Data Processing Addendum

Last Updated: September 15, 2024

Data Processing Addendum ("DPA" or "Data Processing Addendum") to the agreement referencing this DPA under which Aderant processes Client Personal Data ("Agreement"). This DPA is hereby incorporated into and made a part of the Agreement. In the event of a conflict between the DPA and Agreement, the terms and conditions of this DPA will prevail.

1. Definitions

Terms defined in the Agreement will, unless otherwise defined in this DPA, have the same meanings when used in this DPA. Further, the following capitalized terms used herein have the following meanings:

"Aderant" has the meaning set forth in Section 11.6.

"Applicable Data Protection Law" refers to all laws and regulations applicable to Aderant's processing of Personal Data under the Agreement.

"Client" means the customer that enters into the Agreement with Aderant.

"Client Account Data" means Personal Data that relates to Client's relationship with Aderant, including the names and contact information of the individuals authorized by Client to access Client's account and billing information of individuals that Client has associated with its account. Client Account Data also includes any data Aderant may need to collect for the purpose of identity verification (e.g., providing multi-factor authentication services) or as part of its legal obligations to maintain records.

"Client Data" means any Client-provided, non-public or proprietary information exchanged as a result of using the Service, including Client Personal Data. Client Data includes the non-public or proprietary information (including Personal Data) of Client customers for whom Client acts as a processor.

"Client Personal Data" means any Personal Data processed by Aderant on behalf of Client in connection with the Services, as furthered described in Schedule 1 attached hereto. Client Personal Data includes the Personal Data of Client's customers for whom Client acts as a processor.

"Controller" means the Client when, alone or jointly with others, it determines the purpose and means of processing Personal Data.

"Data Subject" means a natural person who can be identified, directly or indirectly.

"Personal Data" means any information relating to a natural person who can be identified, directly or indirectly.

"process" or "processing" means any operation or set of operations which is performed upon Client Data whether or not by automated means.

"Processor" means Aderant when Aderant processes Personal Data on behalf of Client.

"Security Breach" means a breach of Aderant's security resulting in the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Client Data.

"Services" has the same meaning as defined in the Agreement, or if not defined in the Agreement, the processing of Client Data by Aderant on behalf of the Client described in the Agreement.

"Subprocessor" means a processor appointed by Aderant to process Client Personal Data.

2. Instructions for Data Processing

2.1. *Generally*. The Agreement and this DPA will be the Client's instructions to Aderant for the processing of Client Data. Aderant will process Client Data solely for the purpose of providing the Services and will ensure that all individuals with access to Client Data have a duty of confidentiality with respect to that Client Data. Aderant will not sell, share, disclose, retain, or otherwise use Client Data for any other purpose unless specifically instructed by Client in writing or as required by law.

2.2. *Regulatory and Legal Compliance*. Aderant will process Client Data in compliance with Applicable Data Protection Law and provide at least the same level of privacy protection as required by Applicable Data Protection Law. Aderant will provide reasonable assistance to Client in complying with its obligations under Applicable Data Protection Law. Unless prohibited by law, Aderant will notify Client promptly of any inquiries or complaints received about the processing of Client Personal Data from regulators or law enforcement authorities. Aderant will not respond to any such inquiries or complaints except on the documented instructions of Client or as required by law. If disclosure of Client Data is required by applicable law

or a compulsory legal process, Aderant will, unless prohibited by applicable law: (a) notify Client promptly in writing before complying with any such disclosure request and provide Client an opportunity to intervene, if appropriate; and (b) disclose only the minimum amount of Client Data necessary to comply with applicable law or a compulsory legal process.

2.3. *Data Subject Rights.* Unless prohibited by law, Aderant will promptly notify Client of any request from a data subject with respect to Client Personal Data. Aderant will not respond to any data subject request without Client's prior written consent, except to confirm that the request relates to Client. Aderant will provide reasonable and timely assistance to Client in complying with its data protection obligations with respect to data subject rights under Applicable Data Protection Law.

