AUCTANE CUSTOMER DATA PROCESSING AGREEMENT

This Data Processing Agreement (“**DPA**”) is entered into and forms part of the applicable agreement for the provision of Auctane services (“**MSA**”) between the applicable Auctane entity that is party to that agreement (hereafter, “**Auctane**”), and the applicable customer or partner that is party to that agreement (“**Customer**”) and is effective as of the date of the MSA. The Customer and Auctane may be referred to individually as a “**Party**” and collectively as the “**Parties**” under this DPA.

WHEREAS:

(A) The Customer wishes to subcontract certain Services to Auctane under the MSA, which may require the Processing of Personal Data;

(B) The Parties seek to implement this DPA to assist with compliance with applicable Data Protection Laws including the GDPR, CCPA and PIPEDA; and

(C) The Parties wish to identify their rights and obligations.

The parties agree to comply with the following provisions, each acting reasonably and in good faith.

1. Definitions and Interpretation

Unless otherwise defined herein, capitalized terms and expressions used in this DPA shall have the following meaning:

“**Alternative Adequate Level of Protection**” means: (a) the country where Auctane or the applicable Sub-Processor is located is recognized by the Data Protection Laws of the EEA and/or UK (as applicable) to have an adequate level of protection of Personal Data; (b) Auctane or the applicable Sub-Processor have implemented binding corporate rules which provide adequate safeguards as required by the Data Protection Laws of the EEA and/or UK (as applicable); or (c) Auctane or the applicable Sub-Processor has implemented any other similar program or appropriate safeguards that are recognized by the Data Protection Laws of the EEA and/or UK (as applicable) as providing an adequate level of protection.

“**Business**” shall have the meaning given to it in the CCPA.

“**CCPA**” means the California Consumer Privacy Act of 2018, as amended by the California Privacy Rights Act (“**CPRA**”), and its accompanying regulations, each as they may be amended from time to time.

“**Consumer**” shall have the meaning given to it in the CCPA.

“**Controller**” means the entity that determines the purposes and means of the Processing of Personal Data, and also includes a ‘business’ as that term is defined in the CCPA.

“**Data Protection Laws**” means any laws and regulations applicable in any relevant jurisdiction relating to privacy or the use or Processing of Personal Data, including without limitation: (a) US Privacy Laws, including without limitation the CCPA and VCDPA; (b) GDPR; (c) UK GDPR; (d) the DPA 2018; (e) EU Directive 2002/58/EC (as amended by 2009/139/EC) and any legislation implementing or made pursuant to such directive, including (in the UK) the Privacy and Electronic Communications (EC Directive) Regulations 2003; (f) any provincial or federal laws or regulations in Canada, including without limitation PIPEDA and any substantially similar legislation enacted in the Provinces of Alberta, British Columbia and Quebec; and (g) any laws or regulations ratifying, implementing, adopting, supplementing or replacing any of the foregoing; in each case, to the extent in force, and as such are updated, amended or replaced from time to time.

“**Data Subject**” means the identified or identifiable person to whom Personal Data relates, and also includes a ‘consumer’ as that term is defined in the CCPA.

“**DPA**” means this Data Processing Agreement and all Schedules, if any.

“**EEA**” means the European Economic Area, including Switzerland and those countries comprising the European Union (“**EU**”) and the European Free Trade Association.

“EU SCCs” means the standard contractual clauses approved by the European Commission in Commission Decision 2021/914 dated 4 June 2021, for transfers of Personal Data in countries not otherwise recognized as offering an adequate level of protection for Personal Data by the European Commission (as amended and updated from time to time) currently available at https://eurlex.europa.eu/eli/dec_impl/2021/914/oj?locale=en&amp;uri=CELEX:32021D0914. This includes the Controller-to-Processor Clauses and the Processor-to-Processor Clauses which are hereby incorporated by reference.

"**GDPR**" means: (a) General Data Protection 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 and repealing Directive 95/46/EC and any implementing laws in each EU member state, each as they may be amended from time to time.

"**Personal Data**" means all data which is defined as 'personal data' or 'personal information' or similar in the applicable Data Protection Laws, and which is provided by Customer or its customers or end users to Auctane or accessed, stored or otherwise Processed by Auctane in connection with the Services.

"**PIPEDA**" means the Personal Information Protection Electronic Documents Act, SC 2000 c5 and its accompanying regulations, each as they may be amended from time to time.

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

"**Processor**" means the entity that Processes Personal Data on behalf of the Controller, and also includes a 'service provider' as that term is defined in the CCPA.

