ARCHIPELAGO ANALYTICS, INC.
DATA PROCESSING AGREEMENT

Effective Date: November 1, 2021

The Parties have entered into a Master Subscription Agreement whereby the Customer subscribes to the Archipelago Analytics, Inc. ("**Company**") SaaS service and/or other Company services (the "**Agreement**"). This Data Processing Agreement forms part of the Agreement. To the extent that the Company processes any personal data as a processor (as defined below) on behalf of the Customer (or, where applicable, Customer Affiliates) in connection with the provision of the Services, and where that personal data falls within the scope of the GDPR (and/or, if applicable the UK GDPR and/or the Swiss Data Protection Laws as defined in Schedule 6 of the DPA), the Parties have agreed that it shall do so pursuant to the terms of this DPA.

1. DEFINITIONS

1.1 Terms defined in the Agreement agreed by Company and Customer shall, unless otherwise defined in this DPA, have the same meanings when used in this DPA, and the following terms used in this DPA shall be defined as follows:

"Customer Affiliate" means an entity controlled by, controlling, or under common control with the Customer, where "control" means ownership of more than fifty percent (50%) of such entity's voting shares or equivalent;

"**Customer Personal Data**" means the personal data (as defined in the GDPR) processed by the Company on behalf of the Customer in connection with the provision of the Services, as further described in Schedule 2;

"**Data Processing Agreement**" or "**DPA**" means this Data Processing Agreement, including its Schedules;

"**EEA**" means the European Economic Area;

"**GDPR**" means Regulation (EU) 2016/679 (the "**EU GDPR**") or, where applicable, the "**UK GDPR**" as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the UK European Union (Withdrawal) Act 2018 or, where applicable, (the equivalent provision under) Swiss Data Protection Laws as defined in Schedule 6;

"Losses" means any demand, contribution, claim, action, proceeding, liability, loss, damage, costs, expenses and charges;

"**Member State**" means a member state of the EEA, being a member state of the European Union, Iceland, Norway, or Liechtenstein;

"**Standard Contractual Clauses**" or "**SCCs**" means Module Two (*controller to processor*) of the Standard Contractual Clauses annexed to Commission Implementing Decision (EU) 2021/914 which are set out at Schedule 5 of this DPA.

"**Sub-processor**" means a processor appointed by the Company to process Customer Personal Data.

1.2 The terms "**personal data**", "**controller**", "**processor**", "**data subject**", "**process**", "**personal data breach**" and "**supervisory authority**" shall have the same meaning as set out in the GDPR.

1.3 The terms "**data exporter**" and "**data importer**" shall have the same meaning as set out in the SCCs.

2. INTERACTION WITH THE AGREEMENT

2.1 This DPA supplements the Agreement with respect to any processing of Customer Personal Data by the Company, and the Parties agree that this DPA shall, by default, be concluded between Company (as data importer under the SCCs) and Customer as well as any Customer Affiliate, directly or indirectly, bound by the Agreement (respectively as data exporter under the SCCs).

2.2 The Customer warrants that, with respect to the Customer Affiliates directly or indirectly bound by the Agreement, it is duly authorised to conclude this DPA for and on behalf of any such Customer Affiliates, and that each Customer Affiliate that transfers Customer Personal Data to the Company shall be bound by the terms of this DPA as if they were the Customer. Where the Customer may not be duly authorized to conclude the DPA for and on behalf of a Customer Affiliate, Customer warrants that such Customer Affiliate will submit to the Company without delay a signed copy of this DPA which shall have the same effect as the signature of Customer on behalf of a Customer Affiliate. Customer shall be responsible for ensuring that all the information necessary to complete Schedule 1 as to itself and Customer Affiliates is provided to the Company, failing which the Customer shall ensure that the Customer or Customer Affiliate's personal data is not transferred to Company.

2.3 The Customer warrants that it is duly mandated by any Customer Affiliates on whose behalf the Company processes Customer Personal Data in accordance with this DPA to:

(a) enforce the terms of this DPA on behalf of the Customer Affiliates, and to act on behalf of the Customer Affiliates in the administration and conduct of any claims arising in connection with this DPA; and

(b) receive and respond to any notices or communications under this DPA on behalf of Customer Affiliates.

