1. Definitions. The following words and phrases when used in this Agreement shall have the following meanings:

1.1. “Affiliate” of a Party means any other Party that directly or indirectly, through one or more intermediaries, controls, is controlled by, or is under common control with, such Party.

1.2. “Agreement” means all agreements between Aramark and Provider, including but not limited to master service agreements, order forms, purchase orders, browse-wrap, shrink-wrap, click-wrap, and other terms.

1.3. “Aggregated and Anonymized Information” means Aramark Information that has been aggregated and/or anonymized to the extent that it cannot be attributed to an identifiable individual, Aramark, or an Aramark Client.

1.4. “Aramark” means Aramark Services, Inc. and its Affiliates.

1.5. “Aramark Client(s)” means the client(s) of Aramark on whose behalf Aramark is procuring the Services.

1.6. “Aramark Information” means any and all information, data, materials, works, expressions, or other content, that is (a) related to Aramark, Aramark’s Affiliates, Aramark’s customers and/or Aramark’s Clients, (b) uploaded, submitted, posted, transferred, transmitted, or otherwise provided or made available by or on behalf of Aramark, Aramark’s Affiliates, Aramark’s customers, and/or Aramark Clients for use by or through the Services, or (c) collected, or otherwise received by Provider in connection with the Services. All output, copies, reproductions, improvements, modifications, adaptations, translations, and other derivative works of, based on, derived from, or otherwise using any Aramark Information are themselves also Aramark Information. For the avoidance of doubt, Aramark Information includes all Personal Information.

1.7. “Aramark Systems” means any computer, network, application, imaging device, storage device, mobile computing device or software owned, licensed or leased by Aramark or an Aramark Client, or operated by a Third Party on behalf of Aramark or an Aramark Client.

1.8. “CCPA” means the California Consumer Privacy Act, California Civil Code Section 1798.100 et. seq., including all regulations enacted therewith, and as may be amended, supplemented, or replaced from time-to-time.

1.9. “Data Subjects” means a Consumer under the CCPA, a Data Subject under the GDPR, or other natural person granted similar rights under other Privacy and Security Rules.

1.10. “GDPR” means the General Data Protection Regulation (EU) 2016/679, including all regulations enacted therewith, and as may be amended, supplemented, or replaced from time-to-time.

1.11. “Industry Standards” means standards, safeguards and best practices of the industry in which Provider operates relating to the privacy, confidentiality or security of Aramark Information including, without limitation, the ISO 27000 series, the NIST 800 series, and the standards and practices employed by industry peers, as such are updated from time to time.

1.12. “Information Security Incident” means any actual or reasonably suspected: (i) loss or theft of Aramark Information; (ii) unauthorized use, disclosure, destruction, loss alteration or acquisition of or access to, or other unauthorized Processing of Aramark Information; or (iii) unauthorized access to or use of, inability to access, or malicious infection of Aramark Systems or Provider Systems that reasonably may compromise the privacy or confidentiality of Aramark Information.

1.13. “Information Security Program” means Provider’s technological, physical, administrative and procedural safeguards, including without limitation, policies, procedures, guidelines, practices, standards and controls that (i) ensure the confidentiality, security, integrity and availability of Aramark Information; (ii) protect against any anticipated threats or hazards to the security, confidentiality or integrity of Aramark Information; and (iii) protect against any Information Security Incident.

1.14. “Losses” means any and all losses, damages, liabilities, deficiencies, claims, actions, judgments, settlements, interest, awards, penalties, fines, costs, or expenses of whatever kind, including attorneys’ fees, fees, the cost of enforcing any right to indemnification hereunder, and the cost of pursuing any insurance providers.

1.15. “Personal Information” means any information that Provider or Provider Resource Processes in connection with this Agreement that (a) identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular individual or household, (b) is protected under Privacy and Security Rules, or (c) that is linked or combined with information identified in (a) or (b) above, whether such information is in individual or aggregate form and regardless of the media in which it is contained.

1.16. “Privacy and Security Rules” means all laws and regulations of any country or jurisdiction applicable to the Processing of Personal Information under the Agreement, including privacy and information security laws, regulatory guidance that apply to the conduct of either Party under the Agreement, Industry Standards, and Aramark or Aramark Client requirements.
1.17. “Process” (or “Processes” or “Processing”) means to perform any operation or set of operations upon Aramark Information, whether manually or by automatic means, including but not limited to collection, recording, sorting, structuring, accessing, storage, adaptation or alteration, retrieval, consultation, use, transfer, dissemination.

1.18. “Provider” means the entity that executed the Agreement together with its Affiliates.

1.19. “Provider Personnel” means all employees, agents, and contractors of Provider involved in the performance of Services.

