**AMC Technology LLC Data Processing Agreement**

This AMC Technology LLC ("AMC," "us," or "we") Data Processing Agreement and its exhibits ("DPA") reflect the parties' agreement with respect to the Processing of Personal Data by us on behalf of you ("you," "your," or "customer") in connection with the services provided under the AMC cloud services agreement between you and us ("Agreement")

This DPA is incorporated by reference into, and forms an integral part of, the Agreement. This DPA is effective upon its incorporation into the Agreement, which may be specified in the Agreement or in an executed amendment to the Agreement. The parties agree that this DPA governs the processing and security of Personal Data. Separate terms, including different privacy and security terms, govern your use of products and services not offered by AMC.In case of any conflict or inconsistency with the terms of the Agreement, this DPA will take precedence over the terms of the Agreement to the extent of such conflict or inconsistency. We update the terms in this DPA from time to time. If you have an active subscription with us, we will let you know when we do on the AMC website or via in-software notifications. The term of this DPA will follow the term of the Agreement. Terms not otherwise defined will have the meaning as set forth in the Agreement.

This Data Processing Agreement applies to AMC's Processing of Personal Data on your behalf as Controller as defined herein, and AMC as a Processor for the provision of the Services specified in the Agreement. Unless otherwise expressly stated, this version of the Data Processing Agreement shall be effective and remain in force for the term of the Agreement.

You must comply with all laws and regulations applicable to your use of the Services, including but not limited to laws relating to confidentiality of communications and Data Protection Laws. You are responsible for determining whether the Services are appropriate for storage and processing subject to any specific law or regulation and for using the Services in a manner consistent with your legal and regulatory obligations.

## 2. DEFINITIONS

"Affiliate" or "Affiliates" means any entity that directly or indirectly controls, is controlled by, or is under common control with the subject entity. "Control" for purposes of this definition means direct or indirect ownership or control of more than 50% of the voting interests of the subject entity.

“California Personal Information” means Personal Data that is subject to the protection of the CCPA.

"CCPA" means California Civil Code §1798.100 et seq. (also known as the California Consumer Privacy Act of 2018).

"Consumer", "Business", "Sell" and "Service Provider" will have the meanings given to them in the CCPA.

“Controller” means the natural or legal person, public authority, agency, or other body which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data.

“Data Protection Laws” means the CCPA, GDPR, Local EU/EEA Data Protection Laws, and any applicable laws, regulations, and other legal requirements relating to: (i) privacy and data security; and (ii) the use, collection, retention, storage, security, disclosure, transfer, disposal, and other processing of any Personal Data; in each case as amended, repealed, consolidated or replaced from time to time.

“Data Subject” means the individual to whom Personal Data relates.

"Europe" means, strictly for the purpose of this DPA, the European Union, the European Economic Area and/or their member states, Switzerland, and the United Kingdom.

“European Data” means Personal Data that is subject to the protection of European Data Protection Laws.

"European Data Protection Laws" means data protection laws applicable in Europe as defined herein, including: (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 (General Data Protection Regulation) ; (ii) Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector; and (iii) applicable national implementations of (i) and (ii); or (iii) in respect of the United Kingdom, any applicable

national legislation that replaces or converts in domestic law the General Data Protection Regulation or any other law relating to data and privacy as a consequence of the United Kingdom leaving the European Union; and (iv) Swiss Federal Data Protection Act of June 19, 1992 19 June 1992 and its ordinance; in each case, as may be amended, superseded or replaced.

“GDPR” means Regulation (EU) 2016/679 of the European parliament and of the council of April 27, 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC .

“Instructions” means the written, documented instructions issued by a Controller to a Processor, and directing the same to perform a specific or general action with regard to Personal Data (including, but not limited to, depersonalizing, blocking, deletion, making available).

“Local EU/EEA Data Protection Laws” means any subordinate legislation and regulation implementing the GDPR.

"Permitted Affiliates" means any of your Affiliates that (i) are permitted to use the Services pursuant to the Agreement, but have not signed their own separate agreement with us and are not a “Customer” as defined under the Agreement, (ii) qualify as a Controller of Personal Data Processed by us, and (iii) are subject to European Data Protection Laws.

