This Data Protection Attachment (the "**DPA**") sets out the additional terms, requirements and conditions on which the entity identified as the supplier on the contract document or other order form (“**Supplier**”) will obtain, handle, process, disclose, transfer, or store Personal Information when providing services under the contract document.

**1. Definitions and Interpretation**

**1.1.** “**Data Subject**” means an individual who is the subject of Personal Information.

**1.2.** “**Personal Information**” means any information Supplier Processes for GEA that (a) identifies or relates to an individual who can be identified directly or indirectly from that data alone or in combination with other information in Supplier's possession or control or that Supplier is likely to have access to, or (b) the relevant Privacy Laws otherwise define as protected personal information.

**1.3.** “**Processing, processes, or process**” means any activity that involves the use of Personal Information or that the relevant Privacy Laws may otherwise include in the definition of processing, processes, or process. It includes obtaining, accessing, recording, or storing the data, or carrying out any operation or set of operations on the data including, but not limited to, organizing, amending, retrieving, using, disclosing, erasing, or destroying it. Processing also includes transferring Personal Information to third parties.

**1.4.** “**Privacy Laws**” mean all applicable federal, state, and foreign laws and regulations relating to the Processing, protection, or privacy of the Personal Information, including where applicable, the guidance and codes of practice issued by regulatory bodies in any relevant jurisdiction.

**1.5.** "**Security Breach**” means any act or omission that compromises the security, confidentiality, or integrity of Personal Information or the physical, technical, administrative, or organizational safeguards put in place to protect it. The loss of or unauthorized access, disclosure, or acquisition of Personal Information is a Security Breach whether or not the incident rises to the level of a security breach under the Privacy Laws.

**1.6.** This DPA is subject to the terms of the Master Agreement and is incorporated into the Master Agreement.

**1.7.** Except as otherwise required by law, in the case of conflict or ambiguity between the terms of this DPA and the terms of the Master Agreement, the terms of this DPA will prevail.

**2. Personal Information Types and Processing Purposes**

**2.1.** GEA retains control of the Personal Information and remains responsible for its compliance obligations under the applicable Privacy Laws, including providing any required notices and obtaining any required consents, and for the Processing instructions it gives to Supplier.

**2.2.** Appendix A describes the general Personal Information categories and Data Subject types Supplier may Process to fulfill the business purposes of the Master Agreement (as described in Appendix A).

**2.3.** To the extent that Supplier processes or otherwise has access to Personal Information of a California resident, Supplier acknowledges and agrees to comply with the obligations listed in Appendix B.

**3. Supplier's Obligations**

**3.1.** Supplier will only process, retain, use, or disclose the Personal Information to the extent, and in such a manner, as is necessary for the business purposes in accordance with GEA's written instructions. Supplier will not Process, retain, use, or disclose the Personal Information for any other purpose or in a way that does not comply with this DPA or the applicable Privacy Laws. Supplier must promptly notify GEA if, in its opinion, GEA's instruction would not comply with applicable Privacy Laws.

**3.2.** Supplier must promptly comply with any GEA request or instruction requiring Supplier to amend, transfer, or delete the Personal Information, or to stop, mitigate, or remedy any unauthorized Processing.

**3.3.** Supplier will maintain the confidentiality of all Personal Information, will not sell it to anyone, and will not disclose it to third parties unless GEA or this DPA specifically authorizes the disclosure, or as required by law. If Supplier is required by law to Process or disclose Personal Information, Supplier must first inform GEA of the legal requirement and give GEA an opportunity to object or challenge the requirement, unless the law prohibits such notice.

**3.4.** Supplier will reasonably assist GEA with meeting GEA's compliance obligations under the Privacy Laws, taking into account the nature of Supplier's Processing and the information available to Supplier.

**3.5.** Supplier will only collect Personal Information for GEA using a notice or method that GEA specifically pre-approves in writing, which contains an approved data privacy notice informing the Data Subject of GEA's identity, the purpose or purposes for which their Personal Information will be Processed, and any other information that is required by applicable law or regulation. Supplier will not modify or alter the notice without GEA's prior written consent.

**4. Supplier's Employees**

**4.1.** Supplier will limit Personal Information access to those employees on a need-to-know basis and only to the extent who require Personal Information access to meet Supplier's obligations and the part or parts of the Personal Information that those employees strictly require for the performance of their duties.

**4.2.** Supplier will ensure that all employees:

 (a) are informed of the Personal Information's confidential nature and use restrictions;

 (b) have undertaken training on the Privacy Laws relating to handling Personal Information and how it applies to their particular duties; and

 (c) are aware both of Supplier's duties and their personal duties and obligations under the Privacy Laws and this DPA.

**4.3.** Supplier will take reasonable steps to ensure the reliability, integrity, and trustworthiness of all of Supplier's employees with access to the Personal Information.