2.4. *Additional Costs*. If any Client instructions require processing Client Data in a manner that falls outside the scope of the Services, Aderant may either (a) make the performance of any such instructions subject to the payment by Client of any costs and expenses incurred by Aderant or such additional charges as Aderant may reasonably determine; or (b) terminate the Agreement and the Services. In no event will Aderant be required to modify the SaaS Services to support Client's use in any jurisdiction that would violate Aderant policies or applicable laws.

3. Client Undertakings

Client warrants that it has provided all applicable notices and obtained all required consents required for the lawful processing of Client Data. Client has reviewed the security measures set out in Schedule 2 attached hereto and agrees that the security measures are appropriate based on the nature and sensitivity of Client Data.

4. Subprocessors

4.1. *Conditional Authorization.* Client provides a general authorization for Aderant to engage downstream Subprocessors that is conditioned on the following requirements: (a) Aderant will impose contractual data protection obligations on any Subprocessor it appoints to process Client Data to meet the standards required by Applicable Data Protection Law and this DPA; and (b) Aderant will remain liable for any breach of this DPA that is caused by an act, error, or omission of its Subprocessors as if Aderant had caused such act, error, or omission itself.

4.2. *Current Subprocessors and Notification of Changes*. Client authorizes Aderant to engage the Subprocessors listed at http://legal.aderant.com/#subprocessor-list to process Client Data. Aderant may update such list from time and will provide notice of a change to such list at least fourteen days before allowing any new Subprocessor to process Client Personal Data ("Subprocessor Notice Period"). Client may object to Aderant's appointment of a new Subprocessor during the Subprocessor Notice Period, provided such objection is in writing and based on reasonable grounds relating to data protection. In such an event, the Parties agree to discuss commercially reasonable alternative solutions in good faith. If it can be reasonably demonstrated to Aderant that the new Subprocessor is unable to process Client Personal Data in compliance with the terms of this DPA and Aderant cannot provide an alternative Subprocessor, or the Parties cannot reach a resolution within 90 days from the date of Aderant's receipt of Client's written objection, Client may discontinue the use of the affected Services with respect to those aspects of such Services which cannot be provided by Aderant without the use of the new Subprocessor by providing written notice to Aderant. Such discontinuation will be without prejudice to any fees incurred by Client prior to the discontinuation of the affected Services. If no objection has been raised during the Subprocessor Notice Period replacing or appointing a new Subprocessor, Client will be deemed to have authorized the new Sub-processor. Aderant may replace a Subprocessor at any time if the need for replacement is urgent and required for reasons beyond Aderant's reasonable control, and in such case Aderant will notify Client of the replacement Subprocessor as soon as reasonably practicable, the Subprocessor Notice Period for such replacement Subprocessor will end fourteen days from the date Aderant notifies Client of the replacement Subprocessor, and Client shall have the right to object to the replacement Subprocessor pursuant to this Section 4.2.

5. International Provisions

5.1. *Cross Border Data Transfer Mechanisms*. To the extent Client's use of the Services requires the transfer of Personal Data from a jurisdiction identified in Schedule 3 attached hereto to a location outside of that jurisdiction, the terms set forth in Schedule 3 (Cross Border Transfer Mechanisms) attached hereto will apply.

5.2. *Third Country Data*. Client shall not use or allow access to the Services in any manner that would require Client Data to be hosted in a country other than the data center location identified in the applicable Order Form (or if not identified, or outside the country of domicile of the Aderant entity that is a party to the Agreement).