2.4 The Parties agree that any notice or communication sent by the Company to the Customer shall satisfy any obligation to send such notice or communication to a Customer Affiliate.

2.5 As explicitly allowed by Clause 2(a) of the SCCs, Sections 1 through 14 of this DPA supplement the SCCs, in particular, by way of providing guidance for their practical implementation and are not intended to contradict, directly or indirectly, any clauses of the SCCs nor lessen the protection offered by the SCCs to data subjects. In the event of any conflict among contractual documents, the order of prevalence shall be as follows (in accordance with Clause 5 SCCs):

(a) the SCCs (or, with respect to transfers of Customer Personal Data subject to the UK GDPR, the SCCs as amended by clause 11**Error! Unknown switch argument.**, or, with respect to transfers of Customer Personal Data subject to the Swiss Data Protection Laws, the SCC as amended by the terms set out at Schedule 5 if applicable);

(b) the Schedules of this DPA to the extent that they are meant to complete the SCCs;

(c) the main body of this DPA;

(d) the Agreement and any other contractual documents.

3. STANDARD CONTRACTUAL CLAUSES

3.1 Subject to clause 3.3, the SCCs shall apply to any transfers of Customer Personal Data from the Customer and Customer Affiliates (respectively as data exporter) to the Company (as data importer) where such processing of which is governed by the GDPR.

3.2 For the purposes of the SCCs:

(a) Annex I.A (*List of Parties*) of the SCCs shall be deemed to incorporate the information in Schedule 1;

(b) Annex I.B (*Description of Transfer*) of the SCCs shall be deemed to incorporate the information in Schedule 2;

(c) Annex I.C (*Competent Supervisory Authority*) of the SCCs shall be deemed to refer to the supervisory authority respectively identified in Schedule 1;

(d) Annex II (*Technical and Organisational Measures*) of the SCCs shall be deemed to incorporate the information in Schedule 4.

3.3 With respect to any transfers of Customer Personal Data falling within the scope of the UK GDPR from the Customer and Customer Affiliates (respectively as data exporter) to the Company (as data importer):

(a) neither the SCCs nor the DPA shall be interpreted in a way that conflicts with rights and obligations provided for in any laws relating to data protection, the processing of personal data, privacy and/or electronic communications in force from time to time in the UK, including the UK GDPR and the Data Protection Act 2018 (together, the "**UK Data Protection Laws**");

(b) the SCCs are deemed to be amended to the extent necessary so they operate:

(i) for transfers made by the Customer and Customer Affiliates to the Company, to the extent that UK Data Protection Laws apply to the Customer's processing when making that transfer;

(ii) to provide appropriate safeguards for the transfers in accordance with Article 46 of the UK GDPR;

(c) the amendments referred to in clause 3.3(b) include (without limitation) the following:

(i) references to "Regulation (EU) 2016/679" or "that Regulation" are replaced by "UK GDPR" and references to specific Article(s) of "Regulation (EU) 2016/679" are replaced with the equivalent Article of the UK GDPR;

(ii) references to Regulation (EU) 2018/1725 are removed;

(iii) references to the "Union", "EU" and "EU Member State" are all replaced with the "UK";

(iv) the "competent supervisory authority" shall be the Information Commissioner;

(v) clause 17 of the SCCs is replaced with the following:

"*These Clauses are governed by the laws of England and Wales*";

(vi) clause 18 of the SCCs is replaced with the following:

"Any dispute arising from these Clauses shall be resolved by the courts of England and Wales. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of any country in the UK. The Parties agree to submit themselves to the jurisdiction of such courts";

(vii) any footnotes to the SCCs are deleted in their entirety.

3.4 With respect to any transfers of Customer Personal Data falling within the scope of the Swiss Data Protection Laws from the Customer and Customer Affiliates (respectively as data exporter) to the Company (as data importer) the terms set out at Schedule 6 shall apply.

