DATA PROCESSING AGREEMENT

Gordon Food Service, Inc. and Gordon Food Service Canada, Ltd.

Last updated February 19, 2024

This Data Processing Agreement ("**DPA**") applies to any supplier of goods to GFS ("**Supplier**") that has entered into one or more Agreements with Gordon Food Service, Inc. and Gordon Food Service Canada Ltd. (collectively, "**GFS**"). Supplier and GFS are referred to herein as "**Party**" or "**Parties**" as the context requires.

1. Key Definitions

1.1 "**Affiliates**" means any entity that directly or indirectly controls, is controlled by, or is under common control with GFS. "**Control**," for purposes of this definition, means direct or indirect ownership or control of more than 50% of the voting interests of the subject entity.

1.2 "**Agreement**" means one or more agreements between Supplier and GFS pursuant to which Supplier is provided access to, collects or otherwise processes Covered PI.

1.3 "**Covered PI**" means any Personal Information provided by or collected on behalf of GFS to Supplier, collected by Supplier on behalf of GFS, or otherwise made available to Supplier pursuant to the Agreements.

1.4 "**Personal Information**" means (a) any information relating to a consumer or household and (b) any information that falls within the scope of "personal data", "personal information" or "personally identifiable information" (or any materially similar or analogous concept or definition) under any Privacy Laws.

1.5 "**Portable Format**" means to the extent technically feasible a structured, commonly used, machine readable, readily usable format that allows the consumer to transmit the Covered PI to another entity or controller without hindrance, as further specified in the Privacy Laws.

1.6 "**Privacy Laws**" mean any and all privacy and data protections laws and regulations applicable to the processing of the Covered PI under the Agreement, including but not limited to those in the United States and Canada, California Consumer Privacy Act, the California Privacy Rights Act, the Virginia Consumer Data Protection Act, the Colorado Privacy Act, The Personal Information Protection and Electronic Documents Act ("**PIPEDA**"), British Columbia's Personal Information Protection Act ("**BC PIPA**"); Alberta's Personal Information Protection Act ("**AB PIPA**"); and Quebec's Act respecting the Protection of Personal Information in the Private Sector ("**Quebec Privacy Sector Act**"), in each case when and if applicable to the processing of Covered PI by Supplier under this DPA.

1.7 The terms "business," "business purposes," "consumer," "controller," "processing," "processor," "sale," "sensitive data," "sensitive personal information," "service provider," "sharing," and "verifiable consumer request" shall have the meanings given to those terms in the Privacy Laws. In the event of a conflict in the meanings of terms in the Privacy Laws, the Parties agree the meanings from each law apply.

1.8 “**Services**” means the services provided by Supplier to GFS specified in the Agreements.

2. Terms of Data Processing

2.1 ***Relationship of the Parties***. The Parties agree that GFS is the sole Party that determines the purposes and means of processing Covered PI as the “business” or “controller;” and Supplier processes Covered PI as the “service provider” or “processor” on behalf of GFS.

2.2 ***Compliance with Obligations***. Supplier represents and warrants that Supplier, its employees, specialists, subcontractors, and sub-processors (a) will comply with Privacy Laws and this DPA while processing the Covered PI, and (b) will provide GFS with all reasonably-requested assistance to enable GFS to fulfill its own obligations under the Privacy Laws. Upon the reasonable request of GFS, Supplier shall make available to GFS all information in Supplier’s possession reasonably necessary to demonstrate its compliance with this subsection.

2.3 ***Deletion or Return of Covered PI***. Upon written request by GFS or termination of an Agreement, Supplier will discontinue processing Covered PI without undue delay. Within sixty (60) days of a written request by GFS or termination of an Agreement, Supplier will destroy Covered PI unless otherwise instructed by GFS; provided that prior to such destruction Supplier will return or make available to GFS for a period of sixty (60) days, for a complete and secure download, all of the Covered PI in Supplier’s possession. Supplier may retain Covered PI to the extent and for such period of time required by Applicable Law provided that Supplier shall (a) notify GFS of such obligations (unless prohibited from doing so) and (b) ensure the ongoing confidentiality of all such Covered PI. Upon written request by GFS or within 60 days of the termination of an Agreement, Supplier will provide a written certification to GFS that it has complied with these deletion obligations.