“Personal Data” means any information relating to an identified or identifiable individual where such information is contained within, generated as a result of, or necessary to provide the Services,  and is protected similarly as personal data, personal information, or personally identifiable information under applicable Data Protection Laws.

“Personal Data Breach” means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored, or otherwise Processed by us and/or our Sub-Processors in connection with the provision of the Services.

"Personal Data Breach" will not include unsuccessful attempts or activities that do not compromise the security of Personal Data, including unsuccessful log-in attempts, pings, port scans, denial of service attacks, and other network attacks on firewalls or networked systems.

"Privacy Shield" means the EU-U.S. and Swiss-US Privacy Shield self-certification program operated by the U.S. Department of Commerce and approved by the European Commission pursuant to its Decision of July, 12 2016 and by the Swiss Federal Council on January 11, 2017 respectively; as may be amended, superseded or replaced.

"Privacy Shield Principles" means the Privacy Shield Principles (as supplemented by the Supplemental Principles) contained in Annex II to the European Commission Decision of July,12 2016; as may be amended, superseded, or replaced.

“Processing” means any operation or set of operations which is performed on Personal Data, encompassing the collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, or erasure of Personal Data. The terms “Process”, “Processes” and “Processed” will be construed accordingly.

“Processor” means a natural or legal person, public authority, agency, or other body which Processes Personal Data on behalf of the Controller.

“Services” or “Service” means the offering elaborated in Section 1.5 of the Agreement.

“Standard Contractual Clauses” means the standard data protection clauses for the transfer of Personal Data to processors established in countries that do not ensure an adequate level of data protection as described in Article 46 of GDPR and approved pursuant to the European Commission’s decision (C(2010)593) of 5 February 2010, as may be amended, superseded or replaced.

“Sub-Processor” means any Processor engaged by us to assist in fulfilling our obligations with respect to the provision of the Services under the Agreement. Sub-Processors may include third parties but will exclude any AMC employee.

## 3. CUSTOMER RESPONSIBILITIES

Compliance with Laws. Within the scope of the Agreement and in your use of the Services, you will be responsible for complying with all requirements that apply to you under applicable Data Protection Laws with respect to your Processing of Personal Data and the Instructions you issue to us.

In particular but without prejudice to the generality of the foregoing, you acknowledge and agree that you will be solely responsible for: (i) the accuracy, quality, and legality of Personal Data and the means by which you acquired Personal Data; (ii) complying with all necessary transparency and lawfulness requirements under applicable Data Protection Laws for the collection and use of the Personal Data, including obtaining any necessary consents and authorizations (particularly for use by you for marketing purposes); (iii) ensuring you have the right to transfer, or provide access to, the Personal Data to us for Processing in accordance with the terms of the Agreement (including this DPA); (iv) ensuring that your Instructions to us regarding the Processing of Personal Data comply with applicable laws, including Data Protection Laws; and (v) complying with all laws (including Data Protection Laws) applicable to any emails or other content created, sent or managed through the Services, including those relating to obtaining consents (where required) to send emails, the content of the emails and its email deployment practices. You will inform us without undue delay if you are not able to comply with your responsibilities under this sub-section (a) or applicable Data Protection Laws.

Controller Instructions. The parties agree that the Agreement (including this DPA), together with your use of the Services in accordance with the Agreement, constitute your complete and final Instructions to us in relation to the Processing of Personal Data, and additional instructions outside the scope of the Instructions shall require prior written agreement between AMC and you.

## AMC'S OBLIGATIONS

Compliance with Instructions. AMC will use and otherwise process Personal Data only in accordance with your documented instructions as shown at Exhibit 1 attached, and as described and subject to the limitations provided herein (i) to provide you with the Services; and (b) to the extent otherwise required by applicable law. We are not responsible for compliance with any Data Protection Laws applicable to you or your industry that are not generally applicable to us.

