Information Security and Data Protection Requirements

1. **Data Ownership.** Supplier acknowledges that all data and information (including Personal Information (defined below)) pertaining to MDLZ provided to, obtained by, or developed by Supplier in connection with this agreement ("MDLZ Data") shall at all times remain the property of MDLZ and Supplier shall acquire no rights or interests in them. "Personal Information" means any information that directly or indirectly identifies, relates to, describes or can be associated with or reasonably linked to an individual or household, and any other information defined as personal information, personal data, or other similar terms under all applicable Privacy Laws.

2. **Data Security.** Supplier shall use appropriate technical and organizational measures in accordance with industry practices and the sensitivity of the information (including the Personal Information) to secure MDLZ Data and systems to which Supplier has access. Supplier shall comply with any specific data processing and handling requirements reasonably requested by MDLZ or determined by applicable laws and regulations. Supplier shall, upon MDLZ's reasonable request, provide MDLZ a written summary of its practices described in this section. Supplier shall allow access to MDLZ Data only to Supplier personnel who have a need to access it in order to perform obligations under this agreement.

3. **Notice of Security Incidents.** Supplier shall notify MDLZ in writing immediately, but in no event later than within twenty-four (24) hours of (i) actual or suspected Data Breaches (defined below); (ii) any unauthorized access to MDLZ Data or systems or any vulnerability that carries a risk of compromising MDLZ Data or systems or (iii) any possible violations of applicable data protection laws. Supplier shall promptly at its own expense take actions (including any actions MDLZ reasonably requests) to comply with applicable laws and regulations governing Data Breaches and related matters. A Data Breach is any breach of security leading to the accidental or unlawful disclosure, loss, alteration or other compromise of the confidentiality, integrity or availability of MDLZ Personal Information. Supplier shall be responsible for any costs, fines, penalties, or other losses that MDLZ incurs as a result of any Data Breach arising from Supplier's negligence (act or omission) or breach of its obligations under this agreement.

4. **Compliance with Applicable Privacy Laws and Policies.** Supplier acknowledges that in collecting, receiving, or accessing MDLZ Personal Information, including information about MDLZ's consumers, customers, suppliers, business partners, contractors or employees, Supplier shall comply with (i) all state, federal, international, and provincial laws, rules and regulations applicable to Personal Information and any related information ("Privacy Laws"), and (ii) MDLZ privacy notices and policies ("Privacy Policies"). Supplier shall stay informed of possible changes to Privacy Laws and Privacy Policies throughout the course of the agreement. Supplier shall not cause MDLZ to be in violation of any Privacy Laws or Privacy Policies.

5. **Data Processing.** Supplier shall execute any necessary agreements and acquire all necessary permits and authorizations pertaining to processing and handling of MDLZ Data from relevant regulatory authorities. Supplier shall only process or otherwise use MDLZ Personal Information to the extent necessary to provide the Services described in the agreement and as instructed by MDLZ, for the sole benefit of MDLZ (unless differently agreed in writing between Supplier and MDLZ) and in a manner consistent with this agreement. Without limiting the foregoing, Supplier shall not (i) sell any MDLZ Personal Information; (ii) collect, retain, use, disclose, or otherwise process MDLZ Personal Information: (a) for any purpose other than for the specific purpose of performing the Services and as set forth in this agreement and to the extent reasonably necessary; (b) outside of the direct business relationship between MDLZ and Supplier (unless differently agreed in writing between Supplier and MDLZ); and (c) if prohibited by applicable law. Supplier will not use such Personal Information for its own purposes or commercial interests (unless differently agreed in writing between Supplier and MDLZ) and represents, warrants and certifies that it understands and will comply with the restrictions

set forth in this section and the entire agreement. The parties intend and agree that Supplier is a Service Provider, as defined under applicable privacy laws.

6. **Data Subject Requests.** Supplier shall cooperate with MDLZ if a person makes a lawful request for: (i) access to his or her Personal Information; (ii) information about the categories of sources from which the Personal Information is collected; (iii) information about the categories or specific pieces of the individual's Personal Information, including by providing the requested information in a portable and, to the extent technically feasible, readily useable format that allows the individual to transmit the information to another entity without hindrance; or (iv) any other right the person has regarding his or her Personal Information under applicable Privacy Laws. Supplier shall promptly inform MDLZ in writing of any requests with respect to MDLZ Personal Information.