1.20. “Provider Resource(s)” means any Third Party who works on behalf of Provider in connection with Provider’s performance of the Services, including any affiliate, Data Processor, Sub-Processor or subcontractor that Processes or is authorized to Process Aramark Information.

1.21. “Provider Systems” means any computer, computer network, computer application, imaging device, storage device, mobile computing device or software owned, leased or controlled by Provider, or operated by a Provider Resource, that processes Aramark Information or is connected to any Aramark Systems.

1.22. “Securely Dispose” means to ensure that all hardcopy and electronic information (e.g., papers, files, and media) is rendered permanently and completely unreadable and indecipherable.

1.23. “Services” means all services and/or products supplied by Provider to Aramark.

1.24. “Third Party” means any person or entity other than Aramark and Provider.

1.25. The terms “Business”, “Service Provider”, “Data Controller”, “Data Processor”, “Sub-Processor”, and “Supervisory Authority” shall have the same meaning as in the GDPR or the CCPA.

2. Aramark Information

2.1. Roles of the Parties. As between Aramark and Provider, Aramark is and will remain at all times the Data Controller or Data Processor to the extent the GDPR applies and the Business or Service Provider to the extent the CCPA applies with regard to the Processing of Aramark Information. Provider is the Data Processor or Sub-Processor to the extent the GDPR applies and Service Provider to the extent the CCPA applies with regard to Processing of Aramark.

2.2. Processing by Provider. Provider shall solely Process Aramark Information in accordance with Aramark’s instructions and the Privacy and Security Rules, and only to the extent necessary to provide the Services and as specified in Attachment DPA-1 (Data Processing Details). For the avoidance of doubt, Provider shall not Process for marketing purposes, sell, aggregate, analyze or anonymize, or otherwise use, any Aramark Information unless specified in Attachment DPA-1. Provider shall not knowingly perform the Services in a manner that causes Aramark to violate Privacy and Security Rules. Where Provider believes that compliance with any Aramark instruction infringes Privacy and Security Rules, Provider shall immediately notify Aramark. Upon Aramark’s request, the Provider shall provide Aramark with all information necessary for maintaining a record of Processing activities in accordance with art. 30 (1) GDPR. Provider will not: (i) retain, use or disclose the Aramark Information for any purpose other than for the purposes set forth in the instructions and in this Section 2.2 (including in Attachment DPA-1), (ii) sell such information, as such term is defined in the CCPA (iii) retain, use or disclose the Aramark Information outside of the direct business relationship between Aramark and Provider or (iv) use Aramark Information for another business or person unless necessary to detect information security incidents, or protect against fraudulent or illegal activity.

2.3. Aggregated and Anonymized Information. To the extent Provider or Provider Resources Processes Aggregated and Anonymized Information, Provider represents and undertakes as follows:

2.3.1. Provider shall not make any attempts to re-identify the Aggregated and Anonymized Information;

2.3.2. Provider has implemented and will maintain technical safeguards that prohibit re-identification of Aggregated and Anonymized Information;

2.3.3. Provider has implemented and will maintain business processes that prohibit re-identification of Aggregated and Anonymized Information and prevent inadvertent release of Aggregated and Anonymized Information; and

2.3.4. Provider will periodically reassess its technical safeguards and processes to ensure that they are still adequate to prevent the re-identification or the inadvertent release of Aggregated and Anonymized Information.

2.4. Processing by Third Parties. Provider will not permit any Third Party to Process Aramark Information, except as required by applicable law or as expressly permitted in the Agreement. To the extent required by applicable law, Provider may disclose Aramark Information after providing Aramark with written notice. Provider shall provide reasonable cooperation to prohibit or limit the disclosure of Aramark Information through protective order or similar mechanism.

2.5. Transfer outside the United States. Provider shall ensure that no Aramark Information is transferred to, accessed by, or otherwise Processed by Provider Personnel or Provider Resources in any country other than the United States, other than as set forth in Attachment DPA-1.

2.6. Information Destruction or Return. Promptly after (i) Provider no longer needs to Process the Aramark Information to perform the Services, (ii) the Agreement terminates or expires, or (iii) Aramark’s written request, Provider shall return to Aramark, and require all Provider Resources to return to Aramark, all originals and copies of all Aramark Information.
Following the return of such information, Provider shall Securely Dispose of such information from all systems it directly or indirectly controls (including those of Third Parties). Provider shall provide a written statement to Aramark certifying that it has complied with the requirements in this section. Provider shall not be required to return, destroy, or erase any Aramark Information if prohibited by applicable law, in which case the Provider shall retain, in its then current state, all such Aramark Information within its control or possession in accordance with the Agreement and perform its obligations under this Agreement as soon as such law no longer prevents it from doing so, provided that for as long as the Aramark Information is stored by Provider, Provider shall only make such use of the Aramark Information as required by law.