4. INSTRUCTIONS FOR DATA PROCESSING

4.1 The Parties agree that, for the purposes of clause 8.1(a) of the SCCs, the terms of the Agreement, this DPA, and any additional instructions provided by Customer in writing in conformity with the terms of the Agreement, constitute Customer's instructions for the processing of Customer Personal Data.

4.2 To the extent that any of the Customer's instructions require processing of Customer Personal Data in a manner that falls outside the scope of the Services, the Company may:

(a) make the performance of any such instructions subject to the payment by the Customer of any costs and expenses incurred by the Company or such additional charges as the Company may reasonably determine; or

(b) terminate the Agreement and the Services.

4.3 Notwithstanding clause 8.1 of the SCCs, the Company may process Customer Personal Data to the extent required by applicable law in the EEA or a Member State, the UK, or Switzerland, in each case to which the respective processing of Customer Personal Data is subject, and the Company shall, to the extent permitted by such applicable law, inform the Customer of that legal requirement before processing that Customer Personal Data.

5. CUSTOMER WARRANTIES AND UNDERTAKINGS

The Customer represents and warrants that:

(a) it has provided all required notices to data subjects and, to the extent required by applicable law, including the GDPR, obtained consent from data subjects for the lawful processing of Customer Personal Data in accordance with the Agreement and this DPA;

(b) without prejudice to the generality of clause 8 of the SCCs (as applicable), taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the security measures set out in Schedule 4 are:

(i) appropriate to ensure the security of the Customer Personal Data, including protection against a personal data breach; and

(ii) otherwise consistent with the Customer's obligations under Article 32 of the GDPR.

6. SUB-PROCESSORS

6.1 Parties agree that, in accordance with option 2 of Clause 9 of the SCCs, the Customer gives the Company general authorisation to engage sub-processors from the agreed list referred to in Schedule 3.

6.2 In order to fulfil its obligation under option 2 of Clause 9(a) SCC, the Company shall provide the Customer with 30 days' notice of any proposed changes to the sub-processors it uses to process Customer Personal Data (including any addition or replacement of any sub-processors), including any information reasonably necessary to enable the Customer to exercise its right to object.

6.3 If the Customer objects to the Company's use of a new sub-processor (including when exercising its right to object under option 2 of clause 9(a) of the SCC), it shall provide the Company with:

(a) written notice of the objection within 10 days after the Company has provided notice to the Customer as described in clause 7.2; and

(b) documentary evidence that reasonably shows that the sub-processor does not or cannot comply with the requirements in this DPA,

(an "**Objection**").

6.4 In the event of an Objection, the Company will use reasonable endeavours to work with Customer to address the issues raised in the objection or will recommend a commercially reasonable alternative to prevent the applicable sub-processor from processing the Customer Personal Data which Company may consider.

6.5 If the Parties are unable to agree on an alternative in accordance with clause 6.4 within a reasonable period of time, which shall not exceed 60 days from the date when the objection was raised, either Party may terminate the Agreement by providing not less than 30 days' written notice to the other Party. During such notice period, the Company may suspend the affected portion of the Services.

6.6 In accordance with Clause 9(b) SCC, any sub-processor is obliged before initiating the processing, to commit itself by way of written contract to comply with, in substance, the data protection obligations no less protective those set out in the SCCs.

7. SECURITY AND AUDITS

7.1 With respect to any audits conducted under clauses 8.9(c) and (d) of the SCC, the Parties agree that all such audits shall be conducted:

(a) on reasonable written notice to the Company;

(b) only during the Company's normal business hours; and

(c) in a manner that does not disrupt the Company's business;

7.2 The Customer (or, where applicable, a third party independent auditor appointed by the Customer) shall:

(a) enter into a confidentiality agreement with the Company prior to conducting the audit in such form as the Company may request; and

(b) ensure that its personnel comply with the Company's and any sub-processor's policies and procedures when attending the Company's or sub-processor's premises, as notified to the Customer by the Company or sub-processor.