6. Security Measures and Audits

6.1. *Security Measures.* Aderant will implement reasonable physical, organizational, and technical measures to protect against any unauthorized or unlawful access, processing, loss, destruction, theft, damage, use or disclosure of Client Data or systems (collectively, "Appropriate Safeguards"), including, at a minimum, the security measures set forth in Schedule 2 (*Technical and Organizational Measures*) attached hereto. These Appropriate Safeguards will be appropriate to the harm that might result from any risks to Client Data or systems and having regard to the nature of the Client Data or system which is to be protected and will take into consideration the state of the art, the costs of implementation and the nature, scope, context and purpose of the processing and the risks to the rights and freedoms of the Personal Data subjects.

6.2. *Variation of Measures*. Aderant may update Schedule 2 from time to time, provided that any such updates shall not materially diminish the overall security of the Service or Client Data.

6.3. *Compliance Review.* Aderant will cooperate with reasonable assessments by Client as to its compliance with this DPA and Applicable Data Protection Law. Client may provide a written request to Aderant to assess Aderant's compliance with the Agreement. Following receipt by Aderant of such request, Aderant and Client shall mutually agree in advance of the details of such assessment, including the reasonable start date, scope, and duration of, and security and confidentiality controls applicable to, any such assessment. Any such assessment must be conducted (a) on reasonable written notice to Aderant; (b) during Aderant's normal business hours; (c) in a manner that minimizes disruption to Aderant's business; (d) subject to a confidentiality agreement in a form such as Aderant may reasonably request; (e) in compliance with relevant policies for individuals visiting Aderant's or sub-vendors premises; and (f) at Client's expense. Aderant may charge a fee for any such assessment, provided such rates shall be reasonable, accounting for the resources expended by Aderant. Notwithstanding anything to the contrary, the assessment right provided in this Section 6.3 may be satisfied by the provision of a successful assessment result performed by an experienced, qualified independent auditor within the last 18 months. Any assessment, assessment result, and any information arising therefrom shall be considered Aderant's confidential information and may only be shared with a third party (including a third party controller) with Aderant's prior written agreement.

7. Security Breach and Response

7.1. *Breach Notification.* Aderant will promptly notify Client without undue delay and no later than 48 hours upon Aderant becoming aware of a Security Breach. Aderant will use commercially reasonable efforts to notify Client the Client Contact identified in the relevant Agreement (or address as otherwise directed by Client) if it has knowledge that there is, or reasonably believes that there has been, an actual or potential Security Breach. To the extent known, notice will include the following: (a) the nature of the Security Breach, (b) the categories and numbers of data subjects concerned, and the categories and numbers of records concerned; (c) the name and contact details of Aderant's DPO or other relevant contact from whom more information may be obtained; (d) the likely consequences of the Security Breach; and (e) the measures taken or proposed to be taken to address the Security Breach. The Parties acknowledge and agree that Aderant is subject to common, unsuccessful attempts to access its systems that do not result in any unauthorized access, use, disclosure, modification, data destruction, or interference with systems operations ("Unsuccessful Security Incidents"). Aderant hereby notifies Client of Unsuccessful Security Incidents, including without limitation ping sweeps or other common network reconnaissance techniques, attempts to log onto a system with an invalid password or username, and denial of service attacks that do not result in a server being taken offline, which may occur from time to time, and this sentence shall be deemed to meet the requirements for reporting such Unsuccessful Security Incidents under this DPA.

7.2. *Cooperation and Remediation.* Aderant will (a) cooperate with Client in the manner reasonably requested by Client and in accordance with law to investigate and resolve the Security Breach and to mitigate any harmful effects of the Security Breach; (b) promptly implement any necessary remedial measures to ensure the protection of Client Data; and (ci) document responsive actions taken related to any Security Breach.

7.3. *Information to Third Parties.* Except as required by applicable law or regulation, Aderant will not inform any third party of any Security Breach without first obtaining Client's prior written consent, other than to inform a complainant that Client will be informed of the Security Breach, and Client will have the sole right to determine whether notice of the Security Breach is to be provided to any individuals, Supervisory Authorities, regulators, law enforcement agencies, consumer reporting agencies, or others and the contents of any such notice.

