performance metrics for Impartner engineers to identify and troubleshoot tech issues. No logical data access.
Okta, Inc. 10800 NE 8th St, Suite 700 Bellevue, WA, 98004	Lucy McGrath, VP Privacy / DPO, lucy.mcgrath@auth0.com (425) 584-8279	Provides Identity Provider services with logical access to usernames.

Otava LLC 825 Victors Way Ann Arbor, MI 48108	support@otava.com 877-740-5028	Provides IaaS for Impartner Referral. No logical data access.
SendGrid, Inc. 1801 California St #500 Denver, CO 80202	Dana Wagner Chief Legal Officer (303) 552-0653	Provides email service for demand generation (TCMA) notifications.
Solarwinds Worldwide LLC 7171 Southwest Parkway Bdg 400 Austin, TX, 78735	Sarah Crispi, Associate General Counsel technicalsupport@solarwinds.com 1.866.530.8100	Log aggregation and alerting to detect anomalies and debug technical issues.
Syncari, Inc. 8407 Central Ave, Suite 2021 Newark, CA 94560	Neelesh Shastry Data Protection Officer neelesh@syncari.com	Provides bidirectional sync and supports data unification between Impartner objects and CRM entities.
VerticalResponse, Inc. 111 2nd Ave NE – Suite 1500 St Petersburg, FL 33701	S. Carver, Privacy Compliance Manager, Privacy Program Office privacy@verticalresponse.com	Provides email services for TCMA email marketing functionality and has access to Partners' client lists provided by Partners either directly to VerticalResponse or via Impartner.
Wasabi Technologies, Inc. 111 Huntington Avenue Suite 2900 Boston, MA 02199	Support@wasabi.com	Provides offsite backup data storage

ANNEX IV

UK Addendum to EU Standard Contractual Clauses

Part 1: Tables

Table 1: Parties

Start date	Date of the DPA	
The Parties	**Exporter (who sends the Restricted Transfer)**	**Importer (who receives the Restricted Transfer)**
Parties' Details	**Full legal name**: [●] **Main address**: [●] **Official registration number**: [●] Key Contacts: [●]	**Full legal name**: Impartner, Inc. **Main address**: 10897 S River Front Parkway, Ste #500, South Jordan, UT 84095 Key Contacts: Shane Walters, Privacy Officer, dataprocessing@impartner.com
Signature	Incorporated into Agreement by reference.	Incorporated into Agreement by reference.

Table 2: Selected SCCs, Modules and Selected Clauses

"Addendum EU SCCs"	The version of the European Commission approved EU SCCs Module 2 (Controller-to-Processor) dated 4 June 2022, as amended by Clause 4(a) of the DPA (other than amendments in the final three bullet points of that Clause 4(a)), and incorporated into this Addendum by reference.

Table 3: Appendix Information

"Appendix Information" means the information which must be provided for the selected modules as set out in Annex I and II of Schedule A (other than the Parties), and which for this Addendum is set out in:

Annex I(A): List of Parties:

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 these Clauses: Primary business point of contact for relationship with Data Importer
Role (controller/processor): Controller

Data importer(s):

Name: Impartner, Inc.
Address: 10897 S River Front Parkway, Ste #500, South Jordan, UT 84095
Contact person's name, position and contact details: Listed in Table 1 above.
Activities relevant to the data transferred under these Clauses: Responsible for Data Importer's data privacy program

Role (controller/processor): Processor
Annex I(B): Description of Transfer: As set out in **Annex I (Details of the Processing of Company Personal Data)** of the DPA.
Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data: As set out in **Annex II (Technical and Organizational Measures Including Technical and Organizational Measures to Ensure the Security of the Data)** of the DPA.
Annex III: List of Sub processors: As contained in **Annex III (List of Sub-Processors)** of the DPA.

Table 4: Ending this Addendum when the Approved Addendum Changes

Ending this Addendum when the Approved Addendum changes	Which Parties may end this Addendum as set out in Section 19 of the Mandatory Clauses**Error! Reference source not found.**: ☒ Importer ☐Exporter ☐ neither Party

PART 2: MANDATORY CLAUSES

"Mandatory Clauses"	Part 2: Mandatory Clauses of the Approved Addendum, being the template Addendum B.1.0 issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18 of those Mandatory Clauses.