8. COSTS

The Customer shall pay to the Company on demand all costs, including reasonable labour costs calculated on a time-spent basis and expenses incurred by the Company in connection with:

(a) implementing any modifications to the delivery of the Services pursuant to the process set out under clause 6;

(b) facilitating and contributing to any audits of the Company under or clauses 8.9(c) and (d) of the SCCs;

(c) facilitating and contributing to any audits of the Customer conducted by a supervisory authority;

(d) responding to queries or requests for information from the Customer relating to the processing of Customer Personal Data under clauses 8.9(a), (c) or (e) of the SCCs;

(e) any assistance provided by the Company to the Customer with its fulfilment of its obligations to respond to data subjects' requests for the exercise of their rights under the GDPR and under clauses 10(a), (b) or (c) of the SCCs; and

(f) any assistance provided by the Company to the Customer with any data protection impact assessments or prior consultation with any supervisory authority of the Customer.

9. LIABILITY

9.1 Subject to clause 9.2, any exclusions or limitations of liability set out in the Agreement shall 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.

9.2 Nothing in this DPA or the Agreement shall limit or exclude any liability of either Party pursuant to clause 12 of the SCCs.

10. DURATION AND TERMINATION

The duration of this DPA shall be the same as that of the Agreement, subject to application of the SCCs, in particular clause 8.5. The DPA will commence upon commencement of the Services under the Agreement, unless otherwise stipulated herein.

11. MODIFICATIONS

Company may modify or supplement this DPA, with notice to Customer, (i) if required to do so by a supervisory authority or other government or regulatory entity, (ii) if necessary to comply with applicable law, (iii) to implement amended standard contractual clauses laid down by the European Commission or (iv) to adhere to a code of conduct or certification mechanism approved or certified pursuant to Art. 40, 42 and 43 of the GDPR. Customer shall notify Company if it does not agree to a modification no more than thirty (30) days following the effective date of the modification, in which case Company may terminate this DPA and the Agreement with thirty (30) days prior notice, whereby in the case of an objection not based on non-compliance of the modifications with applicable data protection law, Company shall remain entitled to its agreed remuneration until the end of the original term of the Agreement.

12. LAW AND JURISDICTION

12.1 Notwithstanding the provisions of the Agreement, this DPA and the SCCs (pursuant to its Clause 17) shall be governed by and construed in accordance with:

(a) to the extent that the EU GDPR applies to the processing of Customer Personal Data, the law of the Member State in which the Customer is established, provided such Member State law allows for third-party beneficiary rights; otherwise, the law of the Netherlands;

(b) to the extent that UK Data Protection Laws apply to the processing of Customer Personal Data, the law of England and Wales;

(c) to the extent that Swiss Data Protection Laws apply to the processing of Customer Personal Data, the law of Switzerland.

12.2 Notwithstanding the provisions of the Agreement, as regards to this DPA and the SCCs (pursuant to its Clause 18), the Parties submit themselves to the jurisdiction of the following courts:

(a) to the extent that the EU GDPR applies to the processing of Customer Personal Data, the courts of the Member State in which the Customer is established; otherwise, the courts of the Netherlands;

(b) to the extent that UK Data Protection Laws apply to the processing of Customer Personal Data, the courts of England and Wales;

(c) to the extent that Swiss Data Protection Laws apply to the processing of Customer Personal Data, the courts of Switzerland.

SCHEDULE 1

PARTIES TO THE PROCESSING

1. Relevant Information on Company / data importer and Customer / data exporter

Party:	**Customer / data exporter**	**Company / data importer**
Role	**Controller**	**Processor**
Contact	Customer Contact details as set out in the Master Subscription Agreement	Name: Archipelago Analytics, Inc. (Company) Contact details as set out in the Master Subscription Agreement
Where applicable: Data protection officer and/or UK representative	As set out in Customer privacy notice	As set out in Company privacy notice
Where applicable: Data protection officer and/or EU representative	As set out in Customer privacy notice	As set out in Company privacy notice
Activities relevant to the data transferred	Use of Services	Provision of Services (as defined in the Agreement)
Competent supervisory authority	To the extent that the EU GDPR applies and the competent supervisory authority is not explicitly stipulated herein, the text set out in Footnote 1 shall be incorporated herein.[1]]	n/a