"**Schedule**" means a schedule to this DPA, which forms an integral part of this DPA.

"**Security Incident**" means a breach of Auctane security or an Auctane Sub-Processor's security leading to accidental or unlawful destruction, theft, loss, alteration or unauthorized disclosure of, or access to, Personal Data.

"**Selling**" shall have the meaning given to it in the CCPA and "sell" shall be construed accordingly.

"**Services**" means shipping and software services offered by Auctane and any other services provided by Auctane to Customer under the MSA.

"**Service Provider**" shall have the meaning given to it in the CCPA.

"**Sub-Processor**" means another Processor subcontracted by Auctane which is to Process Personal Data for the purpose of the Services.

"**Supervisory Authority**" means the applicable data protection authority or other regulatory authority responsible for regulating the Processing of Personal Data in connection with the Services.

"**UK GDPR**" means the GDPR as it forms part of the law of England and Wales, Scotland, and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018 and the European Union (Withdrawal Agreement) Act 2020 in the UK and including the UK Data Protection Act 2018 ("**DPA 2018**"), and any implementing laws in the United Kingdom, each as they may be amended from time to time.

"**UK Addendum**" means the "International Data Transfer Addendum to the EU Commission Standard Contractual Clauses" issued by the United Kingdom's Information Commissioner's Office, Version B1.0, in force as of March 21, as revised under section 18 of the UK Mandatory Clauses, which is hereby incorporated by reference.

"**US Privacy Laws**" means any laws and their accompanying regulations, each as they may be amended from time to time, applicable at the federal level and in any relevant US state relating to privacy or the use or Processing of Personal Data.

"**VCDPA**" means the Virginia Consumer Data Protection Act and its accompanying regulations, each as they may be amended from time to time.

Capitalized terms used, but not defined, in this DPA are defined in the MSA.

2. Object of this DPA

The Parties acknowledge and agree that, except as provided in the paragraph below, this DPA will apply when Personal Data is Processed by Auctane. In this context, Auctane will act as Processor or Sub-Processor to Customer, who can act either as Controller or Processor of Personal Data.

Notwithstanding anything in this DPA to the contrary, where Auctane captures contact details and payment details for its internal business purposes of sales and marketing, account management, technical support, billing, legal and regulatory compliance and such other activities as set out in its Privacy Policy (a) Auctane is the Controller of such Personal Data, and such activities are outside of the general scope of this DPA; and (b) when acting as the Controller of such data, Auctane shall Process such Personal Data in line with the applicable Privacy Policy of Auctane or its affiliates.

3. Duration and Termination

This DPA shall remain in effect as long as Auctane carries out Processing of Personal Data on behalf of Customer as set forth in the MSA, or until the termination of the Services, whichever period is longer.

Upon the termination or expiration of this DPA or the MSA, any rights and obligations of the Parties accrued prior to the termination or expiration thereof shall continue to exist.

Upon termination or expiration of the DPA or the MSA, or at any earlier moment if the Personal Data are no longer relevant for the delivery of the Services, at the choice of the Customer, Auctane shall delete or return all Personal Data to the Customer and delete existing copies unless Data Protection Laws or other legal, regulatory or professional business standards require storage of or exempt deletion of the Personal Data.

Customer acknowledges and agrees that Auctane shall have no liability for any losses incurred by Customer arising from or in connection with the Auctane's inability to perform the Services as a result of Auctane complying with a request to delete or return Personal Data made by Customer.

The provisions of Sections 1, 3, and 10-13 of this DPA shall survive the termination or expiration of this DPA, the MSA and the Services.

4. Data Protection

Because the performance of the MSA and the delivery of the Services includes the Processing of Personal Data, the Customer and Auctane shall comply with applicable Data Protection Laws to the extent that the Personal Data is within the scope of such Data Protection Laws. It shall be the responsibility of the Customer to inform Auctane which Personal Data Auctane Processes on behalf of the Customer is within the scope of CCPA, VCDPA, GDPR, UK GDPR, PIPEDA or other Data Protection Laws.

As the Controller or Processor of Personal Data, the Customer shall ensure that it has established a valid legal basis for the Processing of the Personal Data by Auctane. Customer's instructions for the Processing of Personal Data shall comply with applicable Data Protection Laws. Customer shall have sole responsibility for the accuracy, quality, and legality of Personal Data and the means by which Customer acquired Personal Data, including compliance with any applicable Data Subject notice and consent requirements.