Conflict of Laws. If we become aware that we cannot Process Personal Data in accordance with your Instructions due to a legal requirement under any applicable law, we will (i) promptly notify you of that legal requirement to the extent permitted by the applicable law; and (ii) where necessary, cease all Processing (other than merely

storing and maintaining the security of the affected Personal Data) until such time as you issue new Instructions with which we are able to comply. If this provision is invoked, we will not be liable to you under the Agreement for any failure to perform the applicable Services until such time as you issue new lawful Instructions with regards to the Processing.

Security. We will implement and maintain appropriate technical and organizational measures to protect Personal Data from Personal Data Breaches, as described under Exhibit 2 to this DPA ("Security Measures"). Notwithstanding any provision to the contrary, we may modify or update the Security Measures at our discretion provided that such modification or update does not result in a material degradation in the protection offered by the Security Measures.

Confidentiality. We will ensure that any personnel whom we authorize to Process Personal Data on our behalf is subject to appropriate confidentiality obligations (whether a contractual or statutory duty) with respect to that Personal Data.

Personal Data Breaches. We will notify you without undue delay after AMC becomes aware of any Personal Data Breach and will provide timely information relating to the Personal Data Breach as it becomes known or reasonably requested by you. At your request, we will promptly provide you with such reasonable assistance as necessary to enable you to report relevant Personal Data Breaches to competent authorities and/or affected Data Subjects, if you are required to do so under Data Protection Laws.

Deletion or Return of Personal Data. We will delete or return all Customer Data, including Personal Data (including copies thereof) Processed pursuant to this DPA, on termination or expiration of the Agreement in accordance with the procedures and timeframes set out in the Agreement, save that this requirement shall not apply to the extent we are required by applicable law to retain some or all of the Personal Data AMC has archived on back-up systems, which data we will securely isolate and protect from any further Processing and delete in accordance with AMC's deletion practices. You may request the deletion of your AMC account after expiration or termination of your subscription by sending a request to support@amctechnology.com.

**DATA SUBJECT REQUESTS**

The Service provides you with a number of controls that you can use to retrieve, correct, delete or restrict Personal Data, which you can use in connection with obligations under Data Protection Laws, including your obligations relating to responding to requests from Data Subjects to exercise their rights under applicable Data Protection Laws ("Data Subject Requests").

To the extent that you are unable to independently address a Data Subject Request through the Service, then upon your written request we will provide reasonable assistance to you to respond to any Data Subject Requests or requests from data protection authorities relating to the Processing of Personal Data under the Agreement. You shall reimburse us for the commercially reasonable costs arising from this assistance.

If a Data Subject Request or other communication regarding the Processing of Personal Data under the Agreement is made directly to us, we will promptly inform you and will advise the Data Subject to submit their request to you. You will be solely responsible for responding substantively to any such Data Subject Requests or communications involving Personal Data.

**SUB PROCESSORS**

You agree that we may engage Sub-Processors to Process Personal Data on your behalf. Where we engage Sub-Processors, we will impose data protection terms on the Sub-Processors that provide at least the same level of protection for Personal Data as those in this DPA (including, where appropriate, the Standard Contractual Clauses), to the extent applicable to the nature of the services provided by such Sub-Processors. We will remain responsible for each Sub-Processor's compliance with the obligations of this DPA and for any acts or omissions of such Sub-Processor that cause us to breach any of AMC's obligations under this DPA.

**ADDITIONAL PROVISIONS FOR EUROPEAN DATA**

Scope of This Section . This 'Additional Provisions for European Data' section shall apply only with respect to European Data.

Roles of the Parties. When Processing European Data in accordance with your Instructions, the parties acknowledge and agree that you are the Controller of European Data and we are the Processor.

Instructions. If we believe that your Instruction infringes European Data Protection Laws (where applicable), we will inform you without delay.

Data Protection Impact Assessments and Consultation with Supervisory Authorities. To the extent that the required information is reasonably available to us, and you do not otherwise have access to the required information, we will provide reasonable assistance to you with any data protection impact assessments, and prior consultations with supervisory authorities or other competent data privacy authorities to the extent required by European Data Protection Laws.