2.7. Suspension of Information Destruction. Upon Aramark’s reasonable request, Provider will immediately suspend any deletion, destruction, or modification practices, or take other reasonable actions such as copying or imaging appropriate storage devices and maintaining activity logs for an extended period of time, so as to preserve such information.

3. Data Subjects Rights. Provider shall notify Aramark within 24 hours of receiving a Data Subject request or any other request or complaint of a Data Subject relating to Aramark Information. Provider shall not respond to any such Data Subject request without Aramark’s prior written instructions. In the event of such a request or complaint, Provider shall cooperate with Aramark and take such action as Aramark may reasonably request to allow Aramark to fulfill its obligations to Aramark Clients or under Privacy and Security Rules. Provider shall cooperate with Aramark to promptly and effectively (a) provide access to, change, block, retain, use, return, Securely Dispose of, mask, disclose, transfer, and/or encrypt any Aramark Information, in any manner reasonably requested by Aramark; and (b) process enquiries, complaints and claims relating to Aramark Information from any government official, authority, or Third Parties.

4. Provider Resources.

4.1. Provider may only utilize Provider Resources to perform its obligations under the Agreement, including Processing of Aramark Information, if (i) there is a legitimate business need for Provider Resources to Process Aramark Information in order for Provider to perform the Services; (ii) the Providers Resources are identified in accordance with Section 4.2, and (iii) the Provider Resources are bound in writing to materially consistent obligations as those to which Provider is subject under this Agreement, including but not limited to Section 9 (EU Transfer).

4.2. Attachment DPA-2 sets forth all Provider Resources and their locations. Any changes to this list must have Aramark’s prior written approval and must be memorialized in an amendment to this Schedule DPA.

4.3. Provider is solely responsible for any Processing of Aramark Information under the control or possession of Provider or any Provider Resources, including all acts or omissions of any Provider Resources. For the avoidance of doubt, all obligations in the Agreement imposed on Provider’s Processing of Aramark Information also apply to Provider Resources’ Processing of Aramark Information. Provider shall remain fully liable to Aramark for the Provider Resources’ acts and omissions, and for the Provider Resources’ performance of any obligations under the Agreement.

4.4. Provider shall conduct regular documented assessments of its Provider Resources (prior to engagement and at reasonable intervals thereafter), consistent with Industry Standards, to ensure that the Provider Resources are capable of complying with requirements regarding the privacy, confidentiality and security of Aramark Information that are at least as protective of Aramark Information as the requirements imposed on Provider under the Agreement and this Schedule DPA. Provider shall provide to Aramark, upon request, written evidence of such investigations.

5. Information Protection and Security

5.1. Security. Provider shall take appropriate administrative, technical, and physical safeguards, including without limitation, policies, procedures, guidelines, practices, standards and controls, to ensure the integrity, availability, security and resilience of Provider’s Systems used for Processing Aramark Information, to ensure that there are no Information Security Incidents, and to protect against the destruction, loss, alteration, unauthorized disclosure of, or access to Aramark Information, as appropriate to the nature and scope of Provider’s activities and Services, and as reasonably requested by Aramark. Without limiting the generality of the foregoing, Provider shall comply with the requirements in Attachment DPA-3 (“Security Terms”).

5.2. Information Security Warranties. Provider represents and warrants that:

5.2.1. it has in place and will maintain a comprehensive, written Information Security Program based on Industry Standards and applicable law, and pursuant to which it has implemented administrative, technical and physical safeguards (“Safeguards”) designed and tested in accordance with Industry Standards to: (1) ensure the confidentiality, integrity, availability and security of Aramark Information; (2) protect against any foreseeable threats or hazards thereto; (3) protect against unauthorized, accidental or unlawful access to or use of Aramark Information, Aramark Systems, and Provider Systems; (4) protect against unauthorized, accidental or unlawful destruction, loss, alteration, encryption or misuse of Aramark Information; (5) ensure that Providers Personnel and Provider Resources are appropriately trained to maintain the confidentiality, integrity, availability and security of Aramark Information and the Privacy and Security Rules; and (6) ensure that Providers Personnel and Provider Resources authorized to process Aramark Information are
6. **Information Protection Oversight**