Auctane shall only Process Personal Data on behalf of and in accordance with Customer's documented instructions (including those set out in the MSA and this DPA) for the following purposes unless required to by applicable laws to which Auctane is subject: (A) Processing in accordance with the MSA; (B) Processing initiated by Customer or Customer's customers or end users in their use of the Services; (C) Processing to comply with other documented reasonable instructions provided by Customer where such instructions are consistent with the terms of the MSA; and (D) as required by applicable Data Protection Laws.

To the extent required by applicable Data Protection Laws, Auctane, in acting as the Customer's Processor, shall:

- take reasonable steps to ensure that persons authorized to Process the Personal Data are subject to statutory or contractual confidentiality obligations or are otherwise bound by confidentiality obligations;

- take technical and organizational measures appropriate (having regard to the state of technological development and cost of implementation) for protection of the security, confidentiality and integrity of Personal Data (including protection against unauthorized or unlawful Processing and against accidental or unlawful destruction, loss, theft, alteration, damage or unauthorized disclosure of, or access to, Personal Data), as set forth in **Schedule 4 (Annex II)** of this DPA;

- notify the Customer of a Security Incident in relation to Customer's Personal Data without undue delay and, at the Customer's request, provide reasonable assistance in relation to any mandatory obligations applicable to the Customer in relation to a Security Incident under applicable Data Protection Laws, in each case at the Customer's cost; provided, however, that nothing in this paragraph shall prohibit Auctane from taking the steps as Auctane deems necessary and reasonable in order to remedy or mitigate the effects of the Security Incident;

- at the Customer's cost and request, assist, insofar as this is possible, to fulfil the Customer's obligations to respond to requests made by Data Subjects in relation to their rights with regard to their Personal Data (as further set forth in Section 7 of this DPA);

- at the Customer's cost and request, provide reasonable assistance in relation to any mandatory obligations applicable to the Customer in relation to the performance of Data Protection Impact Assessments by the Customer under applicable Data Protection Laws;

- make available to the Customer all information necessary to demonstrate compliance with the obligations laid down in this DPA and, at the cost and request of the Customer, allow for and contribute to audits, including inspections conducted by the Customer or another auditor mandated by the Customer, as set forth in Section 9 of this DPA; and

- inform the Customer promptly if it believes that any instruction from the Customer infringes applicable Data Protection Laws.

5. Data Transfers

Customer shall ensure that any data transfers are in compliance with the requirements of Data Protection Laws.

Where Customer acts as a Controller and Auctane as a Processor, and the Personal Data is subject to the Data Protection Laws of the EEA and/or the UK (as applicable), (b) transferred to Auctane outside the EEA and (c) where no Alternative Adequate Level of Protection applies, the Parties hereby agree that the EU SCCs (Controller-to-Processor – Module 2) will apply to the transfer of such Personal Data, as construed by reference to **Schedule 1** hereto. Auctane may terminate the EU SCCs by giving Customer 30 days' notice and implementing an alternative framework as may be required as provided in the Data Protection Laws of the EEA and/or the UK (as applicable).

Where Customer acts as a Processor and Auctane as a Sub-Processor, and the Personal Data is (subject to the Data Protection Laws of the EEA and/or the UK (as applicable), (b) transferred to Auctane outside the EEA and (d) where no Alternative Adequate Level of Protection applies, the Parties hereby agree that the EU SCCs (Processor-to-Processor – Module 3) will apply to the transfer of Personal Data, as construed by reference to **Schedule 1** hereto. Auctane may terminate the EU SCCs by giving Customer 30 days' notice and implementing an alternative framework as required as provided in the Data Protection Laws of the EEA and/or the UK (as applicable).

The Parties hereby agree that the UK Addendum, as construed by reference to **Schedule 2** hereto, will also apply to the transfer of Personal Data from the UK and shall supplement the EU SCCs, to the extent such transfers are subject to the UK GDPR and are to a country where no Alternative Adequate Level of Protection is recognized in the UK (as described in the UK GDPR). Auctane may terminate the UK Addendum by giving Customer 30 days' notice and implementing an alternative framework as may be required as provided in the UK GDPR.

6. US Privacy Laws

Customer and Auctane shall comply with US Privacy Laws to the extent that the Customer is a Business and Auctane is a Service Provider Processing the Personal Data of Consumers on behalf of the Customer. It shall be the responsibility of Customer to inform Auctane which Personal Data Auctane Processes on behalf of the Customer is within the scope of US Privacy Laws.

Customer warrants that it discloses Personal Data of Consumers to Auctane solely for (i) a valid business purpose, and (ii) to permit Auctane to perform the Services. Auctane agrees to provide the same level of protection of the consumer's rights under US Privacy Laws as the Customer and provide the same level of privacy protection as required of businesses by US Privacy Laws and its accompanying regulations.