1 Each supervisory authority of the EU and EEA is competent for the performance of the tasks assigned to and the exercise of the powers on the territory of its own Member State. A list of the supervisory authorities across the European Union and EEA can be found under the following link: https://edpb.europa.eu/about-edpb/about-edpb/members_en

As to Germany, the supervisory authority mentioned under the aforementioned link called "Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit" is responsible for supervising public authorities of the federal government, public-sector companies, insofar as they participate in the competition, and companies which process data from natural and legal persons in order to commercially provide telecommunication services while the responsibility for supervision does not already come from Section 115 para 4 of the Telecommunication Act ("Telekommunikationsgesetzes"). Additionally, there is also a supervisory authority in each federal state ("Bundesland") in Germany which is responsible for private entities established in its respective federal state. Please find a list of these German supervisory authorities under the following link: https://www.bfdi.bund.de/DE/Service/Anschriften/Laender/Laender-node.html;jsessionid=1D7E492F9E963C3ADC18161A232AADBD.intranet241

Where the data exporter is established in an EU Member State: The competent supervisory authority is the one at the establishment of the data exporter.

	[To the extent that UK Data Protection Laws apply to the Customer's processing: The Information Commissioner]	

2. Relevant Information of Customer Affiliates – To be completed by Customer as applicable and submitted to Company

Customer Affiliate	***[complete for each Affiliate]*** Name: [***] Address: [***]
Role	**Controller**
Contact person	Name: [***] Position: [***] Contact details: [***]
Where applicable: Data protection officer and/or UK representative	[***]
Where applicable: Data protection officer and/or EU representative	[***]
Activities relevant to the data transferred	[***]
Competent supervisory authority	[***] [To the extent that the EU GDPR applies and the competent supervisory authority is not explicitly stipulated herein, the text set out in Footnote 1 shall be incorporated herein.] [To the extent that UK Data Protection Laws apply to the Customer Affiliate's processing: The Information Commissioner]

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of the GDPR in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of the GDPR: The competent supervisory authority is the one of the Member State in which the representative is established.

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of the GDPR in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of the GDPR: The competent supervisory authority is the supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behavior is monitored, are located.

SCHEDULE 2

DETAILS OF PROCESSING

1. Categories of data subjects

The categories of data subjects whose personal data may be transferred:

- Prospects, customers, business partners, and vendors of the data exporter (who are physical persons)
- Employees, contractors, affiliates, agents, advisors, and contact persons *of data exporter customers, business partners, and vendors*
- Employees, agents, advisors, and contractors *of data exporter* (who are physical persons)
- Data exporters end users and authorized by data exporter to use the Service

2. Categories of personal data

The transferred categories of personal data may include:

- Name, address and email address, job title
- Employer
- Employee ID data
- Biographical information excluding special category data
- Localization data

3. Special categories of personal data (if applicable)

The transferred personal data includes the following special categories of data:

- None

4. Frequency of the transfer

The frequency of the transfer is:

- Throughout the duration of the Agreement

5. Subject matter of the processing

The subject matter of the processing is:

- Customer employee data: to manage relationship with Customer and related to the performance of the Agreement
- Customer and/or Customer's Users and Customer's service provider's personal data: incidental processing related to the provision of the Services as set out in the Agreement

6. Nature of the processing

The nature of the processing is:

- transfer (by data exporter), recording, storage, erasure, and onward transfer

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

The purpose/s of the data transfer and further processing is/are:

- performance of the Services as described in 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 stated in the Agreement.

9. Sub-processor (if applicable)

As set out in Schedule 3

SCHEDULE 3

SUBPROCESSORS

List of Company of sub-processors available at:

https://www.onarchipelago.com/customers/subprocessors

SCHEDULE 4

TECHNICAL AND ORGANISATIONAL MEASURES

This Schedule 4 sets forth the Company's security principles and architecture with respect to the administrative, technical, and physical controls applicable to the Service. Capitalized terms in this attachment shall have the meaning assigned to them in the Agreement unless otherwise defined herein.