6.1. **Provider Review.** Provider will regularly assess, test, and monitor the effectiveness of the Information Security Program’s key controls, systems, and procedures. Provider will conduct information security risk assessments of the physical and logical security measures and safeguards it maintains, as applicable to its protection of Aramark Information. Such assessments
shall be conducted at least annually and whenever there is a material change in Provider’s business or technology practices that may negatively impact the privacy, confidentiality, security, integrity or availability of Aramark Information. At least quarterly, Provider shall perform vulnerability tests and assessments against all systems Processing Aramark Information. At least annually, Provider shall perform penetration tests against any internet-facing systems used in connection with the Services. Upon Aramark’s request, Provider shall provide a summary of such assessments and tests, including a description of any significant risks identified and an overview of the remediation efforts undertaken to address such risks. Such assessments and tests should be conducted by independent third parties or internal personnel independent of those who develop or maintain the organization’s information systems or information security program. If any audit results in Provider being found that Provider is, or that a service is, not in compliance with Privacy and Security Rules, Provider shall immediately take all corrective actions necessary to henceforward comply with these provisions, and shall comply with the instructions given by Aramark in this regard.

6.2. Aramark Review. Aramark, at its sole expense, may inspect or have its authorized representatives inspect (i) Provider’s Information Security Program, including data centres or premises where the Aramark Information is stored or accessed; and (ii) Provider’s Processing practices. Further, upon the provision of reasonable notice to Provider, and (i) at least once per calendar year during the Term; (ii) following an Information Security Incident; (iii) following any adverse assessment, scan or audit of Provider Systems; (iv) following any discovery or reasonable suspicion by Aramark that Provider is not in compliance with the Agreement; or (v) as requested, demanded or required by any regulator or government body or by applicable laws, Aramark or its designee or a regulator may undertake a security assessment, network scan, forensic investigation, and/or audit of Provider Systems and Information Security Program and Provider shall provide to Aramark, its authorized representatives and designees: (a) reasonable access to Provider’s Information Security Program; (b) reasonable assistance and cooperation of Provider’s relevant staff; and (c) reasonable facilities at Provider’s premises. Aramark can contest the scope, methodology and results of any such audit and may request Provider to take measures following the results of such audit. In the event an audit identifies control gaps in the environment Processing Aramark Information, Provider shall promptly notify Aramark, provide a resolution plan, and remediate such gaps within an agreed-upon timeframe, and reimburse Aramark for all reasonable assessment costs incurred by Aramark.

6.3. Reports. Provider will, on or before November 1 of each calendar year, deliver to Aramark, at Provider’s sole cost and expense, Provider’s Service Organization Control (“SOC”)-1 Type II report and SOC-2 Type II report, each prepared by a reputable, qualified, independent third party audit firm (such as KPMG or comparable firm), dated no earlier than 365 days from Aramark’s receipt of the applicable report, and covering at least a nine (9) month period.

6.4. Interviews and Questionnaires. Provider shall make relevant personnel available for interviews and provide all information and assistance reasonably requested by Aramark regarding Provider’s Processing of Aramark Information. Upon Aramark’s request, Provider will promptly complete a questionnaire regarding Provider’s Processing of Aramark Information. In addition, Provider shall provide Aramark with any documents requested by Aramark related to the foregoing, including without limitation, any security assessment and security control audit reports. Aramark shall make such a request no more than once a year, except in the event of an Information Security Incident. If any assessment requested by Aramark shows a material breach by Provider of the Agreement; or (v) as requested, demanded or required by any regulator or government body or by applicable laws, Aramark or its designee or a regulator may undertake a security assessment, network scan, forensic investigation, and/or audit of Provider Systems and Information Security Program and Provider shall provide to Aramark, its authorized representatives and designees: (a) reasonable access to Provider’s Information Security Program; (b) reasonable assistance and cooperation of Provider’s relevant staff; and (c) reasonable facilities at Provider’s premises. Aramark can contest the scope, methodology and results of any such audit and may request Provider to take measures following the results of such audit. In the event an audit identifies control gaps in the environment Processing Aramark Information, Provider shall promptly notify Aramark, provide a resolution plan, and remediate such gaps within an agreed-upon timeframe, and reimburse Aramark for all reasonable assessment costs incurred by Aramark.

7. Information Security Incident

7.1. Appointment of Primary Contact. In the event of an Information Security Incident, Provider will (a) appoint a primary contact to assist Aramark in resolving issues associated with an Information Security Incident, and (b) send Aramark the primary contact’s name and contact information.

7.2. Notification of Information Security Incident. Provider shall notify Aramark immediately (and in no event later than within 24 hours) of any suspected Information Security Incident via email, with the words “Information Security Incident” in the subject line, to securityassurance@aramark.com and with a copy, to Provider’s primary business contact within Aramark.