**TRANSFER MECHANISMS FOR DATA TRANSFERS**

A. AMC shall not transfer European Data to any country or recipient not recognized as providing an adequate level of protection for Personal Data (within the meaning of applicable European Data Protection Laws), unless it first takes all such measures as are necessary to ensure the transfer is in compliance with applicable European Data Protection Laws. Such measures may include (without limitation) transferring such data to a recipient that is covered by a suitable framework or other legally adequate transfer mechanism recognized by the relevant authorities or courts as providing an adequate level of protection for Personal Data, to a recipient that has achieved binding corporate rules authorization in accordance with European Data Protection Laws, or to a recipient that has executed appropriate Standard Contractual Clauses, in each case as adopted or approved in accordance with applicable European Data Protection Laws.

B. You acknowledge that in connection with the performance of the Services, AMC is a recipient of European Data in the United States. The parties acknowledge and agree the following:

I. Standard Contractual Clauses: AMC agrees to abide by and process European Data in compliance with the Standard Contractual Clauses.

II. Privacy Shield: Although AMC does not rely on the EU-US Privacy Shield as a legal basis for transfers of Personal Data in light of the judgment of the Court of Justice of the EU in Case C-311/18, for as long as AMC is self-certified to the Privacy Shield AMC will process European Data in compliance with the Privacy Shield Principles and let you know if it is unable to comply with this requirement.

C. The parties agree that (i) purely for the purposes of the descriptions in the Standard Contractual Clauses, AMC will be deemed the "data importer" and you will be deemed the "data exporter" (notwithstanding that you may yourself be located outside Europe and/or be acting as a processor on behalf of third party controllers), (ii) notwithstanding the foregoing, where the AMC contracting entity under the Agreement is not AMC, you provide such contracting entity with a mandate to enter into the Standard Contractual Clauses with AMC in its name and on its behalf, such contracting entity (not AMC) will remain fully and solely responsible and liable to you for the performance of the Standard Contractual Clauses by AMC, and you will direct any instructions, claims or enquiries in relation to the Standard Contractual Clauses to such contracting entity; and (iii) if and to the extent the Standard Contractual Clauses (where applicable) conflict with any provision of this DPA, the Standard Contractual Clauses will prevail to the extent of such conflict.

D. Demonstration of Compliance. We will make all information reasonably necessary to demonstrate compliance with this DPA available to you and allow for and contribute to audits, including inspections by you in order to assess compliance with this DPA. You acknowledge and agree that you will exercise your audit rights under this DPA by instructing us to comply with the audit measures described in this sub-section (g). You acknowledge that the Service is hosted by our data center partners who maintain independently validated security programs and that our systems are regularly tested by independent third party penetration testing firms. Upon request, we will supply (on a confidential basis) a summary copy of its penetration testing report(s) to you so that you can verify our compliance with this DPA.

Further, at your written request, we will provide written responses (on a confidential basis) to all reasonable requests for information made by you necessary to confirm our compliance with this DPA, provided that you will not exercise this right more than once per calendar year.

**ADDITIONAL PROVISIONS FOR CALIFORNIA PERSONAL INFORMATION**

Scope of This Section . The 'Additional Provisions for California Personal Information' section of the DPA will apply only with respect to California Personal Information.

Roles of the Parties. When processing California Personal Information in accordance with your Instructions, the parties acknowledge and agree that you are a Business and we are a Service Provider for the purposes of the CCPA.

Responsibilities. The parties agree that we will Process California Personal Information as a Service Provider strictly for the purpose of performing the Services under the Agreement (the "Business Purpose") or as otherwise permitted by the CCPA..

**GENERAL PROVISIONS**

Amendments. Notwithstanding anything else to the contrary in the Agreement we reserve the right to make any updates and changes to this DPA..

Severability. If any individual provisions of this DPA are determined to be invalid or unenforceable, the validity and enforceability of the other provisions of this DPA will not be affected.