2.4 ***Assessments***. If applicable, Supplier shall, upon the reasonable request of GFS, provide GFS with such assistance and information as is reasonably necessary to enable GFS to carry out privacy impact assessments under Privacy Laws.

3. Limitations on Use of Covered PI

3.1 ***Limited Scope of Processing***. Supplier will process Covered PI solely as instructed in the Agreements, this DPA and any other written instructions provided by GFS that are consistent with the terms of the Agreement, in each case for the duration of the provision of the Services to GFS.

3.2 **Data Restrictions**. Supplier will not: (a) sell or share Covered PI, (b) collect, retain, use, or disclose Covered PI for any purpose other than the business purposes specified in the Agreements, such as providing the Services to GFS, (c) retain, use, or disclose Covered PI outside the direct business relationship with GFS, (d) combine the Covered PI with other Personal Information, including for data augmentation or profiling, unless expressly permitted under Privacy Laws for Supplier functions (such as for fraud prevention purposes, or where required by law), and/or (e) export Covered PI outside the country from which it was provided or collected without GFS’s prior written consent. Supplier shall have the right to use Aggregate Data (as defined below) for internal business purposes upon the written consent of GFS (email sufficient) provided that Supplier shall not use or disclose the Aggregate Data for commercial

purposes. "**Aggregate Data**" means Covered PI that is de-identified and aggregated in accordance with Privacy Laws such that the information is not linked or reasonably linkable to any of GFS or its customers.

3.3 ***Audit Rights***. GFS, or, upon GFS's election, a third party reasonably designated by GFS to act on GFS's behalf and acceptable to Supplier, shall have the right to monitor Supplier's compliance with this DPA through measures that may include manual reviews, automated scans, penetration tests, regular assessments, audits, or technical or operational testing. Supplier shall cooperate fully with any audit initiated by GFS, provided that such audit will not unreasonably interfere with the normal conduct of Supplier's business. Supplier shall provide audited results with sufficient detail to understand findings, related risks, and remediation requirements. Unless otherwise required by law, GFS shall provide Supplier no less than 10 days prior notice of any such audit and shall not audit Supplier more

than twice per twelve month period, except that GFS may audit at any time in the event of a Security Incident, as required by a regulator or in connection with the defense of GFS's legal rights. Should the results demonstrate a material failing in Supplier's compliance with this DPA, Supplier shall work in good faith with GFS to remediate such issues to GFS's satisfaction.

3.4 ***Compliance Remediation; Termination Rights***. Supplier agrees to notify GFS without undue delay if Supplier determines that it can no longer meet its obligations under Privacy Laws and the present DPA. Upon receiving notice from Supplier pursuant to this subsection, GFS may direct Supplier to take steps as reasonable and appropriate to remediate unauthorized use of Covered PI or terminate the Agreements.

3.5 ***Subcontractors; Sub-processors.***

1. ***Appointment of Sub-Processors***. Supplier shall have the right to engage sub-processors in connection with the performance of its Services hereunder ("**Sub-processors**"). Prior to the start of any processing of Covered PI by Supplier hereunder, Supplier must provide to GFS the current list of Sub-processors engaged in processing Covered PI for each applicable Service, including a description of their processing activities and countries of location. Supplier shall notify GFS in writing (email sufficient) of any changes concerning the addition or replacement of Sub-processors engaged to process Covered PI. Further, Supplier shall ensure that Supplier's Sub-processors who process Covered PI on Supplier's behalf agree in writing to the same restrictions and requirements that apply to Supplier in this DPA and the Agreements with respect to Covered PI. Supplier shall remain fully liable to GFS for the acts and omissions of its Sub-processors.

2. ***Right to Object***. GFS may object in writing to Supplier's appointment of a new subcontractor or sub-processor on reasonable grounds relating to data protection by notifying Supplier in writing within 30 calendar days of receipt of notice in accordance with Section 3.5. In the event GFS objects, the Parties shall discuss GFS's concerns in good faith with a view to achieving a commercially reasonable resolution. If no such resolution can be reached, Supplier will, in its sole discretion, either not appoint the subcontractor or sub-processor or permit GFS to terminate the Agreements, in such case refunding GFS for any prepaid unused fees.