7.3. Investigation & Coordination. Provider will immediately investigate any Information Security Incident and provide updates and a final report to Aramark. In the event the Information Security Incident involves Personal Information, such updates shall include the following information as it becomes available: root cause analysis, description of the nature of the Information Security Incident, categories and approximate number of individuals impacted, categories and approximate number of data records concerned, location/residency of impacted individuals, measures taken to mitigate impact of Information Security Incident, and other information as requested by Aramark. Without limiting the foregoing, Provider also agrees to fully cooperate with Aramark in Aramark’s handling of an Information Security Incident, including in any Aramark...
investigation of the same, facilitating coordination between Aramark and Provider Resources and Third Parties, and making available all relevant records, logs, files, data reporting or other information as requested by Aramark.

7.4. Remediation. Provider will take, at its sole cost, immediate steps to remedy any Information Security Incident, including properly documenting responsive actions taken. Provider will reimburse Aramark for expenses reasonably incurred by Aramark in connection with an Information Security Incident, including (i) expenses to provide warning or notice of the Information Security Incident to affected individuals and entities, regulators, law enforcement agencies, consumer reporting agencies, the media, and other third parties; (ii) expenses to investigate, assess or remediate the Information Security Incident; (iii) expenses to hire any public relations consultants to respond to the Information Security Incident; (iv) expenses to provide credit monitoring services to individuals affected by the Information Security Incident; (v) expenses to retain a call center to respond to inquiries regarding the Information Security Incident; (vi) expenses to respond to or address any investigation by regulators, law enforcement agencies, or other Third Parties; and (vii) expenses related to remediation actions required by applicable law. The Parties hereto agree that this section is not a liquidated damages provision and shall in no way or manner limit any amounts payable to, or recovery by, Aramark. Further, Provider will promptly take all appropriate actions to prevent a recurrence of the Information Security Incident. As part of the remediation, Aramark may suspend Provider’s Processing of Aramark Information, terminate Provider’s connectivity with Aramark Systems, or request other appropriate actions.

7.5. Third Party Notifications. Except as may be strictly required by Privacy and Security Rules, Provider will not inform any Third Party of any Information Security Incident without first obtaining Aramark’s prior written consent. If Privacy and Security Rules require Provider to independently notify a Third Party of an Information Security Incident, and do not permit Provider to delegate such duty to Aramark, Provider will inform Aramark in writing of such obligation prior to notifying the Third Party. Provider will fully cooperate with Aramark in connection with issuing any notice related to the Information Security Incident. Aramark will have the sole right to determine: (a) whether notice of the Information Security Incident is to be made; (b) the contents of such notice; (c) whether any type of remediation may be offered to affected persons; and (d) the nature and extent of any such remediation. Any such notice or remediation will be at Provider’s sole cost and expense.

7.6. Coordination – Litigation. Provider shall cooperate with Aramark in any litigation or other formal action by or against Third Parties arising from an Information Security Incident.

8. Insurance. Provider will maintain insurance for Cyber Liability and/or Professional Liability / Errors & Omissions Liability as appropriate to provide coverage for the Services contemplated and obligations assumed under this Agreement and Schedule DPA. The policy(ies) will cover the liability of Aramark and its Affiliates by reason of any actual or alleged error, omission, negligent act, or wrongful act of Provider committed in rendering or failing to render any products or services, including Services provided in accordance with the Agreement and the obligations agreed to in this Schedule DPA. The liability will include but is not limited to damage to and loss of intangible property, including any Aramark Information that is lost or incorrectly transmitted or recorded (including unauthorized access and use, transmission, or disclosure of Aramark Information), failure of security, breach of confidential information, privacy perils, as well as breach mitigation costs, regulatory coverage (including fines and penalties) and defense costs. The policy(ies) shall provide limits of not less than ten million US dollars ($10,000,000) per claim (or local currency coverage of an equivalent value). Upon termination of the Agreement, Provider will maintain an active policy, or purchase an extended reporting period providing for claims first made and reported to the insurance company within four (4) years after final payment for Services. Aramark and its Affiliates will be named as additional insureds. Provider shall ensure that any insured vs. insured exclusion will have a carve-back for those added as additional insureds under the policy. Provider shall waive any right of subrogation of the insurers against Aramark or any of its Affiliates.

9. Transfer of Information under the GDPR. If and to the extent that Provider Processes any Personal Information: (a) originating from, or on behalf of, an Aramark Affiliate established in a Member State of the European Economic Area or Switzerland or in the United Kingdom; or (b) of Data Subjects located in a Member State of the European Economic Area or Switzerland or the United Kingdom (as indicated by the Services, or by Aramark), Provider shall implement EU Standard Contract Clauses or another mechanism acceptable under applicable Data Protection Laws for the cross border transfer as required by Chapter V of the GDPR or other applicable Data Protection Laws, if applicable. “Standard Contractual Clauses” means the Standard Contractual Clauses published in European Commission decision C(2010) 593 for the transfer of personal data to processors established in third countries, which are available at https://ec.europa.eu/info/law/law-topic/data-protection_en (as amended or updated from time to time).