**5. Security**

**5.1.** Supplier must at all times implement appropriate technical and organizational measures designed to safeguard Personal Information against unauthorized or unlawful Processing, access, copying, modification, storage, reproduction, display, or distribution, and against accidental loss, destruction, or damage, including, but not limited to, those listed in Appendix C. Supplier must document those measures in writing and periodically review them, at least annually, to ensure they remain current and complete.

**5.2.** Supplier will immediately notify GEA if it becomes aware of any advance in technology and methods of working, which indicate that the parties should adjust their security measures.

**5.3.** Supplier must take reasonable precautions to preserve the integrity of any Personal Information it Processes and to prevent any corruption or loss of the Personal Information, including but not limited to establishing effective back-up and data restoration procedures.

**6. Security Breaches and Personal Information Loss**

**6.1.** Supplier will promptly notify GEA if any Personal Information is lost or destroyed or becomes damaged, corrupted or unusable. Supplier will restore such Personal Information at its own expense.

**6.2.** Supplier will immediately notify GEA if it becomes aware of any Security Breach or any other unauthorized or unlawful Processing of the Personal Information:

**6.3.** Immediately following any unauthorized or unlawful Personal Information Processing or Security Breach, the parties will coordinate with each other to investigate the matter. Supplier will reasonably cooperate with GEA in GEA's handling of the matter, including:

 (a) assisting with any investigation;

 (b) providing GEA with physical access to any facilities and operations affected;

 (c) facilitating interviews with Supplier's employees, former employees and others involved in the matter; and

 (d) making available all relevant records, logs, files, data reporting, and other materials required to comply with all Privacy Laws or as otherwise reasonably required by GEA.

**6.4.** Supplier will not inform any third party of any Security Breach without first obtaining GEA's prior written consent, except when law or regulation requires it.

**6.5.** Except to the extent Supplier has a legal obligation to disclose information regarding a Security Breach, GEA has the sole right to determine:

 (a) whether to provide notice of the Security Breach to any Data Subjects, regulators, law enforcement agencies, or others, as required by law or regulation or in GEA's discretion, including the contents and delivery method of the notice; and

 (b) whether to offer any type of remedy to affected Data Subjects, including the nature and extent of such remedy.

**6.6.** Supplier will cover all reasonable expenses associated with the performance of the obligations under Section 6.2 and Section 6.3, unless the matter arose from GEA's specific instructions, negligence, willful default, or breach of this DPA.

**6.7.** Supplier will also reimburse GEA for actual reasonable expenses GEA incurs when responding to and mitigating damages, to the extent that Supplier caused a Security Breach, including all costs of notice and any remedy as set out in Section 6.5. The obligations of Supplier in Sections 6.6 and 6.7 of this DPA shall not be limited by any limitation or exclusion of liability in the Master Agreement.

**7. Cross-Border Transfers of Personal Information**

**7.1.** If applicable law or requirements restrict cross-border Personal Information transfers, GEA will only transfer that Personal Information to Supplier under the following conditions:

 (a) Supplier, either through its location or participation in a valid cross-border transfer mechanism under applicable law or regulation, as identified in Appendix A, may legally receive that Personal Information; however, Supplier must immediately inform GEA of any change to that status;

 (b) GEA obtained valid Data Subject consent to the transfer under applicable law or regulation; or

 (c) the transfer otherwise complies with applicable law or regulation for the reasons set forth in Appendix A.

**7.2.** If any Personal Information transfer between Supplier and GEA so requires, the parties will complete all relevant details in, and execute, the Standard Contractual Clauses, which can be located at <https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en>, and take all other actions required to legitimize the transfer.

**7.3.** Supplier will not transfer any Personal Information to another country unless the transfer complies with applicable law or regulation. In Appendix A, Supplier must identify the legal basis supporting any transfers it makes and must immediately inform GEA of any change to that status.

**8. Subcontractors**

**8.1.** Supplier may only authorize a third party to Process the Personal Information if:

 (a) GEA provides prior written consent after Supplier supplies GEA with full details regarding such third party;

 (b) Supplier enters into a written contract with the third party that contains terms substantially the same as those set out in this DPA and, upon GEA's written request, provides GEA with copies of such contracts;

 (c) Supplier maintains control over all Personal Information it entrusts to the third party; and

 (d) the third party’s contract terminates automatically on termination of this DPA.

**8.2.** Supplier must list all approved subcontractors in Appendix A and include any subcontractor's name and location and contact information for the person responsible for privacy and data protection compliance.

**8.3.** If the subcontractor fails to fulfill its obligations under such written agreement, Supplier remains fully liable to GEA for the subcontractor's performance of its agreement obligations.

**8.4.** The Parties consider Supplier to control any Personal Information controlled by or in the possession of its subcontractors.