7. **Deletion.** Upon MDLZ's request, Supplier shall promptly delete a particular individual's Personal Information from Supplier's records. In the event Supplier is unable to delete the Personal Information of a particular individual for reasons permitted under applicable law, Supplier shall: (i) promptly inform MDLZ of the reason(s) for its refusal of the deletion request; (ii) ensure the privacy, confidentiality and security of such Personal Information; and (iii) delete the Personal Information promptly after the reason(s) for Supplier's refusal has expired.

8. **Protection.** In addition to its Data Security obligations above, Supplier shall maintain the security, integrity, and availability of all MDLZ Data, including compliance with the following measures in a manner that meets or exceeds the relevant industry standards:

   A. Maintain hardware firewall and security settings;

   B. Deploy security and maintenance patches (software and firmware);

   C. Maintain and periodically test a disaster recovery plan, providing system backup, technology replacement, and alternate (recovery) site capabilities;

   D. Encrypt all transmissions and storage of MDLZ Data, including storage on mobile devices;

   E. Maintain and update an anti-virus program used customarily in large, commercial environments;

   F. Maintain physical security and access controls for all of Supplier's data center(s) and facilities;

   G. Use access control methods (including use of user id and strong passwords, auditing and logging, and information security change control procedures) for any system or device that could allow access to the MDLZ Data;

   H. Maintain an updated inventory of systems and entities that process Personal Information as well as a list of authorized people that have access to or process such information;

   I. Use dedicated or segregated computing equipment, including server(s) and database(s), when storing and processing Personal Information;

   J. Conduct quarterly vulnerability assessments and provide MDLZ with copies of the findings;

   K. At least annually, obtain and provide to MDLZ an SSAE 16 or an ISO 27001 report on its data security practices (or, if Supplier cannot obtain an SSAE 16 or ISO 27001 report, an alternative report that conforms to ISAE 3402 standards) from a recognized provider of such reports; and

   L. Implement additional reasonable security requirement requests of MDLZ to ensure adequate security and proper reporting, whether to mitigate risk to the business or for compliance with Privacy Laws.

9. **Subcontractor and Third Party Access.** Supplier shall not subcontract any data processing operations under this agreement or otherwise provide a third party with access to MDLZ Data without MDLZ prior written consent. When MDLZ has provided such consent, Supplier shall take all reasonable steps to ensure the reliability of such third parties, and shall require their compliance with this agreement

(and, if MDLZ requires, or if required by Privacy Laws, they will execute a separate confidentiality or other agreement with protections similar to those in this agreement). Supplier shall be responsible for any noncompliance of a third party, and this noncompliance will constitute a breach of this agreement as if committed directly by Supplier.

10. **Changes in Security Practices.** Supplier shall provide MDLZ with reasonable advance notice in writing of any planned changes to the hosting location of MDLZ Data, or other security policies, standards, and practices related to MDLZ Data. If MDLZ determines that Supplier's changed policies, standards, or practices do not conform with MDLZ's then-current security policies, standards, and practices, Supplier shall take the actions MDLZ reasonably requests to ensure its policies, standards, and practices conform to MDLZ's policies or MDLZ may terminate this agreement on a no fault basis.

11. **Record Retention.** Supplier shall retain MDLZ Data only for as long as required to perform its obligations under this agreement, except where (i) another retention period is strictly required by applicable law; or (ii) MDLZ asks Supplier in writing to retain certain MDLZ Data because of pending or anticipated litigation, investigation, audit or other purposes. At the termination of this agreement, Supplier shall, at MDLZ's option, return to MDLZ or securely destroy (such that no content is recoverable) all MDLZ Data. If MDLZ does not exercise this option within 30 days of the termination or expiry of this agreement, Supplier must provide 60 days' advance written notice to MDLZ and then proceed to permanently dispose of or destroy the MDLZ Data in a manner that prevents content recovery. If requested by MDLZ, Supplier shall provide a certificate to MDLZ attesting to its proper deletion or destruction of MDLZ Data.