To the extent US Privacy Laws apply, Auctane shall not retain, use, or disclose Personal Data of Consumers obtained in the court of providing Services, including for any commercial purpose other than the business purposes specified in the MSA except:

- To process or maintain Personal Data of Consumers on behalf of the Customer in compliance with the MSA;

- To retain and employ another Service Provider as a Sub-Processor, where the Sub-Processor meets the requirements for a Service Provider under US Privacy Laws;

- For internal use by Auctane to build or improve the quality of its services, provided that the use does not including building or modifying Consumer profiles to use in providing Services to another Business or correcting or augmenting data acquired from another source; and/or

- To detect data Security Incidents, or to protect against fraudulent or illegal activity.

This DPA shall not restrict Auctane's ability to:

- Comply with federal, state, or local laws;

- Comply with a civil, criminal, or regulatory inquiry, investigation, subpoena or summons by federal, state, or local authorities;

- Cooperate with law enforcement agencies concerning conduct or activity that the Customer, Auctane, or a third party reasonably and in good faith believes may violate federal, state, or local law; and/or

- Exercise or defend legal claims.

For clarity, Auctane shall not sell or share a Consumer's Personal Data as the term 'sell' or "share" is defined in the applicable US Privacy Laws when a Consumer has opted-out of the sale of their Personal Data with the Customer and such request has been conveyed to Auctane.

Auctane shall refrain from combining Personal Data received from Customer with Personal Data (1) received from, or on behalf of, one or more entities to which it is a Service Provider or Processor, or (2) collected from Auctane's own interaction with the consumer, or (3) of opted-out consumers which Auctane receives from or on behalf of Customer with Personal Data which Auctane receives from or on behalf ·of another person or persons, or collects from its own interaction with consumers.

Auctane shall notify Customer if it makes a determination that it can no longer meet its obligations under US Privacy Laws.

Auctane grants Customer the right, upon notice, to take reasonable and appropriate steps to stop and remediate unauthorized use of Personal Data.

Auctane shall use the Personal Data only for the limited and specified purposes set out in **Schedule 3 (Annex I)**.

Auctane certifies that it understands and will comply with the restrictions set out in this Addendum. If Auctane at any time determines that it can no longer meet its obligations under this Addendum or Law, Auctane shall immediately notify Customer after Auctane makes such determination. Auctane grants Customer the right to take reasonable and appropriate steps to ensure that Auctane uses the Personal Data that it collected pursuant to the MSA in a manner consistent with Customer's obligations under US Privacy Laws and its regulations. Auctane shall cooperate with Customer including but not limited to, providing documentation to Customer verifying that Auctane no longer retains or uses Personal Data of Consumers who have made a valid request to delete with the Customer.

Auctane agrees, except as may be necessary to fulfil the express requirements of the MSA, to refrain from attempting to reidentify or identify any individual based on Personal Data.

7. Rights of Data Subjects

Auctane shall respond to any Data Subject complaint, inquiry, or request to exercise their rights regarding Personal Data (including right of access, right to rectification, restriction of Processing, erasure, data portability, object to the Processing, or its right not to be subject to an automated individual decision making) (a "**Data Subject Request**") by either asking the Data Subject to make their request to Customer or by promptly notifying the Customer of the same.

Auctane will, in a manner consistent with the functionality of the Services, enable Customer to access, rectify, erase and restrict Processing of Personal Data (including via the deletion functionality provided by the Services, if available), and to export Personal Data.

To the extent Customer, in its use of the Services, does not have the ability to address a Data Subject Request, Auctane shall upon Customer's request (and taking into account the nature of the Processing) provide commercially reasonable efforts to assist Customer in fulfilling its obligation to respond to Data Subject Requests that are required under applicable Data Protection Laws. To the extent legally permitted, Customer shall be responsible for any reasonable costs arising from Auctane's provision of such assistance.

8. Sub-Processing

To the extent permitted under the MSA, Auctane may appoint third parties to assist in providing the Services who may be considered Sub-Processors, provided that such Sub-Processors:

(a) agree to act only on Auctane's instructions when Processing Personal Data (which instructions shall be consistent with the Customer's Processing instructions to Auctane); and

(b) have entered into a written agreement with Auctane containing data protection obligations no less protective than those in this DPA with respect to the Processing of Personal Data to the extent applicable to the nature of the Services provided by such Sub-Processor.