Limitation of Liability. Each party and each of their Affiliates' liability, taken in aggregate, arising out of or related to this DPA (and any other DPAs between the parties) and the Standard Contractual Clauses (where applicable), whether in contract, tort or under any other theory of liability, will be subject to the limitations and exclusions of liability set out in Section 15 of the Agreement and any reference in such section to the liability of a party means aggregate liability of that party and all of its Affiliates under the Agreement (including this DPA).

Governing Law. This DPA will be governed by and construed in accordance with venue and dispute resolution provisions in Section 22 of the Agreement.

**PARTIES TO THIS DPA**

A. Affiliates. By signing the Agreement, you enter into this DPA on behalf of yourself and, to the extent required under applicable Data Protection Laws, in the name and on behalf of your Affiliates, thereby establishing a separate DPA between us and each such Affiliate subject to the Agreement and the 'General Provisions' and 'Parties to this DPA' sections of this DPA. Each Affiliate agrees to be bound by the obligations under this DPA and, to the extent applicable, the Agreement. For the purposes of this DPA only, and except where indicated otherwise, the terms "Customer", "you" and "your" will include you and such Affiliates.

B. Authorization. The party agreeing to and entering into this DPA represents that it is authorized to agree to and enter into this DPA for and on behalf of you and, as applicable, each of your relevant Affiliates.

C. Remedies. Except where applicable Data Protection Laws require an affiliate to exercise a right or seek any remedy under this DPA against us directly by itself, the parties agree that (i) solely the entity that is the contracting party to the Agreement will exercise any right or seek any remedy any Affiliate may have under this DPA , and (ii) the entity that is the contracting party to the Agreement will exercise any such rights under this DPA not separately for each affiliate individually but in a combined manner for itself and all of itsaffiliates together. The entity that is the contracting entity is responsible for coordinating all communication with us under the DPA and will be entitled to make and receive any communication related to this DPA on behalf of its affiliates.

D. Other rights. The parties agree that you will, when reviewing our compliance with this DPA pursuant to the 'Demonstration of Compliance' section, take all reasonable measures to limit any impact on us and our Affiliates by combining several audit requests carried out on behalf of the Customer entity that is the contracting party to the Agreement and all of its Affiliates in one single audit.

Exhibit 1 - Details of Processing

This Exhibit forms part of the DPA.

A. Nature and Purpose of Processing

We will Process Personal Data as necessary to provide the Services pursuant to the Agreement, as further specified in the Order Form, and as further instructed by you in your use of the Services.

B. Duration of Processing

Subject to the 'Deletion or Return of Personal Data' section of this DPA, we will Process Personal Data for the duration of the Agreement, unless otherwise agreed in writing.

C. Categories of Data subjects

You may submit Personal Data in the course of using the Service, the extent of which is determined and controlled by you in your sole discretion, and which may include, but is not limited to Personal Data relating to the following categories of Data Subjects:

Your Contacts and other end users including your employees, contractors, collaborators, customers, prospects, job applicants, suppliers, and subcontractors. Data Subjects may also include individuals attempting to communicate with or transfer Personal Data to your end users.

D. Categories of Personal Data

You may submit Personal Data to the Services, the extent of which is determined and controlled by you in your sole discretion, and which may include but is not limited to the following categories of Personal Data:

- Contact Information (such as name, home address, home telephone or mobile number, fax number, email address).

- Any other Personal Data submitted by, sent to, or received by you, or your end users, via the Service.

E. Special categories of data (if appropriate)

The parties do not anticipate the transfer of special categories of data.

F. Processing operations

Personal Data will be Processed in accordance with the Agreement (including this DPA) and may be subject to the following Processing activities:

a) Storage and other Processing necessary to provide, maintain and improve the Services provided to you; and/or

b) Disclosure in accordance with the Agreement (including this DPA) and/or as compelled by applicable laws.

Exhibit 2 - Security Measures

This Exhibit forms part of the DPA.

We currently observe the Security Measures described in this Exhibit 2. All capitalized terms not otherwise defined herein shall have the meanings as set forth in the Master Terms.

a) Access Control

i) Preventing Unauthorized Product Access

Outsourced processing: We host our Service with outsourced cloud infrastructure providers. Additionally, we maintain contractual relationships with vendors in order to provide the Service in accordance with our DPA. We rely on contractual agreements, privacy policies, and vendor compliance programs in order to protect data processed or stored by these vendors.

