Data Processing Addendum

This Data Processing Addendum ("**DPA**") supplements the agreement in place between Customer and Supplier governing Customer's use of the Services ("**Agreement**"). Unless otherwise defined in this DPA, capitalized terms used in this DPA have the meanings given to them in the Agreement.

1. Definitions

"**Applicable Data Protection Law**" means all laws and regulations applicable to the Processing of Personal Data by a party, including, as applicable, the GDPR, the CCPA, the UK Data Protection Act of 2018, and Canada's Personal Information Protection and Electronic Documents Act (PIPEDA).

"**CCPA**" means the California Consumer Privacy Act, and its implementing regulations.

"**Controller**" means the entity which determines the purposes and means of the Processing of Personal Data.

"**GDPR**" means 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of such data, and any implementing, derivative or related legislation, rule, or regulation, as amended, extended, repealed and replaced, or re-enacted from time to time.

"**Personal Data**" means any information that identifies or relates to a natural person, or which otherwise constitutes "personal data", "personal information", "personally identifiable information" or similar terms as defined in Applicable Data Protection Law that is Processed under this DPA.

"**Process**" or "**Processing**" means any operation or set of operations performed on Personal Data, whether or not by automatic means, including collecting, obtaining, developing, producing, recording, organizing, structuring, making available, deleting, accessing, or using Personal Data.

"**Processor**" means the entity which Processes Personal Data on behalf of the Controller.

"**SCCs**" means the standard contractual clauses between controllers and processors (Module 2), annexed to the European Commission's Implementing Decision 2021/914 of 4 June 2021, currently available at https://commission.europa.eu/publications/publications-standard-contractual-clauses-sccs_en.

"**Security Incident**" means any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data.

"**Subprocessor**" means any third party engaged by Supplier to Process Personal Data.

2. **Scope and Applicability.** This DPA applies when Supplier Processes Personal Data on behalf of Customer. In this context, Supplier is a Processor to Customer and Customer is the Controller of the Personal Data. The details of Supplier's Processing under this DPA, including the type of Personal Data, categories of data subjects, nature, purpose, and duration of Processing is set out in Exhibit A. This DPA will remain in effect until Supplier no longer Processes Personal Data.

3. **Compliance with Laws**. Each party will comply with all laws, rules, regulations applicable to it, including Applicable Data Protection Law in the performance of this DPA.

4. **Customer's Instructions**. Supplier will only Process Personal Data on the documented instructions of Customer as set out in this Agreement or any other document agreed by the parties in writing. Supplier will promptly inform Customer if, in the opinion of Supplier, an instruction of Customer relating to the Processing of Personal Data infringes Applicable Data Protection Law. Notwithstanding any other provision of this Agreement, Supplier may Process Personal Data if and to the extent that Supplier is required to do so by applicable law or regulatory authority. In such case, Supplier will inform Customer of the legal requirement before Processing, unless that law prohibits such information on important grounds of public interest.

5. **Confidentiality**. Supplier will ensure that persons authorized to Process Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality

6. **Security**. Supplier will implement appropriate technical and organizational measures designed to protect the security, confidentiality, integrity, and availability of Personal Data and to protect against Security Incidents. At a minimum, Supplier will implement security measures in accordance with the Security Standards available at https://www.octanner.com/legal/security-standards.

7. **Subprocessors**

   7.1 Customer provides general authorization to Supplier's use of Subprocessors in accordance with this Section. The list of Subprocessors currently engaged by Supplier is available at https://www.octanner.com/legal/subprocessors. At least 10 business days before engaging a new Subprocessor, Supplier will provide written notice to Customer. To object to a Subprocessor, Customer may provide notice to Supplier detailing its objections. Customer's objections must be reasonable and be made in good faith. If Customer's objection is not resolved to the mutual satisfaction of the parties within a reasonable time, either party may terminate this DPA.

   7.2 Where Supplier engages a Subprocessor as described in this Section, Supplier will: (i) ensure that the Subprocessor's Processing of Personal Data is limited to what is necessary to provide services under the Agreement, and for no other purpose; (ii) enter into an agreement with the Subprocessor that imposes on the Subprocessor substantially equivalent obligations that Supplier has under this DPA; and (iii) remain responsible for compliance with the obligations of this DPA and for any of the Subprocessor's acts or omissions that, if committed by Supplier, would breach Supplier's obligations under this DPA.

