

Information Security and Data Protection Requirements

1. **Data Ownership.** The Supplier acknowledges that all data and information (including personal information) pertaining to MDLZ provided to, obtained by, or developed by Supplier in connection with its agreement with MDLZ (“MDLZ Data”) shall at all times remain the property of MDLZ and the Supplier shall acquire no rights or interests in them.
2. **Data Security.** The Supplier shall use appropriate technical and organizational measures in accordance with industry practices and the sensitivity of the information to secure MDLZ Data and systems to which Supplier has access. The Supplier shall comply with any specific data processing and handling requirements reasonably requested by MDLZ or determined by applicable laws and regulations. The Supplier shall, upon MDLZ’s reasonable request, provide MDLZ a written summary of its practices described in these Information Security and Data Protection terms. The Supplier shall allow access to MDLZ Data only to employees who have a need to access it in order to perform obligations under its agreement with MDLZ.
3. **Notice of Security Incidents.** The Supplier shall notify MDLZ as soon as possible in writing of (i) any unauthorized access to MDLZ Data or systems or any vulnerability that carries a risk of compromising MDLZ Data or systems or (ii) 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. The Supplier shall be responsible for any costs, fines, penalties, or other losses that MDLZ incurs as a result of any unauthorized access arising from the Supplier’s negligence (act or omission) or breach of its obligations under its agreement with MDLZ.
4. **Compliance with Applicable Privacy Laws.** The Supplier may have access to specific information which can identify individuals who are MDLZ’s consumers, customers, suppliers, business partners, contractors or employees (known as “Personally Identifiable Information”). The Supplier shall comply with (i) all laws and regulations applicable to Personally Identifiable Information and any related information, and (ii) MDLZ privacy notices and policies (collectively, “Privacy Laws”). The Supplier shall stay informed of possible changes to Privacy Laws throughout the course of the agreement. The Supplier shall not cause MDLZ to be in violation of any Privacy Laws.
5. **Data Collection and Use.** The Supplier warrants that (i) any Personally Identifiable Information it will disclose to MDLZ under its agreement with MDLZ will be collected in accordance with Privacy Laws; (ii) any individual who provides Personally Identifiable Information to Supplier has been informed of MDLZ’s identity, how to contact MDLZ, and all other matters required by Privacy Laws; (iii) MDLZ is authorized either by consent of individuals or by law to obtain Personally Identifiable Information from Supplier (if the Supplier collects such information in the course of performing its obligations under its agreement with MDLZ) and use and disclose it for the purposes of its agreement with MDLZ; (iv) The Supplier shall notify MDLZ of any complaint or request it receives concerning the Personally Identifiable Information under its agreement with MDLZ and comply with any reasonable direction of MDLZ, including providing access by MDLZ to its premises, personnel, materials, and systems; and (v) The Supplier shall not access, transfer or make accessible Personally Identifiable Information in any jurisdiction which is not expressly contemplated by its agreement with MDLZ without MDLZ’s prior written consent.
6. **Data Processing.** The 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.
7. **Protection.** In addition to its Data Security obligations above, the 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 Personally Identifiable 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 Personally Identifiable 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.
8. **Subcontractor and Third Party Access.** The Supplier shall not subcontract any data processing operations under its agreement with MDLZ or otherwise provide a third party with access to MDLZ Data without MDLZ prior written consent. When MDLZ has provided such consent, the Supplier shall take all reasonable steps to ensure the reliability of such third parties, and shall require their compliance with its agreement with MDLZ (and, if MDLZ requires, they will execute a separate confidentiality or other agreement with protections similar to those in its agreement with MDLZ). The Supplier shall be responsible for any noncompliance of a third party, and this noncompliance will constitute a breach of its agreement as if committed directly by the Supplier.
9. **Changes in Security Practices.** The Supplier shall provide MDLZ with reasonable advance notice in writing of any planned changes to the hosting location of MDLZ Data, use of third party providers, 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 its agreement with MDLZ.
10. **Record Retention.** The Supplier shall retain MDLZ data only for as long as reasonably and legally required to perform any obligations under its agreement with MDLZ. The Supplier shall then dispose of or destroy it in a manner that prevents content recovery. Unless MDLZ asks the Supplier in writing to retain certain MDLZ Data because of pending or anticipated litigation, investigation, audit or other purposes, the Supplier shall, at MDLZ's option, return to MDLZ or destroy MDLZ Data whenever it is no longer needed to perform any obligations under its agreement with MDLZ. If requested by MDLZ, the Supplier shall provide a certificate to MDLZ attesting to its proper deletion or destruction of MDLZ Data. At the termination or expiration of its agreement with MDLZ, the Supplier shall notify MDLZ that it has MDLZ Data and shall follow MDLZ's reasonable directions

regarding return, destruction, or other disposal of such MDLZ Data. If MDLZ does not provide such direction, the 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.