Appendix B

Service Level Agreement

Production Commitment	Impartner Production Environment
SLA Production target – application	99.5% system availability excluding scheduled maintenance.
Scheduled maintenance	Most scheduled maintenance is done non-disruptively. If the system is needed to be shut down for maintenance purposes, advanced notice is given to the customer, and work is performed off hours. Typical availability is not affected by more than 15 minutes. Routine maintenance and patching are conducted without impacting availability, and work is performed during off-peak weekend hours without advanced notice.
Phone support window	Standard Support includes 24/7 access to online customer support, as well as phone support Monday through Friday from 2 AM to Midnight (12 AM) MT (US).
Issue severity definition and turnaround/resolution timelines	Service requests may be submitted by you online through Impartner's web-based customer support systems (Customer support ticket or Support Request Form), by email, or by telephone. The service request severity level is selected by you and should be based on the following severity definitions: **Severity 1** Your production use of the SaaS program is stopped or so severely impacted that you cannot reasonably continue work. You experience a complete loss of service. The operation is mission critical to the business and the situation is an emergency. A Severity 1 service request has one or more of the following characteristics: ▪ Impartner application or partner portal is unavailable from web browser. ▪ Critical documented functionality is not available. ▪ System performance is such that it prevents users from performing necessary functions. Impartner will use reasonable efforts to respond to Severity 1 service requests within one (1) hour. Impartner will work 24/7 until the Severity 1 service request is resolved or as long as useful progress can be made. You must provide Impartner with a contact during this 24/7 period, either on site or by mobile phone, to assist with data gathering, testing, and applying fixes. You are requested to propose this severity classification with great care, so that valid Severity 1 situations obtain the necessary resource allocation from Impartner. **Severity 2** You experience a severe loss of service. Important features of the SaaS program are unavailable with no acceptable workaround; however, operations can continue in a restricted fashion. Impartner Support works to provide an initial response within 4 hours. **Severity 3** You experience a minor loss of service. The impact is an inconvenience which may require a workaround to restore functionality. Impartner Support works to provide an initial response within 24 hours to the

	creation of a Severity 3 request. We request all Severity 3 requests be made online using our Customer support ticket ticketing system. **Severity 4** You request information, an enhancement, professional services or content placement on the portal or documentation clarification regarding the SaaS program, but there is no impact on the operation of such program. You experience no loss of service. The result does not impede the operation of a system. We request all Severity 4 requests be made online using our Customer support ticket ticketing system. Impartner Support works to provide an initial response within 24 business hours to the creation of a Severity 4 request.
SLA for professional service work	SLA for most portal content updates and changes is 24-48 business hours. Updates that involve custom programming or other professional services will take longer. Impartner will make commercially reasonable efforts to complete the tasks submitted or enter a commitment or completion time for such tasks in Customer support ticket within 24-48 business hours after submission.
Notification of root cause and corrective action for unscheduled downtime	In the rare case that there is downtime outside the SLA described above, Impartner will provide an email notification of such downtime and explain root cause and corrective measures that have been taken. ▪ Recovery Time Objective (RTO): The primary business impact is the loss of public confidence and the interruption of sales cycles. The expected RTO is less than 12 hours. ▪ Recovery Point Objective (RPO): The unrecovered transactions will have to be reentered into the system. The data loads from other system will have to rerun to recover lost data. The expected RPO is less than 12 hours.
Uptime reporting	Client may request this report monthly via Customer support ticket, and Impartner will provide a report of portal uptime.
Critical patches and updates	Impartner commits to making system, software, and hardware updates and patches to Production environments in a commercially reasonable manner per its internal policies.

Development & Stage Commitment	**Impartner Development & Stage**
SLA Development & Stage systems target – application	99% system availability excluding scheduled maintenance.
Maintenance windows or other planned down time	Most scheduled maintenance is done non-disruptively. If the system is needed to be shut down for maintenance purposes, it is the intent of Impartner to perform this during night or weekend hours (US) to avoid disruption to the service. Typically availability is not affected by more than 15 minutes. Routine maintenance and patching are conducted without impacting availability, and work is performed during off-peak weekend hours without advanced notice.
Support window	Customer Care provides 24/7 access to online customer support, as well as phone support Monday through Friday from 8 AM to 5 PM MT (US). Phone support outside these hours is available at an additional cost.

Issue severity definition and turnaround/resolution timelines	Service requests may be submitted by you online through Impartner's web-based customer support systems (Customer support ticket or Support Request Form), by email, or by telephone. Please note that these systems are provided for convenience and testing. However, testing and server sync times do not reflect that of production services. Such that these systems are not production based, the SLA for these systems will be as follows: - Initial response time will be within 48 business hours - Time to resolution will be based on commercially reasonable efforts while ensuring production items take priority Please note that Impartner is not responsible to ensure that content, data, assets and/ or other information in PRM matches that of production.
Support escalation process	Escalating an issue brings a heightened level of awareness to management and, when appropriate, more resources to resolve a given issue. In the case of Development and Stage environments, escalations can be submitted, but will not be prioritized over Production issues nor held to the same standard of the Production environment. Service request severity escalation requests can be made online or by calling the dedicated support manager. To escalate an issue, contact the dedicated support manager who will then engage the appropriate team members to work with you to develop an action plan.
Notification of root cause and corrective action for unscheduled downtime	In the rare case that there is downtime outside the SLA described above, Impartner will provide information related to these systems upon request of the client for root cause information.
Critical patches and updates	Impartner commits to making system, software, and hardware updates and patches to Development and Stage environments in a commercially reasonable manner per its internal policies.