1. Principles.

The following principles guide the Company's design and implementation of its security program and practices: (a) physical and environmental security to protect the Services against unauthorized access or use; (b) maintenance of availability for operation and use of the Services; (c) confidentiality to protect Customer Personal Data; and (d) integrity to maintain the integrity of data maintained in the Services.

2. Security Program.

The Company maintains an information security program, which includes: (a) a formal risk management program; (b) periodic risk assessments of systems and networks that process Customer Personal Data conducted on at least an annual basis; (c) monitoring for security incidents and maintenance of a tiered remediation plan to implement timely fixes to discovered vulnerabilities; (d) a written information security policy and incident response plan in furtherance of the security, confidentiality, integrity, and availability of Customer Personal Data.

3. Data Centers.

The Company currently uses Amazon Web Services (AWS) to provide management and hosting of production servers and databases. AWS employs a robust physical security program with multiple certifications, including SSAE 16 and ISO 27001 certification. For further details of these controls please visit: https://aws.amazon.com/compliance/data-center/controls/.

4. Access, Controls, and Policies.

Access to manage the Company's AWS environment requires multi-factor authentication, ssh access to the Services is logged, and access to Customer Personal Data is restricted to a limited set of approved Company personnel. All personnel with access to Customer Personal Data have passed background checks. Personnel are trained on documented information security and privacy procedures. Access to the Company's AWS environment must be requested with a valid business reason / job duty responsibility and subject to approval by authorized personnel. Access is promptly revoked upon termination of employment or change of duties.

AWS networking features, such as security groups, are leveraged to restrict access to AWS instances and resources and are configured to restrict access using the principle of least privilege.

For support and onboarding purposes, the Company application implements a role-based access control model allowing varying levels of access and explicit grants of access to Customer Personal Data for support and onboarding purposes. All access is logged.

All Customer Personal Data onboarding activity managed by the Company on the customer's behalf is project managed and executed through an onboarding job application that allows an assigned data engineer to propose changes that are then reviewed and approved by a data manager before going live. An audit trail of changes is recorded.

5. Capture of Personal Data

The Company aims to capture the minimal personally identifiable information about its users in order to provide support for application functionality, analytics on application use, and communication.

The Company utilizes a robust third party identity service, currently Auth0, for user authentication and profile services. User profile data is stored in our Auth0 tenant instance. Privileged application roles are recorded in the Company database by email. Auth0 provides logging and user lifecycle capabilities such as automated and manual blocking.

6. **Encryption.**

Customer Personal Data remains encrypted at rest and the connection to platform.onrchipelago.com is encrypted with 256-bit encryption and supports TLS 1.2 and annual key rotation. Logins and sensitive data transfer are performed over encrypted protocols such as TLS or SSH.

7. Isolation / Separation

The Company application follows standard multi-tier web application architecture with the main web application being delivered and executed within the user's web browser. This connects to a load balanced API tier over SSL. The API tier connects to the data tier over SSL. The minimal access required between tiers is enforced utilizing standard AWS features.

Code deployment and infrastructure management follows CI / CD best practices. All changes are peer reviewed and tested prior to code merge. The production release process is fully automated taking an existing certified build from the staging environment and deploying this to production after an approval action performed by authorized personnel.

8. Backup and Restoration.

The Company utilizes a two-tier strategy for database backups. First, the native AWS RDS backup and restore capability is utilized which performs automated daily snapshots and retains database logs in addition to enable near real time point in time restore. In addition, a second logical backup is scheduled daily which saves the data to an encrypted private S3 bucket. The database is configured with multiple availability zones and configured for automated failover to a standby in the event of primary database or AWS availability zone failure.

9. Vendor Management.

The Company takes reasonable steps to select and retain only third-party service providers that will maintain and implement the security measures consistent with the measures stated herein. Before software is implemented or a software vendor can be used at the Company, the Company security reviews the vendor's security policies, certifications, protocols, and security track record. Company security may reject use of any software or software vendor for failure to demonstrate the ability to sufficiently protect the Company's data and Users.