3.6 ***Re-identification***. Supplier will not, and will not allow its subcontractors or sub-processors to, re-identify any de-identified, anonymized, or pseudonymized data derived from Covered PI that is processed by Supplier on behalf of GFS, unless instructed by GFS in writing (email is sufficient).

4. Consumer Requests

4.1 ***Fulfillment of Consumer Requests***. Supplier will implement and maintain sufficient processes and procedures to satisfy GFS's requests to access, correct, and/or delete Covered PI held by Supplier. Within ten (10) calendar days of a written request from GFS (email is sufficient), Supplier shall, as applicable: (a) securely erase or destroy, or cause to be erased or destroyed, specific pieces of Covered PI, including any copies of such Covered PI maintained by Supplier's subcontractor(s) or sub-processor(s); (b) Provide information requested by GFS about Supplier's processing of the Covered PI; (c) Provide the specific pieces of Covered PI that Supplier and/or one of its subcontractors or sub-processors has collected or otherwise obtained about the consumer on behalf of GFS in a Portable Format; (e) modify, and direct its subcontractors or sub-processors to modify, specific pieces of Covered PI; or (f) limit processing of Covered PI defined in Privacy Laws as "sensitive personal information" or "sensitive data," in accordance with the instructions of GFS.

4.2 ***Referral of Direct Requests***. Supplier must refer to GFS applicable consumer requests submitted directly to Supplier for Covered PI and not to respond to any such requests other than to notify requester that the request is referred to GFS.

5. Security Controls

5.1 ***Duty of Confidentiality***. Supplier, its employees, specialists, subcontractors, and sub-processors are subject to a duty of confidentiality with respect to the Covered PI.

5.2 ***Security Measures***. Supplier shall implement and maintain reasonable technical and organizational security measures, procedures, and practices appropriate to the nature of the Covered PI to protect such Covered PI from unauthorized access, destruction, use, modification, or disclosure ("**Security Measures**"). Such Security Measures shall meet or exceed applicable industry standards (e.g., NIST Cybersecurity Framework) and any obligations set forth in the Agreements or applicable law. Supplier shall comply with the requirements of the **Security Exhibit** attached hereto.

5.3 ***Security Incident***.

(a) ***Notification***. Supplier will inform GFS within twenty-four (24) hours of Supplier's suspected unauthorized access, destruction, use, modification, or disclosure (each, a "**Security Incident**") of any Covered PI. Supplier will notify GFS via email with read-receipt to **privacy@gfs.com** and a copy to **legal@gfs.com** and Supplier's primary business contact at GFS. Supplier shall: (i) provide GFS with the name and contact information for an employee of Supplier who shall serve as GFS's primary security contact and shall be available to assist GFS twenty-four (24) hours per day, seven (7) days per week as a contact in resolving obligations associated with a Security Incident. Written notification provided pursuant to this paragraph will include a brief summary

of the available facts, the status of Supplier's investigation, and if known and applicable, the potential number of persons affected by release of data relating to such person.

(b) ***Management & Remediation***. Supplier will provide GFS with any information and cooperation reasonably requested by GFS regarding such Security Incident, including providing GFS or its designated forensic investigator reasonably acceptable to Supplier with physical access to the facilities and operations affected, facilitating interviews and making available relevant records, logs and other materials reasonably required by GFS. Supplier shall immediately remedy any Security Incident at its own expense in accordance with applicable laws. Supplier shall reimburse GFS for actual costs incurred by GFS in responding to, and mitigating damages caused by, any Security Incident, including all costs of notice and remediation. Unless required by law, Supplier shall not inform any third party of any Security Incident without written approval of GFS. Further, Supplier agrees that GFS shall have the sole right to determine whether notice of the Security Incident is to be provided, the contents of such notice, and the nature and extent of any remediation.

5.4 ***Oversight***. Upon request and on an annual basis, Supplier will provide GFS with the results of any audit(s) performed (e.g., SOC1, SOC2, ISO27001, etc) by or on behalf of Supplier that assesses the effectiveness of Supplier's information security program as relevant to the security and confidentiality of Covered PI ("Controls Report"). Supplier shall ensure that each subcontractor or sub-processor makes available to GFS a Controls Report on an annual basis or following a Security Incident.