10. Onward transfer: If the Parties are relying on the Standard Contractual Clauses for the onward transfer of such data then the following shall be included in the agreement between Provider and the Sub-Processor in addition to all requirements of Art 28.

10.1. The Sub-Processor agrees to comply with the clauses of the Standard Contractual Clauses that are applicable to sub-processors, these being Clauses 1, 3, 5, 6, 7, 8(2), 8(3), 9, 10, 11 and 12 and appendices 1 and 2 (the “Sub-processor Clauses”), for the transfer of Personal Information to processors established in third countries which do not ensure an adequate level
of data protection. Such Sub-Processor Clauses are hereby incorporated by reference as through fully rewritten herein. The Sub-Processor Clauses are governed by the law of the member state in which the relevant Controller is established.

10.2. The Sub-Processor agrees to comply with the obligations described in the Sub-Processor Clauses even if Personal Information is processed in an Adequate Country (as such term is defined under the GDPR).

10.3. Where the Sub-Processor Clauses Sub-Processor Clauses contain any obligation to notify the "Data Exporter" (as such term is defined in the Sub-Processor Clauses), such notification shall be made via Aramark.

11. Co-operation with Regulators and Conduct of Claims

11.1. Provider shall promptly notify Aramark of all inquiries or requests from a regulator or a governmental authority ("Regulator") that Provider receives related to Aramark Information, the provision or receipt of the Services or either party’s obligations under this Agreement, unless prohibited from doing so by applicable law. If Provider or Aramark receives such an inquiry or request from a Regulator, Provider shall to the extent permitted by applicable law: (i) promptly provide Aramark with such information as Aramark may reasonably request to satisfy such inquiry or request, and (ii) co-operate with Aramark’s efforts, if any, to prevent disclosure, or obtain protective treatment.

11.2. Unless Aramark notifies Provider that Provider will be responsible for handling a communication or correspondence with a Regulator or a Regulator requests in writing to engage directly with Provider, Aramark will handle all communications and correspondence relating to Aramark Information or the Services.

11.3. Aramark shall have the right, at its sole discretion, to assume control of the defence and settlement of any governmental or regulatory proceeding or third-party claim that relates to Aramark Information, provided that Aramark shall not enter into any compromise or settlement of such claim or compromise any such claim without Provider’s prior written consent if such compromise or settlement would assert any liability against Provider, increase the liability of Provider, or impose any obligations or restrictions on Provider. Where required, such consent shall not be unreasonably withheld or delayed. Aramark’s exercise of its rights under this section shall be without prejudice to its contractual, legal, equitable or other rights to seek recovery of such costs.

11.4. Provider shall provide Aramark with such assistance and information as Aramark may reasonably request in order for Aramark to comply with any obligation to carry out a data protection impact assessment or consult with a Regulator pursuant to Articles 35 and 36 of the GDPR.

12. Termination. This Schedule DPA will terminate upon the earliest of: (i) termination or expiration of the Agreement; or (ii) as agreed by the Parties in writing. Upon termination, Provider shall cease Processing all Aramark Information and comply with its obligations under Section 2.5. The obligations set forth in this Schedule DPA survive for as long as Provider has access to or Processes any Aramark Information.

13. Precedence. Nothing in this Schedule DPA reduces Provider’s obligations under the Agreement with respect to the protection of Aramark Information or permits Provider to Process Aramark Information in a manner that is prohibited by the Agreement. With regard to the subject matter of this Schedule DPA, in the event of inconsistencies between the provisions of this Schedule DPA and any other agreements between the Parties, including the Agreement and including agreements entered into or purported to be entered into after the date of this Schedule DPA, the provisions of this Schedule DPA shall prevail.


14.1. Aramark’s Affiliates shall have third-party rights in accordance with the Agreement and Data Subjects are granted third-party rights to the extent required by law. All other third-party rights are excluded.

14.2. Notwithstanding anything to the contrary in the Agreement, the rights, remedies and indemnification provisions set forth in this section are not subject to any limitations of liability.

14.3. An Information Security Incident or Provider’s failure to comply with any of the obligations set forth in this Schedule DPA shall be deemed a material breach of this Agreement.