The list of current Auctane Sub-Processors can be found at: https://auctane.com/legal/sub-processors/. When any new Sub-Processor is appointed that will Process Personal Data, Auctane will notify Customer by email or by posting at: https://auctane.com/legal/sub-processors/ at least thirty (30) days before the new Sub-Processor begins Processing Personal Data ("**Notice Period**").

In the event that Customer reasonably objects to the Processing of its Personal Data by any Sub-Processor, it shall inform Auctane immediately by emailing its objection and the grounds for its objection to the email address(es) for notice as listed in the MSA. In such event, Auctane will do one of the following at Auctane's option: (a) instruct the Sub-Processor to cease any further Processing of the Customer's Personal Data, in which event this DPA shall continue unaffected (Customer acknowledges that the inability to use a particular new Sub-Processor may result in delay in performing the Services, inability to perform the Services or increased fees), or (b) allow the Customer to terminate this DPA and the MSA and related Services immediately with no further liability to Auctane. Customer's failure to object in writing within the Notice Period time period shall constitute approval to use the new Sub-Processor.

Auctane shall be liable for the acts and omissions of its Sub-Processors to the same extent Auctane would be liable if performing the services of each Sub-Processor directly under the terms of this DPA.

9. Audit Rights

To the extent that Audit Rights are specifically authorized by the applicable Data Protection Law, upon Customer's request, with not less than thirty (30) days' notice, Auctane agrees (at Customer's expense) to permit Customer to perform reviews of Auctane's compliance with its security obligations set forth under the DPA (the "**Customer Audits**"). Customer Audits may be conducted by the internal and external auditors and personnel of Customer who have entered into Auctane's form of nondisclosure agreement (collectively, "**Auditors**"). The scope of such Customer Audits shall be agreed in advance with Auctane. Such Customer Audits shall be conducted in accordance with Auctane's security policies and procedures, without undue disruption to Auctane's operations, in a commercially reasonable manner, and shall be limited to the security aspects of the Services provided to Customer. Customer Audit(s) will be performed at Customer's sole cost and Customer will reimburse Auctane for its reasonable costs associated with such additional Customer Audits. Customer shall promptly notify Auctane with information regarding the results of Customer Audits, including any information that Auctane is not Processing Personal Data in accordance with its obligations under this DPA. If the requested scope of the Customer Audit is addressed in an SSAE 16/ISAE 3402 Type 2, ISO, NIST or similar audit report performed by a qualified third party auditor within twelve (12) months of the request of the Customer Audit and Auctane confirms there are no known material changes in the controls audited, Customer agrees to accept those findings in lieu of requesting an audit of the controls covered by the report.

10. Customer Instructions

Auctane shall not be liable for any claim brought by Customer or any end user or customer of Customer or any other third party arising from Auctane's compliance with Customer's instructions.

11. Limitation of Liability

The total liability of Auctane (and its Affiliates and their respective employees, directors, officers, agents, successors, and assigns) arising out of or related to this DPA and the MSA, whether in contract, tort, or other theory of liability, shall in the aggregate, be subject to the limitation of liability set forth in the MSA.

12. Miscellaneous Provisions

This DPA, together with the MSA, sets out all of the terms that have been agreed between the Parties in relation to the subjects covered by it hereof and supersedes and replaces all prior agreements or understandings, whether written or oral, with respect to the same subject matter that are still in force between the Parties.

Any amendments to this DPA, as well as any additions or deletions, must be agreed to in writing by both Parties.

Customer acknowledges that Auctane may disclose any information processed pursuant to this DPA, and any other relevant data protection and privacy provisions to the U.S. Department of Commerce, the Federal Trade Commission, or any other judicial or regulatory body upon their request.

To the extent that any provision of this DPA conflicts with any provision of the MSA, the terms of the DPA shall prevail, as to the specific subject matter of the DPA.

Whenever possible, the provisions of this DPA shall be interpreted in such a manner as to be valid and enforceable under the applicable law. If any part of this DPA is held invalid, illegal or unenforceable, the validity of all remaining parts will not be affected. Moreover, in such an event, the Parties shall amend the invalid, illegal or unenforceable parts and/or agree on a new provision to reflect as much as possible the intended purpose of the invalid, illegal or unenforceable provision.

Any failure, delay, action or inaction by a Party to exercise its rights under this DPA, shall not be considered a waiver of that Party's rights under this DPA, and shall not operate to preclude such rights. Any waiver of a right must be express and in writing.