10. Security Incident Response.

The Company maintains an incident response plan designed to establish a reasonable and consistent response to security incidents and suspected security incidents involving the accidental or unlawful destruction, loss, theft, alteration, unauthorized disclosure of, or access to, Customer Personal Data transmitted, stored, or otherwise processed by the Company.

11. Antivirus and Security Scans.

Anti-virus or anti-malware applications have been installed to detect or prevent unauthorized or malicious software. The Company runs security scans on a regular basis. For virus monitoring, the Company automatically or manually updates most software it runs and outsources to AWS when logical and possible. The Company maintains a vulnerability scanning process for production systems. The scope of vulnerability scans includes both external and internal systems in the production environment. The Company's security team performs vulnerability scans at least quarterly and determines a severity rating for each vulnerability based on the assessment tools criteria such that high or higher-level ranked vulnerabilities require remediation Vulnerability scans are also run after any significant change to the production environment as determined by the Company security team. A third party penetration test is run at least annually and identified vulnerabilities are resolved according to priority and severity.

12. Change Management.

The Company has established a change management policy to ensure changes meet the Company's security, confidentiality, and availability goals. Management reviews and approves the policy annually. Any change to production or IT configuration with unknown or foreseeable security consequences must be reviewed by the relevant teams holding the area of responsibility ("AoR") prior to deployment.

The Company reserves the right to update this document from time to time and modify its security practices, provided that such update or modification will not materially and adversely diminish the overall security of the Services during the customer's Subscription Term.

SCHEDULE 5

STANDARD CONTRACTUAL CLAUSES GOVERNING TRANSFERS OF CUSTOMER PERSONAL DATA

MODULE TWO: Transfer controller to processor

SECTION I

Clause 1 Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 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) (1) for the transfer of personal data to a third country.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter 'entity/ies') transferring the personal data, as listed in Annex I.A (hereinafter each 'data exporter'), and

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A (hereinafter each 'data importer')

have agreed to these standard contractual clauses (hereinafter: 'Clauses').

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2 Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3 Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii) Clause 8: Clause 8.1(b), 8.9(a), (c), (d) and (e);

(iii) Clause 9 – Clause 9(a), (c), (d) and (e);

(iv) Clause 12 – Clause 12(a), (d) and (f);

(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e);

(viii) Clause 18 –Clause 18(a) and (b);

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4 Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.
(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.
(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5 Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6 Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

SECTION II – OBLIGATIONS OF THE PARTIES

8.1 Instructions

(a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.
(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data

processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter 'personal data breach'). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and

offences (hereinafter ‘sensitive data’), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (4) (in the same country as the data importer or in another third country, hereinafter ‘onward transfer’) if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter’s request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

(d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9 Use of sub-processors

(a) The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least 30 days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. (8) The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10 Data subject rights

(a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

Clause 11 Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12 Liability

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.

(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13 Supervision

(a) The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees

to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:
(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;
(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards (12);
(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it

concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15 Obligations of the data importer in case of access by public authorities

15.1 Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16 Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:
(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;
(ii) the data importer is in substantial or persistent breach of these Clauses; or
(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.
In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17 Governing law
These Clauses shall be governed by the law of the EU Member State in which the data exporter is established. Where such law does not allow for third-party beneficiary rights, they shall be governed by the law of another EU Member State that does allow for third-party beneficiary rights. The Parties agree that this shall be the law of the Netherlands.

Clause 18 Choice of forum and jurisdiction
(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts of the Netherlands.
(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.
(d) The Parties agree to submit themselves to the jurisdiction of such courts.

SCHEDULE 6

SWISS ADDENDUM

As stipulated in Section 3.4 of the DPA, this Swiss Addendum shall apply to any processing of Customer Personal Data subject to Swiss data protection law or to Swiss data protection law and the GDPR.