7.4. *Key Contacts.* Client's key contact for notification of Security Breach is the Client primary contact identified in the applicable Order Form or as otherwise instructed in writing to Aderant. Aderant's key contact for notifications related to Security Breaches is the Director of Information Security and Privacy at data.protection@aderant.com.

8. Liability

Any exclusions or limitations of liability set out in the Agreement will apply to any losses suffered by either Party (whether in contract, tort (including negligence) or for restitution, or for breach of statutory duty or misrepresentation or otherwise) under this DPA.

9. Duration and Termination

9.1. *Return/Deletion of Client Data*. Aderant will, within 30 days of the date of termination or expiry of the Agreement: (a) if requested by Client within that period, return a copy of Client Data in such format reasonably agreed to by Aderant and Client in accordance with the Agreement; and (b) other than any Client Data retained by Aderant after termination of the Agreement in accordance with the Agreement as expressly permitted by this DPA or as required by the Standard Contractual Clauses, delete, and use all reasonable efforts to procure the deletion of all other copies of Client Data processed by Aderant or any sub-processors.

9.2. *Certification.* Upon Client's request, Aderant will promptly certify in writing to Client that it has destroyed or returned all Client Data. In the event that Aderant is unable to return or destroy all Client Data, Aderant will retain Client Data only to the extent and for such period as required by applicable laws, maintain the security and confidentiality of all such retained Client

Data in accordance with the protections of this DPA, and ensure that such Client Data is only processed as necessary for the purposes specified in the applicable laws preventing its deletion and for no other purposes.

9.3. *Compliance with this DPA.* In the event that Aderant determines that it can no longer meet its obligations under this DPA or Applicable Data Protection Law, Aderant will notify Client of that determination within 5 business days and work with Client to take reasonable and appropriate steps to stop and remediate the unauthorized use of Client Data.

10. Law and Jurisdiction

Except to the extent expressly overridden by Schedule 3, the Parties agree that the laws, jurisdictions, and venues set forth in the Agreement will also govern this DPA.

11. General

11.1. *Third Party Rights*. A person who is not a party to this DPA may not enforce any of its terms, except to the extent required by applicable law.

11.2. *Rights and Remedies*. Except as expressly provided in the Agreement, the rights and remedies provided in this DPA are in addition to, and not exclusive of, any rights or remedies provided by law.

11.3. *No Partnership or Agency*. Nothing in the DPA is intended to, or will be deemed to, establish any partnership or joint venture between any of the Parties, constitute any Party the agent of another Party, or authorize any Party to make or enter into any commitments for or on behalf of any other Party.

11.4. *Waiver*. No forbearance or delay by either Party in enforcing its rights will prejudice or restrict the rights of that Party, and no waiver of any such rights or any breach of any contractual terms will be deemed to be a waiver of any other right or of any later breach.

11.5. *Severability*. If any provision of the DPA is judged to be illegal or unenforceable, the continuation in full force and effect of the remainder of the provisions of the DPA will not be prejudiced.

11.6. *Aderant Entity.* "Aderant" means the applicable Aderant entity identified in the table below that entered into the Agreement with Client. If an Agreement specifies a different Aderant contracting entity than would otherwise apply based on Client's domicile, then Aderant shall mean the Aderant entity specified in the Agreement:

Aderant Entity	For customers domiciled in:
Aderant North America, Inc.	United States or Canada, or any other region not identified below
Aderant Legal (UK) LTD	United Kingdom, Europe (Excluding Netherlands), India, Africa, or Middle East
Hansco Automatisering B.V.	Netherlands
Aderant Legal Holdings (AUS) Pty Ltd	Australia, Japan, Singapore, or one of the ASEAN member states
Aderant Legal Holdings (NZ) ULC	New Zealand

SCHEDULE 1 TO DPA
DETAILS OF PROCESSING

1. **Categories of data subjects**

The categories of data subjects whose Personal Data are transferred: (a) employees of Clients who are natural persons, (b) customers or vendors of Client who are natural persons, (c) employees or contact persons of Client's customers and vendors

2. **Categories of Personal Data**

The transferred categories of Personal Data are: identification and contact information (e.g., *name, address, title, and contact details)* and IT information *(e.g. IP addresses)*.