13. Applicable Law and Jurisdiction

To the extent required by applicable Data Protection Laws (e.g., in relation to the governing law of the EU SCCs and the UK Addendum), this DPA shall be governed by the law of the applicable jurisdiction. In all other cases, the laws of the jurisdiction specified in the MSA shall apply to this DPA.

List of Schedules:

- Schedule 1: References to EU Standard Contractual Clauses - Controller to Processor and Processor to Processor
- Schedule 2: (if applicable) UK International Data Transfer Addendum to the EU Commission Standard Contractual Clauses
- Schedule 3: Data Processing Details (also Annex I to the EU SCCs)
- Schedule 4: Security (also Annex II to the EU SCCs SCCs)
- Schedule 5: Sub-Processors (also Annex III to the EU SCCs)

Schedule 1 - EEA Transfers

This Schedule shall apply when the Personal Data is (a) subject to the Data Protection Laws of the EEA and/or the UK (as applicable), (b) transferred to Auctane outside the EEA and/or UK and (c) where no Alternative Adequate Level of Protection applies (the “**EEA Transfer**”).

The Parties hereby agree that the EU SCCs shall be construed as set forth below. Auctane may terminate the EU SCCs by giving Customer 30 days’ notice and implementing an alternative framework as may be required as provided by the Data Protection Laws of the EEA and/or the UK (as applicable).

1) The EEA Transfer shall be governed by the EU SCCs and references in the EU SCCs and in this Schedule 1 to the **data exporter** shall be Customer and references to the **data importer** shall be Auctane.

2) The EU SCCs are hereby incorporated into this DPA with and construed as follows (with references in this paragraph 1.2 to Clauses being to Clauses of the EU SCCs):

   a) All footnotes and explanatory notes in the EU SCCs are deleted;

      i) Where the EEA Transfer is a **Controller to Processor** transfer, specifically where Customer acts as the Controller and data exporter, and Auctane acts as the Processor and data importer, only the provisions relating to **Module 2** apply to such EEA Transfer;

      ii) Where the EEA Transfer is a **Processor to Processor** transfer, specifically where Customer acts as the Processor and data exporter, and Auctane acts as the Sub-Processor and data importer, only the provisions relating to **Module 3** apply to such EEA Transfer;

   b) Clause 7 (Docking Clause) of the EU SCCs (Module 2 and Module 3) applies;

   c) The instructions to the data importer shall be construed by reference to Section 4 of this DPA and which in the case of Module 3 constitute the instructions of the relevant Controller(s);

   d) Clause 8.5 (Duration of processing and erasure or return of data) of the EU SCCs (Module 2 and Module 3) shall be construed by reference to Section 3 of this DPA;

   e) Clause 8.9(d) (audits) of the EU SCCs (Module 2 and Module 3) shall be construed by reference to Section 9 of this DPA;

   f) With respect to Clause 9 (sub-processors), ‘Option 2: General Written Authorisation’ applies, and the data importer shall specifically inform the data exporter in writing of any intended changes to the Sub-Processor list set forth at Annex III in accordance with Section 8 of this DPA;

   g) The optional provision in Clause 11(a) (Redress) of the EU SCCs (Module 2 and Module 3) does not apply;

   h) With respect to Clause 13(a) (supervision), the following wording shall apply: “where the data exporter is established in an EU Member State, the Supervisory Authority shall be the Supervisory Authority of that EU Member State. Where the data exporter is not established in an EU Member State but has appointed an EU representative pursuant to the GDPR, the Supervisory Authority shall be the Supervisory Authority of the EU Member State in which the EU representative is established. In all other cases, the Supervisory Authority shall be the Supervisory Authority of Ireland”;

   i) In respect of Clause 17 (governing law), Option 1 shall apply, and the Clauses shall be governed by the laws of Ireland; and

   j) In respect of Clause 18 (choice of forum and jurisdiction), the relevant courts shall be the courts of Ireland.

3) Annex I of the EU SCCs shall be completed with the information set out in Schedule 3 of this DPA.

4) Annex II of the EU SCCs shall be completed with the information set out in Schedule 4 of this DPA.

5) Annex III of the EU SCCs shall be completed with the information set out in Schedule 5 of this DPA.

6) Where the Data Protection Laws of Switzerland apply, the governing law, jurisdiction and Supervisory Authority shall be those of Switzerland. In addition, references in the EU SCCs to:

   a) the “EU”/”Member State” shall be construed as references to Switzerland;

b) the GDPR shall refer to the Data Protection Laws of Switzerland; and

c) “supervisory authority” shall refer to the Supervisory Authority of Switzerland.