**8.5.** Upon GEA's reasonable request, Supplier will audit a subcontractor's compliance with its obligations regarding GEA's Personal Information and provide GEA with the audit results.

**9. Complaints, Data Subject Requests and Third Party Rights**

**9.1.** Supplier must notify GEA immediately if it receives any communication that directly or indirectly relates to the Personal Information Processing or to either Party's compliance with Privacy Laws.

**9.2.** Supplier must notify GEA within five (5) business days if it receives a request from a Data Subject for access to or deletion of their Personal Information.

**9.3.** Supplier will assist GEA in responding to any communication or Data Subject request.

**9.4.** Supplier must not disclose the Personal Information to any Data Subject or to a third party unless the disclosure is either at GEA's request or instruction, permitted by this DPA or otherwise is required by law.

**10. Term and Termination**

**10.1.** This DPA will remain in effect as long as the Master Agreement is in effect or Supplier possesses or controls Personal Information related to the Master Agreement.

**10.2.** Any provision of this DPA that is necessary to protect Personal Information, expressly or implicitly, will continue to apply after termination or expiration of the Master Agreement.

**10.3.** Supplier's failure to comply with this DPA is a material breach of the Master Agreement. In such event, GEA may immediately terminate the Master Agreement upon written notice to Supplier, with no further liability or obligation to Supplier.

**10.4.** If a change in any Privacy Laws renders a Party’s Processing of Personal Information non-compliant, the affected Party will suspend such Processing until the Processing complies with the new requirements. If a Party is unable to comply within ten (10) days, GEA may terminate the Master Agreement upon written notice to Supplier.

**11. Data Return and Destruction**

**11.1.** At GEA's request, Supplier will give, within a reasonable time, GEA a copy of or access to all or part of GEA's Personal Information in its possession or control in the format and on the media reasonably specified by GEA.

**11.2.** On termination or expiration of the Master Agreement, Supplier will securely destroy (and certify in writing such destruction within fourteen (14) days) or, if directed in writing by GEA, return any Personal Information in its possession or control. Unless otherwise provided herein, Supplier will not retain any Personal Information after termination or expiration.

**11.3.** If Supplier is required by law to retain any documents or materials that Supplier would otherwise be required to return or destroy, it will notify GEA in writing of that retention requirement, giving details of the documents or materials that it must retain, the legal basis for retention and establishing a specific timeline for destruction once the retention requirement ends. Supplier may only use this retained Personal Information for the required retention reason.

**12. Records**

**12.1.** Supplier will maintain records regarding any Processing of Personal Information it carries out for GEA, including but not limited to, the access, control and security of the Personal Information, approved subcontractors and affiliates, the Processing purposes and any other records required by applicable law or regulation. Such records shall be sufficient to enable GEA to verify Supplier's compliance with its obligations under this DPA.

**12.2.** Supplier must review the information listed in the Appendices once a year to confirm its current accuracy and update it if necessary.

**13. Audit**

**13.1.** At least once per year, Supplier will conduct site audits of its Personal Information Processing practices and the information technology and information security controls for all facilities and systems used in complying with its obligations under this DPA, including, but not limited to, obtaining a network-level vulnerability assessment performed by a recognized third-party audit firm based on recognized industry best practices.

**13.2.** Upon GEA's written request, Supplier will make all of the relevant audit reports available to GEA for review.

**13.3.** Supplier will promptly address any issues, concerns, or exceptions noted in the audit reports with the development and implementation of a corrective action plan by Supplier's management.

**13.4.** Upon request, with reasonable advance notice and conducted in such a manner not to unduly interfere with Supplier’s operations, GEA reserves the right to conduct an audit of Supplier’s compliance with the requirements in this DPA relating to GEA data including but not limited to: (a) a review of Supplier’s applicable policies, processes, and procedures; (b) a review of the results of Supplier’s most recent vulnerability assessment (e.g., application vulnerability scanning, penetration testing, and similar testing results) and accompanying remediation plans; and (c) on-site assessments of Supplier’s physical security controls and Supplier Information Systems during Supplier’s regular working hours that will not interfere with Supplier’s operations, pursuant to a mutually agreeable audit plan.

**13.5.** GEA acknowledges and agrees that nothing in Section 13 above shall oblige Supplier to divulge any information relating to its other customers in such a manner that may put Supplier in breach of its confidentiality obligations to such customers or any other legal requirements.

**14. Warranties**

**14.1.** Supplier warrants and represents that:

 (a) it has no reason to believe that any Privacy Laws prevent it from providing any of the Services; and

 (b) considering the current technology environment and implementation costs, it will take appropriate technical and organizational measures to prevent the unauthorized or unlawful Processing of Personal Information and the accidental loss or destruction of, or damage to, Personal Information, and ensure a level of security appropriate to:

 (i) the harm that might result from such unauthorized or unlawful Processing or accidental loss, destruction, or damage; and

 (ii) the nature of the Personal Information protected; and

 (iii) comply with all applicable Privacy Laws and its information and security policies, including the security measures required in Section 5.