3. **Special categories of Personal Data (if applicable)**

The transferred Personal Data includes the following special categories of data: Not applicable.

4. **Frequency of the transfer**

The frequency of the transfer is: continuous during the term of the Agreement.

5. **Subject matter / Purpose of the processing**

The subject matter of the processing is: providing Client with Services as described in the Agreement.

6. **Nature of the processing**

The nature of the processing is: collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, use, transmit or otherwise making available, alignment or combination, restriction, erasure or destruction, in accordance with the Agreement.

7. **Purpose(s) of the data transfer and further processing**

The purpose/s of the data transfer and further processing is/are: to provide and support Client's use of Aderant technology solutions provided under the Agreement.

8. **Duration**

The period for which the Personal Data will be retained, or, if that is not possible, the criteria used to determine that period: as set out in Section 9 of the DPA.

9. **Sub-processor (if applicable)**

See http://legal.aderant.com/#subprocessor-list

SCHEDULE 2 TO DPA
TECHNICAL AND ORGANIZATIONAL MEASURES

Description of the technical and organizational security measures implemented by the data importer / Aderant to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, as well as the risks for the rights and freedoms of natural persons.

1. **Pseudonymization and Encryption** *(Art. 32, para 1, point a GDPR)*

a. **Encryption**. Aderant encrypts Client Data at rest using AES 256-bit (or better) encryption. Aderant uses encrypted network connections or protocols (e.g., TLS 1.2, HTTPS, VPN) for Client Data in transit over untrusted networks.

b. **Key Management**. Aderant logically separates encryption keys from Client Data and encryption keys are regularly rotated.

2. **Confidentiality** (*Art 32, para 1, point b GDPR)*

a. **Confidentiality Generally**. Aderant uses measures designed to (a) prevent unauthorized persons from gaining access to Aderant systems with which Client Data are stored, processed, or used; (b) prevent systems processing Client Data from being used without authorization, (c) ensure that persons entitled to use a system that processes Client Data only have access to the data which they have a right of access, (d) prevent unauthorized reading, copying, modification, or removal of Personal Data in the course of processing or use and after storage, and (e) ensure data collected for different purposes can be processed (stored, amended, deleted, transmitted) separately.

b. **Physical Access Controls**. Aderant uses physical access control systems, such as proximity badges, at its offices. Aderant requires its cloud service providers meet industry-standard physical security controls, and Aderant regularly reviews the appropriateness of such physical controls as audited under the cloud service provider's third-party audits and certifications.

c. **System/Electronic Access Controls**. Aderant personnel access Aderant systems hosting Client Data using unique user IDs, multifactor authentication, and passwords in accordance with industry standards. Access to Client Data is restricted to Aderant personnel with a need to access such Client Data in connection with the Services or as required by law. Aderant uses an industry standard security information and event management system. Infrastructure management and configuration management tools are used for security hardening and monitoring baseline configuration standards for Aderant systems that process Client Data.

d. **Isolation/Separation Controls**. Aderant allocates permissions and privileges on a least privilege principle and assigns network and data access rights based on user group and job function. Aderant regularly reviews Aderant personnel's access privileges to Aderant systems and removes access on a timely basis for all separated personnel. Aderant logically separates Client Data from its other customers data and logically separates production environments from development environments.