Schedule 2 – UK Transfers

This Schedule shall apply in addition to Schedule 1 when the Personal Data is (a) subject to the UK GDPR and the DPA 2018, (b) transferred to Vendor outside the UK and (c) where no Alternative Adequate Level of Protection applies (the "**UK Transfer**").

The Parties hereby agree that the **UK Addendum** supplements the EU SCCs and shall be construed as set forth below. Auctane may terminate the UK Addendum by giving Customer 30 days' notice and implementing an alternative framework as may be required as provided by the UK GDPR and the DPA 2018. In the event of any conflict between Schedule 1 and this Schedule 2, this Schedule 2 takes precedence.

1) The UK Transfer shall be governed by the UK Addendum and the EU SCCs which are hereby incorporated into this DPA and construed as follows.

2) References in the UK Addendum and in this Schedule 2 to the data exporter shall be Customer and references to the data importer shall be Auctane.

3) Table 1 of the UK Addendum shall be completed as follows:

   a) The parties' details shall be the parties set forth in Schedule 3 of this DPA.

   b) The Key Contact shall be the contacts set forth in Schedule 3 of this DPA.

4) Table 2 of the UK Addendum shall be completed as follows: the Approved EU SCCs referenced in Table 2 shall be the EU SCCs as set forth in Schedule 1 of this DPA.

5) Table 3 of the UK Addendum shall be completed as follows: Annexes 1A and 1B shall be as set forth in Schedule 3 of this DPA; Annex II shall be as set forth in Schedule 4 of this DPA; and Annex III shall be as set forth in Schedule 5 of this DPA.

6) Table 4 of the UK Addendum shall be completed as follows: Customer or Auctane may end this Schedule 2 as set out in Section 19 of the EU SCCs.

Schedule 3 - Data Processing Details

(also Annex I to the EU SCCs)

A. LIST OF PARTIES

Customer/Data Exporter details:

Name: The entity identified as "Customer" in the MSA and this DPA.

Address: The address for Customer as otherwise specified in the DPA or the MSA.

Contact person's name, position and contact details: The contact details associated with Customer's account, or as otherwise specified in the DPA or the MSA.

Activities relevant to the data transferred under these Clauses: Receipt of the Services under the MSA.

Role: Controller or Processor (as applicable)

Auctane/Data Importer details:

Name: Auctane, as identified in the MSA and DPA.

Address: The address for Auctane as specified in the DPA or MSA.

Contact person's name, position and contact details: The contact details for Auctane, as specified in the DPA or MSA.

Activities relevant to the data transferred under these Clauses: Provision of the Services under the MSA.

Role: Processor or Sub-Processor (as applicable).

B. DESCRIPTION OF TRANSFER

1. **Categories of Data Subjects**

The Personal Data Processed concern the clients of the Customer and such other Data Subjects as required to provide the Services and such other Data Subjects as applicable to the Services.

2. **Categories of Personal Data Transferred**

The categories of Personal Data involved are: Personal Data that may include, amongst others, first name, surname, date of birth (to the extent applicable, e.g., to comply with age requirements on certain deliveries, etc.), contact information (including postal address, telephone number, email address), and description of package contents and such other Personal Data as required to provide the Services.

3. **Sensitive Personal Data**

Such Sensitive Personal Data as required to provide the Services.

4. **Frequency of Transfer**

Continuous

5. **Nature of the Processing**

The Processing operations performed by Auctane on behalf of the Customer relate to the provision of the Services and the collection, recording, organization, storage, use, and transmission of Personal Data to provide the Services in the MSA.

6. Purpose of the Data Transfer and Further Processing

The purpose is the scope of Services provided under the MSA, which includes, but is not limited to, (i) selecting carrier rates based on the addresses of expedition and receipt; (ii) creating expedition labels; (iii) transmitting the Personal Data to third party carriers and partners acting as independent Controllers for the purpose of making the deliveries; (iv) following up on returns by customers; and (v) tracking deliveries.

Processing by Sub-Processors is addressed in Schedule 5.

7. Retention Period

The shortest duration between (i) your deletion of the Personal Data from the Customer's Auctane account, and (ii) the end of the contractual relationship between Customer and Auctane, subject to Section 3 of the DPA.

8. Duration of Processing

The Processing performed by Auctane on behalf of the Customer shall be for the term set forth in the MSA and/or DPA.

C. COMPETENT SUPERVISORY AUTHORITY

As per Schedule 1 and Schedule 2 (as applicable) of this DPA.

Schedule 4 - Security

(also Annex II to EU SCCs)

ANNEX II - TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

This Annex forms part of the Clauses.