8. **Assistance**

8.1 Supplier will provide reasonable assistance to Customer through appropriate technical, physical, administrative, and organizational measures, taking into account the nature of the Personal Data Processed by Supplier, and to the extent possible, for the fulfilment of Customer's obligation to respond to requests for exercising data subject rights under Applicable Data Protection Law. If Supplier receives a data subject request concerning Personal Data, Supplier will promptly forward the request to Customer, and will not respond directly to the data subject (other than to inform the data subject that the request has been forwarded to Customer) unless (i) required by Applicable Data Protection Law; or (ii) instructed to do so by Customer.

8.2 Supplier will provide reasonable assistance to Customer, taking into account the nature of Supplier's Processing and information available to Supplier, to ensure Customer's compliance with obligations under Applicable Data Protection Law concerning: (i) the security of Personal Data; (ii) notification obligations related to a Security Incident; (iii) data protection impact assessments; and (iv) prior consultations with data protection supervisory authorities.

9. **Audits.** Supplier will make available to Customer all information necessary to demonstrate compliance with its obligations set forth in this DPA, and allow for and contribute to audits, including inspections, conducted by Customer or a third party mandated by Customer that is reasonably acceptable to Supplier. Such audits may only occur once per calendar year, unless in response to: (i) a Security Incident; or (ii) a request by a regulatory or supervisory authority. Customer agrees to provide Supplier with at least 30 days advance written notice of any audit or inspection requested under this DPA. Customer is responsible for its costs associated with audits or inspections under this DPA.

10. **Security Incident**. Supplier will notify Customer within forty-eight (48) hours of becoming aware of a Security Incident. Supplier's notice shall, to the extent known at the time, include the nature of the Security Incident, the number of individuals affected, and the steps Supplier has taken, or will take to mitigate the effects of the Security Incident. Supplier will provide all information reasonably necessary for Customer to meets its notification obligations under Applicable Data Protection Law. Customer will have sole control over the timing, content, and method of any notification to a data subject or regulatory authority to the extent: (i) the Security Incident relates solely to Personal Data Processed under this DPA; and (ii) Supplier does not have a legal obligation to notify under Applicable Data Protection Law.

11. **Deletion and Return of Personal Data**. Upon termination or expiration of the Agreement (or at any time upon Customer's written request), and as instructed by Customer, Supplier will delete or return Personal Data to Customer. Notwithstanding the foregoing, Supplier may retain Personal Data as required by applicable law; provided that Supplier will comply with the applicable terms of this DPA with respect to retained Personal Data and will not further Process it except as required by applicable law. Customer acknowledges and agrees that the deletion of Personal Data prior to the termination of the Agreement, as instructed by Customer may affect Supplier's ability to validate and honour any applicable product warranties provided in the Agreement.

12. **Jurisdiction-Specific Terms**. To the extent Supplier Processes Personal Data that is subject to Applicable Data Protection Law in one of the jurisdictions listed in the Jurisdiction-Specific Terms, available at https://www.octanner.com/legal/jurisdiction-specific-terms, the terms specified for the applicable jurisdiction will apply, including the terms of the SCCs for cross-border transfers of Personal Data.

Exhibit A
Description of Processing

CATEGORIES OF DATA SUBJECT

Employees, officers, agents, or contractors of Customer who have been deemed eligible by Customer for participation in the Program.

TYPES OF PERSONAL DATA

Personal Data Customer provides to Supplier, including: name, work contact information (work address, work email address, work phone number, shipping address), employee identification number, position, and hire date.

Depending on the nature of the Services, Supplier may also Process home address, personal phone number, personal email address, user generated information and content (e.g., messages, photos, comments, redemption history), ID number (if necessary to fulfil an order) language configuration, and IP address.

PURPOSE OF PROCESSING

Supplier will Process Personal Data to provide the Services to Customer under the Agreement.

NATURE OF PROCESSING

Processing includes collection, organization, structuring, storage, use, and disclosure by transmission in accordance with the terms of the Agreement, including the DPA.

DURATION

Supplier will Process Personal Data for the term of the Agreement and as outlined in the DPA.