6. Inquiries

6.1 ***Notification of Regulatory Inquiry***. Supplier shall notify GFS of any regulatory inquiry or correspondence regarding Covered PI (an "**Inquiry**") within three (3) calendar days of receiving such Inquiry. Supplier shall provide GFS with all copies of documents and correspondence relating to the Inquiry without unduly delay.

6.2 ***Response to Inquiry***. Supplier shall not disclose any confidential information of GFS or any affiliated party to the applicable authority without GFS's prior written consent. Supplier shall take all other measures necessary to respond to or otherwise address the Inquiry adequately and in a timely manner.

7. Miscellaneous

7.1 ***Severability***. If any provision of this DPA shall be found to be void by a court of law, such provision shall be deemed to be severable from the other provisions of this DPA, and the remainder of this DPA shall be given effect, as if the Parties had not included the severed provision.

7.2 ***Seizure or Confiscation***. If any Covered PI may be endangered by seizure or confiscation, insolvency proceedings (including a sale) or composition proceedings, or any other events or measures taken by a third party, Supplier shall inform GFS with reasonable advance notification. In addition, Supplier shall inform any such third party that sovereignty and ownership of the Covered PI belong to GFS.

7.3 ***Survival***. All representations, warranties, and indemnities shall survive the termination and/or expiration of this DPA and shall remain in full force and effect. All of a Party's rights and privileges, to the extent they are fairly attributable to events or conditions occurring or existing on or prior to the termination and/or expiration of this DPA, shall survive termination and shall be enforceable by that Party.

7.4 ***General***. Except as expressly set forth herein, the terms of the Agreements shall remain unmodified and in full force and effect. In the event of a conflict between the terms of the Agreements and the terms of this DPA, the terms of this DPA shall control unless the Agreement(s) includes a specific cross-reference to the section of DPA intended to be modified. Headers are for convenience and do not affect the interpretation of the terms of this DPA.

SECURITY EXHIBIT

1. ***Policies and Procedures***. Supplier shall maintain and ensure compliance with Supplier's written security management policies and procedures ("**Supplier Policies**") to prevent, detect, contain, and correct violations of measures taken to protect the confidentiality, integrity, or availability of Supplier information systems that store, process, transfer or access GFS's confidential information ("**Supplier Systems**"). Supplier Policies shall at minimum: (i) to the extent Supplier has access to Covered PI, treat Covered PI at all times as highly sensitive information; (ii) include a formal risk management program, which includes periodic risk assessments; and (iii) provide an adequate framework of controls that safeguard Supplier's Systems, including without limitation any hardware or software supporting GFS and GFS's confidential information.

2. ***Security Evaluations***. Supplier shall annually conduct and document technical security assessment of its Supplier Policies and Supplier Systems to ensure continued compliance with the obligations set forth in this Schedule and as otherwise imposed by law. Such evaluations shall ensure that GFS's confidential information is stored confidentially and in a secure manner within Supplier Systems and evaluate the maintenance and structure of Supplier's Systems.

3. ***Certifications***. Upon GFS's written request, Supplier shall provide GFS with the results of any audit performed by or on behalf of Supplier that assesses the effectiveness of Supplier's information security program as relevant to the security and confidentiality of Covered PI shared during the course of the Agreement ("**Controls Report**"). Supplier shall ensure that each Sub-processor prepares and makes available to GFS a Controls Report on an annual basis or following a Security Incident.

4. ***Physical Security***. Supplier shall maintain appropriate physical security controls (including facility and environmental controls) to prevent unauthorized physical access to Supplier Systems.

5. ***Access Limitation***. Supplier shall implement appropriate access controls restricting access to Covered PI to only such employees, specialists, subcontractors, and sub-processors as need to know the information in order to perform their obligations in

furtherance of the Agreements.

6. ***Visitor Access Logs***. Supplier shall maintain sign in access logs for visitors and guests ("**Supplier Guest Log**") and ensure that such visitors and guests are escorted while in any facility that allows either physical or virtual access to Supplier's Systems and maintain Supplier Guest Log in a secure location for a minimum of three (3) months.

7. ***Perimeter Controls***. Supplier shall maintain reasonable network perimeter controls such as firewalls at all perimeter connections to Supplier's Systems.