1. Interpretation of this Addendum

1.1 Where this Addendum uses terms that are defined in the SCCs, those terms shall have the same meaning as in the SCCs. In addition, the following terms have the following meanings:

This Addendum	this Addendum to the Clauses
Clauses	the SCCs
Swiss Data Protection Laws	the Swiss Federal Act Data Protection of 19 June 1992 and the Swiss Ordinance to the Swiss Federal Act on Data Protection of 14 June 1993, and any new or revised version of these laws that may enter into force for time to time.

1.2 This Addendum shall be read and interpreted in the light of the provisions of Swiss Data Protection Laws, and so that if fulfils the intention for it to provide the appropriate safeguards as required by Article 46 GDPR and/or Article 6(2)(a) of the Swiss Data Protection Laws, as the case may be.

1.3 This Addendum shall not be interpreted in a way that conflicts with rights and obligations provided for in Swiss Data Protection Laws.

1.4 Any references to legislation (or specific provisions of legislation) means that legislation (or specific provision) as it may change over time. This includes where that legislation (or specific provision) has been consolidated, reenacted and/or replaced after this Addendum has been entered into.

2. Hierarchy

In the event of a conflict or inconsistency between this Addendum and the provisions of the Clauses or other related agreements between the Parties, existing at the time this Addendum is agreed or entered into thereafter, the provisions which provide the most protection to data subjects shall prevail.

3. Incorporation of the Clauses

3.1 In relation to any processing of personal data subject to Swiss Data Protection Laws or to both Swiss Data Protection Laws and the GDPR, this Addendum amends the DPA including the Clauses to the extent necessary so they operate:

a. for transfers made by the data exporter to the data importer, to the extent that Swiss Data Protection Laws or Swiss Data Protection Laws and the GDPR apply to the data exporter's processing when making that transfer; and

b. to provide appropriate safeguards for the transfers in accordance with Article 46 of the GDPR and/or Article 6(2)(a) of the Swiss Data Protection Laws, as the case may be.

3.2 To the extent that any processing of personal data is exclusively subject to Swiss Data Protection Laws, the amendments to the Data Processing Agreement including the Clauses as required by Section 3.1 above, include (without limitation):

a. References to the "Clauses" or the "SCC" means this Addendum as it amends the Clauses.

b. Clause 6 Description of the transfer(s) is replaced with:
"The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are those specified in Annex I.B where Swiss Data Protection Laws apply to the data exporter's processing when making that transfer."

c. References to "Regulation (EU) 2016/679" or "that Regulation" or "“GDPR" are replaced by "Swiss Data Protection Laws" and references to specific Article(s) of "Regulation (EU) 2016/679" or "GDPR" are replaced with the equivalent Article or Section of Swiss Data Protection Laws extent applicable.

d. References to Regulation (EU) 2018/1725 are removed.

e. References to the "European Union", "Union", "EU" and "EU Member State" are all replaced with "Switzerland".

f. Clause 13(a) and Part C of Annex I are not used; the "competent supervisory authority" is the Federal Data Protection and Information Commissioner (the "FDPIC") insofar as the transfers are governed by Swiss Data Protection Laws;

g. Clause 17 is replaced to state
"These Clauses are governed by the laws of Switzerland insofar as the transfers are governed by Swiss Data Protection Laws".

h. Clause 18 is replaced to state:
"Any dispute arising from these Clauses relating to Swiss Data Protection Laws shall be resolved by the courts of Switzerland. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of Switzerland in which he/she has his/her habitual residence. The Parties agree to submit themselves to the jurisdiction of such courts."
Until the entry into force of the revised Swiss Data Protection Laws, the Clauses shall also protect personal data of legal entities and legal entities shall receive the same protection under the Clause as natural persons.

3.3 To the extent that any processing of personal data is subject to both Swiss Data Protection Laws and the GDPR, the Data Processing Agreement including the Clauses will apply (i) as is and (ii) additionally, to the extent that a transfer is subject to Swiss Data Protection Laws, as amended by Sections 3.1 and 3.2 above, with the sole exception that Clause 17 shall not be replaced as stipulated under Section 3.2(g).

3.4 Customer warrants that it and/or Customer Affiliates have made any notifications to the FDPIC which are required under Swiss Data Protection Laws.