3. **Integrity** *(Art 32, para 1, point b GDPR)*

a. **Encryption**. Aderant uses secure transmission between client and server and to external systems via industry-standard encryption as set forth in Section 1 above.

b. **Firewalls**. Aderant maintains firewalls and other measures to appropriately limit access to and from Aderant systems. Aderant uses industry-standard firewall or security group technologies with deny-all default policies to prevent in-bound and out-bound network protocols to Aderant systems other than those that are reasonably required to perform Services in accordance with the Agreement.

c. **Data Input Control**. Aderant uses monitoring tools to log certain activities and changes within Aderant systems. Aderant monitors these logs for abnormalities and securely stores such logs for at least one year.

d. **Anti-Malware**. Aderant maintains anti-malware controls to protect against malicious software causing accidental or unauthorized destruction, loss, alteration, disclosure, or access to Client Data.

4. **Availability and Resilience** *(Art 32 para 1 point c GDPR)*

a. **Backups**. Aderant maintains backups of Client Data stored in the primary Aderant system and maintains backups of Client Data to a secondary system on at least a daily basis.

b. **System Monitoring.** Aderant monitors Aderant systems using defined processes for security alerting, escalation, and remediation consistent with the applicable Service. Aderant uses an issue tracking system to maintain, manage, and track changes to Aderant systems. Enterprise monitoring applications are configured to monitor in-scope systems and alert operation personnel when predefined thresholds are met, and Aderant uses tools to monitor security events, latency, and network performance.

c. **Disaster Recovery and Business Continuity Plan**. Aderant maintains disaster recovery and business continuity plans designed to minimize interruption of Services. Such plan includes disaster recover incident management, procedures for

recovering access to Client Data, and periodic testing of the disaster recovery plan. Production data centers are designed to mitigate the risk of single points of failure and support service continuity and performance. Incident response procedures that outline security event response are used, and Aderant and reviews lessons learned to evaluate effectiveness of the procedures.

5. **Vulnerability Management**.

a. **Vulnerability Detection**. Vulnerabilities meeting defined risk criteria trigger alerts and are prioritized for remediation based on the potential impact to Services. Aderant maintains standard patch management processes for Aderant systems to protect against security vulnerabilities.

b. **Risk Assessments**. Aderant performs an annual security operational risk assessment of Aderant systems processing Client Data. Results from risk assessment activities are documented in a risk register and prioritized for treatment by risk level. Aderant performs risk-based control monitoring throughout the year by performing control testing using a formal methodology. The testing results are documented and reviewed by management, including remediation plans for identified observations.

6. **Data Governance and Management**.

a. **Information Security Plan**. Aderant maintains a comprehensive, documented information security program designed to protect Client Data against unauthorized or accidental destruction, loss, alteration, disclosure, or access. Aderant maintains commercially reasonable controls for information governance and data management.

b. **Security Officer**. Aderant has appointed one or more security officers to coordinate information security and monitor information security rules and procedures.

7. **Personnel**.

a. **Roles and Responsibilities**. Aderant maintains written policies defining the roles and responsibilities of Aderant personnel with access to Client Data.

b. **Policies.** Aderant requires criminal background screening of Aderant employees as part of its hiring process, to the extent permitted by law.

c. **Confidentiality.** Aderant ensures that Aderant personnel authorized to access Client Data are bound to confidentiality obligations or under appropriate statutory obligations of confidentiality.

d. **Training**. Aderant maintains an information security training and awareness program for Aderant personnel and requires Aderant personnel to complete such training annually.

8. **Data Minimization, Quality, and Portability**

a. **Data Minimization, Quality, and Portability**. Aderant will use reasonable efforts to use only the minimum necessary Personal Data in the performance of Services. As part of SaaS Services, Client may access, amend, delete, and extract Client Data within the applicable SaaS Services to assist Client with its data quality, minimization, and portability efforts.

b. **Data Destruction.** Aderant ensures that residual magnetic, optical, physical, or electrical representations of Personal Data that have been deleted may not be retrieved or reconstructed when storage media is transferred, becomes obsolete, or is no longer usable or required by Aderant. Personal Data stored on Aderant media (e.g., hard drive, digital media, tapes) must be rendered unreadable using the NIST Guidelines for Media Sanitization prior to the media being disposed of or moved off site.