8. ***Vulnerability Management and Testing***. Supplier shall employ reasonable vulnerability management processes to mitigate data security risks, including, without limitation, mitigation steps to resolve issues identified by Supplier, GFS, or as required by law. Supplier shall permit security vulnerability testing by GFS and its approved third parties for the purpose of identifying public facing security vulnerabilities in Supplier's web functionality used by GFS, and GFS's customers, clients and independent contractors, provided such testing shall be subject to GFS providing reasonable prior notice and Supplier obtaining any necessary consents from its hosting platform provider.

9. ***System Hardening***. Supplier's configuration parameters for Supplier Systems shall include procedures to disable all unnecessary services on devices and servers and shall be applied to all Supplier Systems that access, transmit or store GFS's confidential information.

10. ***Patch Management***. Supplier shall establish and adhere to Supplier Policies for patching Supplier Systems which ensure all Supplier Systems are maintained at current stable patch level.

11. ***Virus Detection***. Supplier shall install commercially reasonable malicious code detection software, to include virus detection and malware detectors, on all systems vulnerable to malware that are used to access, process or store GFS's confidential information, and Supplier shall keep antimalware virus signatures up to date.

12. ***System Logs***. Supplier shall maintain system logs that uniquely identify individual users and their access to associated systems and identify the attempted or executed activities of such users. All systems creating system logs shall be synchronized to a central time source. Supplier shall identify, investigate and respond to any suspicious or malicious activity identified in such Supplier System log. Supplier shall preserve a security log audit trail for Supplier System. Supplier shall maintain these logs for the longer of the term of the Agreement or for one (1) year, or as otherwise required by law.

13. ***Background Checks***. Supplier shall require all personnel accessing GFS's confidential information via Supplier Systems to complete a background check. Supplier shall further ensure that its personnel engaged in the Processing of GFS confidential information are informed of the confidential nature of the Covered PI, have received appropriate training on their responsibilities and have executed written confidentiality agreements. Supplier

shall ensure that such confidentiality obligations survive the termination of the personnel engagement.

14. ***Change Control Process***. Supplier shall maintain reasonable change control processes to approve and track changes within Supplier's computing environment.

15. ***Protection of Storage Media***. Supplier shall ensure that storage media containing GFS's confidential information is properly sanitized of all GFS's confidential information or is destroyed prior to disposal or re-use for non-Supplier processing. All media on which GFS's confidential information is stored shall be protected against unauthorized access or modification. Supplier shall maintain reasonable and appropriate processes and mechanisms to maintain accountability and tracking of the receipt, removal and transfer of storage media used for Supplier information systems or on which GFS's confidential information is stored.

16. ***System Accounts***. Supplier shall maintain appropriate Supplier Policies for requesting, approving, auditing, and administering accounts and access privileges for Supplier information systems and GFS's confidential information. Supplier personnel who access systems that store, transmit or process GFS's confidential information shall be assigned individual system accounts to ensure accountability for access granted.

17. ***Passwords***. Supplier shall implement appropriate password parameters for systems that access, transmit or store GFS's confidential information ("**Related Systems**"). Supplier shall implement strong two factor authentication and complex passwords ("**Passwords**") for all network and systems access to Related Systems. Supplier shall adhere to industry standard password practices. Default manufacturer passwords used in Supplier's products shall be changed upon installation.

18. ***Business Continuity***. Supplier shall ensure that it has adequate processes and procedures that will enable a business to sustain the service in the event of a disaster ("**Business Continuity Plans**") in place to ensure its compliance with the terms of this DPA and shall review and test plans no less than annually.

19. ***Data Destruction***. All GFS's confidential information shall be securely destroyed once it is no longer needed via commercially reasonable processes. Supplier's strategy for data destruction must be documented and include logs for all GFS's confidential information destroyed, which shall be available for GFS's review.

20. ***Payment Card Industry Data Security Standards (PCI DSS) Compliance***. With respect to the Services, to the extent applicable, Supplier shall maintain the required level of PCI DSS compliance and certification, and shall provide related documentation upon GFS's request. Supplier is responsible for the security of cardholder data that it encounters, uses and/or maintains pursuant to this DPA or in order to provide the Services. Supplier is required to implement and maintain reasonable security measures. These security measures should be appropriate in light of the sensitivity of the information and should protect the information from unauthorized access, use or disclosure.