Physical and environmental security: We host our product infrastructure with multi-tenant, outsourced infrastructure providers. We are CSA Star Level 1 certified and we also reference SOC 2 Type II and ISO 27001 criteria in our assessments.

Authentication: We implement a uniform password policy for our customer products. Customers who interact with the products via the user interface must authenticate before accessing non-public customer data.

Authorization: Customer Data is stored in multi-tenant storage systems accessible to Customers via only application user interfaces and application programming interfaces. Customers are not allowed direct access to the underlying application infrastructure.

The authorization model in each of our products is designed to ensure that only the appropriately assigned individuals can access relevant features, views, and customization options. Authorization to data sets is performed through validating the user's permissions against the attributes associated with each data set.

Application Programming Interface (API) access: Public product APIs may be accessed using an API key or through Oauth authorization.

ii) Preventing Unauthorized Product Use

We implement industry standard access controls and detection capabilities for the internal networks that support its products.

Access controls: Network access control mechanisms are designed to prevent network traffic using unauthorized protocols from reaching the product infrastructure. The technical measures implemented differ between infrastructure providers and include

Virtual Private Cloud (VPC) implementations, security group assignment, and traditional firewall rules .

Intrusion detection and prevention: We implement a Web Application Firewall (WAF) solution to protect hosted customer websites and other internet-accessible applications. The WAF is designed to identify and prevent attacks against publicly available network services.

Static code analysis: Security reviews of code stored in our source code repositories is performed, checking for coding best practices and identifiable software flaws.

Penetration testing: We utilize OWASP-based third party scanning tools.

iii) Limitations of Privilege & Authorization Requirements

Product access: A subset of our employees have access to the products and to customer data via controlled interfaces. The intent of providing access to a subset of employees is to provide effective customer support, to troubleshoot potential problems, to detect and respond to security incidents and implement data security. Access is enabled through “just in time” requests for access; all such requests are logged.

Employees are granted access by role, and reviews of high-risk privilege grants are conducted frequently. Employee roles are reviewed at least quarterly, upon hiring, termination, or role change.

Background checks: All AMC Technology LLC employees undergo a third-party background check prior to being extended an employment offer, in accordance with and as permitted by the applicable laws. All AMC Technology LLC employees are required to conduct themselves in a manner consistent with company guidelines, non-disclosure requirements, and ethical standards.

b) Transmission Control

In-transit: We make HTTPS encryption (also referred to as SSL or TLS) available on every one of its login interfaces and for free on every customer site hosted on the AMC Technology LLC products. Our HTTPS implementation uses industry standard algorithms and certificates.

At-rest: We store user passwords following policies that follow industry standard practices for security. We have implemented technologies to ensure that stored data is encrypted at rest.

c) Input Control

Detection: We designed our infrastructure to log extensive information about the system behavior, traffic received, system authentication, and other application requests. Internal

systems aggregated log data and alert appropriate employees of malicious, unintended, or anomalous activities. Our personnel, including security, operations, and support personnel, are responsive to known incidents.

Response and tracking: We maintain a record of known security incidents that includes description, dates and times of relevant activities, and incident disposition. Suspected and confirmed security incidents are investigated by security, operations, or support personnel; and appropriate resolution steps are identified and documented. For any confirmed incidents, we will take appropriate steps to minimize product and Customer damage or unauthorized disclosure. Notification to you will be in accordance with the terms of the Agreement.

d) Availability Control

Infrastructure availability: The infrastructure providers use commercially reasonable efforts to ensure a minimum of 99.7% uptime. If you deploy an App on your infrastructure or on a third-party infrastructure, you are responsible for the availability of the App running within that infrastructure. AMC is responsible for ensuring that connections from DaVinci iPaaS are operational, but AMC is not responsible for the end-to-end connection or its configuration.

Data Backups: Backup strategies are designed to ensure redundancy protection during a significant processing failure. Customer data is backed up to multiple durable data stores and replicated across multiple availability zones.