9. **Testing, Assessing, and Evaluating the Technical and Organization Measures** *(Art. 32 para 1 point D GDPR)*. Aderant follows measures to regularly review and assess its technical and organizational measures.

a. **Internal Assessments**. Aderant internal resources review Aderant's information security practices on an annual basis.

b. **Vulnerability Testing**. Aderant conducts vulnerability testing on Aderant systems in accordance with Section 5 above.

c. **Penetration Testing**. Aderant engages an independent third-party organization to perform penetration testing of Aderant systems annually.

d. **Business Continuity**. Aderant tests its business continuity and disaster response plan annually.

10. **Data Subject Requests** *(Clause 10(b) SCC).* During the applicable SaaS Services term, Client may access, extract, and delete Client Data from the SaaS Services in accordance with the Documentation to respond to data subjects' requests to exercise one or more of their rights available under Applicable Data Protection Laws.

SCHEDULE 3 TO DPA
CROSS BORDER TRANSFER MECHANISMS

1. **Definitions.**
"**EEA**" means the European Economic Area.

"**EU Standard Contractual Clauses**" means the Standard Contractual Clauses approved by the European Commission in decision 2021/914.

"**UK International Data Transfer Agreement**" means the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses issued by the UK Information Commissioner, Version B1.0, in force 21 March 2022.

2. **Applicability.** This Schedule will apply when Client's use of the Services requires the transfer of Personal Data from the EEA, the United Kingdom, or Switzerland to another jurisdiction.

3. **Cross Border Data Transfer Mechanisms.**

3.1. *Order of Precedence*. In the event the Services are covered by more than one Transfer Mechanism, the transfer of Personal Data will be subject to a single Transfer Mechanism in accordance with the following order of precedence: (a) the EU Standard Contractual Clauses as set forth in Section 3.2 (EU Standard Contractual Clauses) of this Schedule; (b) the UK International Data Transfer Agreement as set forth in Section 3.3 (UK International Data Transfer Agreement) of this Schedule; and, if neither (a) nor (b) is applicable, then (c) other applicable data Transfer Mechanisms permitted under Applicable Data Protection Law.

3.2. *EU Standard Contractual Clauses*. The Parties agree that the EU Standard Contractual Clauses will apply to Personal Data that is transferred via the Services from the EEA or Switzerland, either directly or via onward transfer, to any country or recipient outside the EEA or Switzerland that is not recognized by the European Commission (or, in the case of transfers from Switzerland, the competent authority for Switzerland) as providing an adequate level of protection for Personal Data. For data transfers from the EEA that are subject to the EU Standard Contractual Clauses, the EU Standard Contractual Clauses will be deemed entered into (and incorporated into this DPA by this reference) and completed as follows:

(a) Module One (Controller to Controller) of the EU Standard Contractual Clauses will apply where Aderant is processing Client Account Data;

(b) Module Two (Controller to Processor) of the EU Standard Contractual Clauses will apply where Client is a Controller of Client Data and Aderant is processing Client Data;

(c) Module Three (Processor to Processor) of the EU Standard Contractual Clauses will apply where Client is a processor of Client Data and Aderant is processing Client Data on behalf of Client;

(d) Module Four (Processor to Controller) of the EU Standard Contractual Clauses will apply where Client is a Processor of Client Data and Aderant processes Client Account Data; and

(e) For each Module, where applicable:

i. in Clause 7 of the EU Standard Contractual Clauses, the optional docking clause will not apply;

ii. in Clause 9 of the EU Standard Contractual Clauses, Option 2 will apply and the time period for prior written notice of sub-processor changes will be as set forth in Section 4.2 (Current Sub-processors and Notification of Sub-processor Changes) of this DPA;

iii. in Clause 11 of the EU Standard Contractual Clauses, the optional language will not apply;

iv. in Clause 17 (Option 1), the EU Standard Contractual Clauses will be governed by Irish law;

v. in Clause 18(b) of the EU Standard Contractual Clauses, disputes will be resolved before the courts of Ireland;

vi. in Annex I, Part A of the EU Standard Contractual Clauses:

- Data Exporter: Client
- Data Exporter Contact details: Set forth in Section 7.4 of the DPA
- Data Exporter Role: Controller
- Signature and Date: By entering into the Agreement, Data Exporter is deemed to have signed these EU Standard Contractual Clauses incorporated herein, including their Annexes, as of the effective date of the Agreement.
- Data Importer: Aderant
- Data Importer Contact details: Set forth in Section 7.4 of the DPA
- Data Importer Role: Processor

- Signature and Date: By entering into the Agreement, Data Importer is deemed to have signed these EU Standard Contractual Clauses, incorporated herein, including their Annexes, as of the effective date of the Agreement;

vii. in Annex I, Part B of the EU Standard Contractual Clauses:
- The categories of data subjects are located in Section 1 of Schedule 1
- The Sensitive Data transferred are located forth in Section 3 of Schedule 1
- The frequency of the transfer is a continuous basis for the duration of the Agreement
- The nature of the processing is located in Section 6 of Schedule 1.
- The purpose of the processing is located in Section 7 of Schedule 1
- The period for which the Personal Data will be retained is located in Section 8 of Schedule 1
- For transfers to sub-processors, the subject matter, nature, and duration of the processing are located in Schedule 2.
- in Annex I, Part C of the EU Standard Contractual Clauses: The Irish Data Protection Commission will be the competent supervisory authority; and

viii. Schedule 3 (Technical and Organizational Security Measures) of this DPA serves as Annex II of the EU Standard Contractual Clauses.

ix. Notwithstanding anything to the contrary, in the event of a conflict between Clause 12 of the EU Standard Contractual Clauses and Section 8 of the DPA, Clause 12 will prevail.

3.3. *UK International Data Transfer Agreement*. The Parties agree that the UK International Data Transfer Agreement will apply to Personal Data that is transferred via the Services from the United Kingdom, either directly or via onward transfer, to any country or recipient outside of the United Kingdom that is not recognized by the competent United Kingdom regulatory authority or governmental body for the United Kingdom as providing an adequate level of protection for Personal Data. For data transfers from the United Kingdom that are subject to the UK International Data Transfer Agreement, the UK International Data Transfer Agreement will be deemed entered into (and incorporated into this DPA by this reference) and completed as follows:

(a) In Table 1 of the UK International Data Transfer Agreement, the Parties' details and key contact information is located in Section 3.3 (e)(vi) of this Schedule 3.

(b) In Table 2 of the UK International Data Transfer Agreement, information about the version of the Approved EU SCCs, modules and selected clauses which this UK International Data Transfer Agreement is appended to is located in Section 3.2 (EU Standard Contractual Clauses) of this Schedule 5.

(c) In Table 3 of the UK International Data Transfer Agreement:
- The list of Parties is located in Section 3.2(e)(vi) of this Schedule 3.
- The description of the transfer is located in Sections 6 and 7 (Nature and Purpose of the Processing) of Schedule 2 (Details of the Processing).
- Annex II is located in Schedule 2 (Technical and Organizational Security Measures)
- The list of sub-processors is set forth in Schedule 1 of this DPA.

(d) In Table 4 of the UK International Data Transfer Agreement, both the Importer and the exporter may end the UK International Data Transfer Agreement in accordance with the terms of the UK International Data Transfer Agreement.

3.4. *Conflict*. To the extent there is any conflict or inconsistency between the EU Standard Contractual Clauses or UK International Data Transfer Agreement and any other terms in this DPA, the Agreement, or the Aderant Privacy Notice, the provisions of the EU Standard Contractual Clauses or UK International Data Transfer Agreement, as applicable, will prevail.