14.4. In addition to any indemnification obligations contained in the Agreement, Provider agrees to indemnify, defend and hold harmless Aramark and its Affiliates, subsidiaries, successors and assigns (and the officers, directors, shareholders, employees, sublicensees, customers, representatives, and agents of Aramark and its affiliates, subsidiaries, successors and assigns) from and against any and all Losses arising from, in connection with, relating to, or based on allegations of (i) any violation of any provision of this Schedule DPA or the Privacy and Security Rules; (ii) the negligence of more culpable conduct of Provider or Provider Personnel; (iii) acts or omissions of Provider Resources; or (iv) any Information Security Incident.

14.5. Aramark may, at its option and expense, participate and appear pari passu with Provider in the defense of any claim related to Aramark Information or this Schedule DPA that is conducted by Provider as set forth herein. Provider may not settle any claim regarding Aramark Information without the prior written approval of Aramark. From the date of written notice by Provider to Aramark of any such claim, Aramark shall may withhold any payments due to Provider under the Agreement to offset its defense costs and for additional reasonable amounts required as security for Provider’s obligations under this Schedule DPA.
Attachment DPA-1
Information Processing Details Addendum

This Attachment forms part of Schedule DPA and must be completed by Provider and sent to Aramark for Aramark’s approval prior to execution of the Agreement.

**Type, Nature and Purpose of the Processing** – Subject to Section 2 of this Schedule DPA, Provider will process Aramark Information solely as necessary to perform the Services pursuant to the Agreement, as further instructed by Aramark in its use of the Services.

**Duration of Processing** – Subject to Section 2 of this Schedule DPA, Provider will Process Aramark Information until the applicable Agreement terminates, or until Provider no longer needs to Process the Aramark Information to perform the Services.

**Categories of Data Subjects** – The categories of Data Subjects may include any of the following:

- Aramark Employees
- Aramark Customers
- Aramark Client Employees

Attachment DPA-2
Provider Resources

Before the effective date of the Agreement, Provider shall email privacy@aramark.com with a list of all Provider Resources that Provider will use in the performance of the Services, detailing the information set forth in the chart below.

<table>
<thead>
<tr>
<th>Authorized Provider Resource</th>
<th>Role / Purpose</th>
<th>Aramark Information Processed</th>
<th>Location (incl. any international data export solution in place)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## Attachment DPA-3
### Security Terms

<table>
<thead>
<tr>
<th>Security Control</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Segregation of Duties</td>
<td>Segregate duties and areas of responsibility of Provider Personnel in accordance with Industry Standards to reduce opportunities for unauthorized or unintentional modification or misuse of Aramark Information of relevant information systems.</td>
</tr>
</tbody>
</table>
| Access Controls      | • Identify the Provider Personnel, classes of such Provider Personnel and Provider Resources whose documented business functions and responsibilities require access to Aramark Information, relevant information systems and Provider’s physical premises;  
                          • Permit access to Aramark Information, relevant information systems and Provider’s premises only to such authorized personnel and third parties;  
                          • Maintain a current record of Provider Personnel and Provider Resources who are authorized to access or otherwise Process Aramark Information, relevant information systems and the Provider’s premises, and the purposes of such access;  
                          • Maintain logical and physical access controls, secure user authentication protocols, secure access control methods, and firewall protection;  
                          • Prevent terminated Provider Personnel and Provider Resources from accessing or otherwise Processing Aramark Information and relevant information systems by taking all necessary actions, including immediately terminating such parties' physical and electronic access to Aramark Information and relevant information systems. |
| Secure User Authentication | Manage and limit access to Aramark Information and relevant information systems by taking all reasonable actions in accordance with Industry Standards, including the following:  
                          • Maintain secure control over user IDs, passwords and other authentication identifiers;  
                          • Require passwords controlling access to Aramark Information to have minimum complexity requirements and be at least 8 characters in length;  
                          • Maintain a secure method for selecting and assigning passwords and use multi-factor authentication and other reasonable authentication technologies;  
                          • Assign unique user identifications and passwords that are not vendor supplied default passwords;  
                          • Require Provider Personnel and Provider Resources to change passwords at regular intervals or based on the number of access attempts, and whenever there is any indication of possible system or password compromise;  
                          • Frequently (and at least every 90 days) change passwords for accounts that have access to Aramark Information;  
                          • Avoid reusing or recycling old passwords;  
                          • Restrict access to Aramark Information and relevant information systems to only active users and accounts;  
                          • Block user access after multiple unsuccessful attempts to login or otherwise gain access to Aramark Information or relevant information systems;  
                          • Terminate user access after a predetermined period of inactivity;  
                          • Promptly revoke or change access in response to personnel termination or changes in job functions. |
| Incident Detection and Response | Maintain policies and procedures to detect, monitor, document and respond to actual or reasonably suspected Information Security Incidents, and encourage the reporting of such incidents, including through:  
                          • Training Provider Personnel and Provider Resources with access to Aramark Information to recognize actual or potential Information Security Incidents and to escalate and notify senior management of such incidents;  
                          • Mandatory post-Security Incident review of events and actions taken concerning the security of Aramark Information;  
                          • Maintain current and regularly reviewed policies governing the reporting of Information Security Incidents to regulators and law enforcement agencies. |
| Encryption            | Apply encryption in accordance with Industry Standards to Aramark Information:  
                          • Stored on laptops, mobile devices, portable storage devices or removable archival media;  
                          • Stored on file servers or in application databases;  
                          • Stored outside of Provider’s organizational physical controls;  
                          • Transmitted across any public network (such as the Internet) or wirelessly;  
                          • Transmitted in email attachments;  
                          • In transit outside of the Provider Systems;  
                          Maintain policies prohibiting such storage or transmission unless required encryption has been applied. |
| Network               | Implement network security controls such as firewalls, layered DMZs and intrusion detection/prevention systems. |