Auctane has established a security program, dedicated to ensuring customers have the highest confidence in our processing of their data. Auctane has defined roles and responsibilities to delineate which roles in the organization are responsible for operating the various aspects of Auctane’s Information Security Program

The responsibility of Auctane’s Global Information Security function which is led by Auctane’s Chief Information Security Officer (CISO).

Key aspects of Auctane’s security program:

Product & Application Security

- **Physical Security**
  - Auctane’s Brand’s products are hosted in Public Clouds (AWS or GCP) and therefore utilize their strong physical security practices.
- **Audit Logging**
  - Auctane maintains strong audit logs for both maintaining its services operationally as well as for security-based alerting and investigations.
- **Vulnerability Management**
  - Auctane uses an Industry leading Cloud Security Posture Management (CSPM) solution which provides Agentless and Cloud-Native Vulnerability Management and provides its Cloud Native Application Protection Platform (CNAPP).
  - Auctane uses an Industry leading solution to perform Dynamic Application Security Testing (DAST) of all its brand’s internet facing applications.
- **Data Security**
  - Encryption-at-Rest is implemented to meet industry standard based on the public cloud resource used and keys are managed via an Industry leading solution
  - Encryption-in-transit: up to HTTPS TLSv1.2 is supported.
  - Auctane use of CSPM provides Integrated Data Exposure Protection (DSPM)
- **Code Analysis**
  - Auctane has implemented an Industry leading solution to perform Automated Static Application Security Testing (SAST) & Software Composition Analysis (SCA) within the Software Development Lifecycle (SDLC).
- **Risk Management**
  - Annual 3rd Party penetration testing is carried out on all Brands applications.
    - Customer facing reports are available on request.
  - There is a Vendor Management security posture process in place to assess 3rd Party Risk.
- **Remediation Management**
  - Auctane’s current remediation Policy is that only Critical and High risks are addressed as a priority, the remaining severity levels will be accepted at this time but will be factored into the continuous platform improvements.
- **Developer Secure Code Training**
  - All Auctane Engineers have access to an Industry leading Training Platform for Secure Code Training.

Infrastructure & Network Security

- **Access Monitoring**
    - Auctane uses the relevant AWS & GCP inbuilt security monitoring tools to monitor access to production systems.
- **Access Management**
    - Access to Auctane Public Cloud environments is only via centralized VPN Solution (behind Auctane’s IDP) following Role Based Access and Least Privilege principles.
    - Auctane’s use of a CSPM solution provides Cloud Infrastructure Entitlement Management (CIEM).
- **Vulnerability Management**
    - Auctane’s use of a CSPM solution provides a Cloud workload protection platform (CWPP) regards:
        - Infrastructure as Code (IAC) Scanning
        - Vulnerability Management for Virtual Machines
        - Runtime analysis of Containers & Serverless Functions
- **Remediation Management**
    - Same as “Product & Application Security - Remediation Management”
- **End Point Protection**
    - All Auctane’s cloud VMs and Containers are protected by an Industry leading Endpoint Detection and Response (EDR) Solution.
- **Network Protection**
    - Auctane has deployed Web Application Firewalls (WAFs) and DDOS protection across all its Brands.

Security Incident Response

- **Threat Detection**
    - Auctane’s use of a CSPM solution enables Cloud Detect, Investigate, and Respond to Cloud Threats (CDR)
    - AWS & GCP inbuilt threat detection solutions are centralized across all Auctane’s public cloud envs’.
- **Security Incident Management Process**
    - If a Security Incident is deemed to impact customer's specific services or data, then customers will be contacted as per customer contract service level agreement (if any).

Corporate Security

- **Employee Training**
    - All Auctane employees take mandatory annual Information Security and Data Protection training on Industry leading Training Platform.
- **Access Control**
    - Auctane corporate system is all SaaS based and access is controlled and managed by Industry leading Identify and Access Platform; ‘Single sign on’ using MFA.
- **Email Protection**
    - Auctane’s email protection is via Industry leading Email Protection Platform.
- **End Point Protection**
    - All Auctane’s endpoints are protected by an Industry leading Endpoint Detection and Response (EDR) Solution.

Schedule 5 - Security

(also Annex III to EU SCCs)

The list of current Auctane Sub-Processors can be found at: https://auctane.com/legal/sub-processors/.

When any new Sub-Processor is appointed that will Process Personal Data, Auctane will notify Customer by email or by posting at: https://auctane.com/legal/sub-processors/ at least thirty (30) days before the new Sub-Processor begins Processing Personal Data.