---

DPA for Aramark Vendors  
Applies if Incorporated Expressly  
Into Contract with Aramark  

Updated 8/20/2020
<table>
<thead>
<tr>
<th>Security Control</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security</td>
<td>Implement firewalls between the organization’s information systems, the Internet (including internal networks connected to the Internet) and other public networks, and internal networks that are not necessary for processing Aramark Information. Firewalls and intrusion detection/prevention systems must be reasonably designed to maintain the security of Aramark Information and relevant information systems. Firewalls and IDS/IPS must be updated regularly and critical vulnerability must be patched within 30 days.</td>
</tr>
<tr>
<td>Information Segregation</td>
<td>Maintain physical or logical segregation of Aramark Information to ensure it is not comingled with another party’s information except as approved by Aramark in writing.</td>
</tr>
</tbody>
</table>
| Malicious Code Detection | - Implement and maintain software that detects, prevents, removes and remedies malicious code designed to perform an unauthorized function on, or permit unauthorized access to, any information system, including without limitation, computer viruses, Trojan horses, worms, and time or logic bombs;  
  - Run malicious code detection software at least daily;  
  - Update malicious code detection software at least daily, including by obtaining and implementing the most current available virus signatures. |
| Vulnerability and Patch Management | Maintain vulnerability management and regular application, operating system and other infrastructure patching procedures and technologies to identify, assess, mitigate and protect against new and existing security vulnerabilities and threats, including viruses, bots, and other malicious code. |
| Application Security | Maintain application security and software development controls designed and tested in accordance with Industry Standards to prevent the introduction of security vulnerabilities in software developed by Provider that Processes Aramark Information. |
| Change Controls | - Prior to implementing changes to the Provider Systems, follow a documented change management process to assess the potential impact of such changes on privacy, confidentiality, security, integrity and availability of Aramark Information, and determine whether such changes are consistent with Provider’s Information Security Program.  
  - No changes should be made to the Provider Systems or Provider’s Information Security Program that increase the risk of an Information Security Incident or fail to comply with the Provider’s contractual or other legal obligations. |
| Off-Premise Information Security | - Maintain policies governing the security of the storage, access, transportation and destruction of records or media containing Aramark Information outside of Provider’s business premises.  
  - Monitor and document movement of records or media containing Aramark Information.  
  - Create copies of Aramark Information before movement of records or media containing the information. |
| Physical Security | - Maintain reasonable restrictions on physical access to Aramark Information and relevant information systems (e.g., clean desk policy).  
  - Maintain physical protection against damage from fire, flood, earthquake, explosion, civil unrest, and other forms of natural or man-made disaster.  
  - Lock workstations with access to Aramark Information when unattended.  
  - Document repairs and modifications to information security-related physical components of the Provider Systems. |
| Contingency Planning | Maintain policies and procedures for responding to an emergency or other occurrence that can compromise the privacy, confidentiality, integrity or availability of Aramark Information or damage the Provider Systems; such policies and procedures should provide for:  
  - Creating and maintaining retrievable copies of Aramark Information;  
  - Restoring any loss of Aramark Information;  
  - Enabling continuation of critical business processes involving Aramark Information in emergency mode;  
  - Assessing relative criticality of specific applications and Aramark Information in support of other contingency plan components;  
  - Periodic testing and updates of contingency and business continuity plans. |
| Point of Contact | Provider will designate an individual who will serve as Aramark’s ongoing point of contact for purposes of addressing issues with respect to the Processing and security of Aramark Information during the term of and following the termination or expiration of the Agreement. Such individual will be accessible to Aramark and will cooperate with Aramark to address such issues. |