Appendix a – PERSONAL INFORMATION PROCESSING DETAILS

1. Personal Information Processing Purposes and Details

Business Purposes:

Personal Information Categories:

Data Subject Types:

Approved Subcontractors:

[Authorized Persons:]

[Countries where Supplier may receive, access, transfer or store Personal Information:

2. Supplier’s legal basis for receiving personal information with cross-border restrictions (if applicable)

 Located in an EEA Member State or in a country with a current determination of adequacy (list country): \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

 Binding Corporate Rules

 Standard Contractual Clauses

 EU-US Privacy Shield Certified

 Other (describe in detail):\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Appendix B - CCPA Service Provider Terms

Supplier acknowledges and understands that GEA and/or its Affiliates may be obligated impose on Supplier certain responsibilities regarding the processing of personal information, in accordance with the California Consumer Privacy Act of 2018 (“**CCPA**”). This Appendix B is designed and intended to satisfy any such obligations. Any terms used herein shall have the meaning ascribed to them in the CCPA, notwithstanding any other definition used in the Contract.

To the extent GEA discloses to Supplier any “personal information” to use in providing GEA any services or goods (Services), Supplier agrees to protect the personal information as detailed herein, except as applicable law may otherwise require.

1. Supplier is prohibited from retaining, using, collecting, or disclosing the personal information:

 a. for any purpose except performing the Services

 b. for any “commercial purpose” other than performing the Services

 c. outside the direct business relationship between you and GEA

2. Supplier is prohibited from “selling” any personal information.

3. Except to the extent necessary to perform the services, Supplier is prohibited from reconfiguring, de-identifying, re-identifying, or aggregating the personal information or any data derived from the personal data.

4. Supplier shall promptly (and in any case within five days) notify GEA of requests from individuals whose data is included in the personal information and shall assist GEA in responding to such requests.

5. These terms supplement and do not replace any existing Supplier obligations related to the privacy and security of personal information. The obligations herein shall survive for as long as Supplier holds or processes personal information.

Appendix C – IT SECURITY CONTROLS

**Organizational security controls shall include the following at a minimum:**

1. Supplier must have an IT security organization with clearly defined information security roles, responsibilities and accountability.

2. Supplier and Supplier personnel shall Process GEA data, and access and use GEA networks, only on a need-to-know basis and only to the extent necessary to perform services under the contract document or as otherwise instructed by GEA or the applicable GEA Affiliate in writing.

3. Supplier personnel accessing GEA data shall be limited to those obligated to comply with the level of security required in the contract document and this DPA. Supplier shall take reasonable steps to ensure continuing compliance by such Supplier personnel with this DPA and shall remain responsible for their compliance including, but not limited to, appropriate information security awareness training prior to obtaining access to GEA data and thereafter on at least an annual basis while such personnel have access to GEA data.

4. Unless otherwise agreed upon in the contract document, Supplier shall obtain GEA’s prior written approval to provide access to GEA data to Suppliers, subcontractors or agents that were not pre-qualified by or otherwise disclosed to GEA in writing prior to Supplier’s performance of services under the contract document.

5. Supplier must maintain formal written policies and procedures for the administration of information security throughout its organization consistent with the requirements of this DPA and maintain a current inventory of Supplier systems or computers that will process or store GEA data.

6. Supplier shall terminate Supplier personnel access to GEA data, whether physical or logical, no later than the date of personnel separation or termination from supplier organization via an automated process. In the event of a role change or internal transfer, supplier should have a periodic process to review access controls to ensure access to GEA data is removed.

7. GEA data shall not be Processed on personal accounts (e.g., individual email or cloud services accounts (e.g., Gmail, Yahoo, Dropbox, Google Drive)) or on personally-owned computers, devices or media.

8. Unless prohibited by applicable law or regulation, Supplier shall notify GEA promptly and act only upon GEA’s instruction concerning any request by a third party for disclosure of GEA data or for information concerning the Processing of GEA data in connection with the contract document or this DPA, as well as any request received from an individual concerning his/her Personal data.

**Technical security controls on Supplier Information Systems shall include the following at a minimum:**

9. Supplier must use strong password controls utilizing industry standards which include; password complexity, account lockout for failed attempts, expiration period, encryption, changing of default passwords, and usage of temporary passwords. User account credentials (e.g., login ID, password) must not be shared.

10. Supplier must implement and maintain controls to detect and prevent unauthorized access, intrusions and computer viruses and other malware. At a minimum such controls must include network layer security devices (e.g. firewalls and intrusion detection/prevention systems), client and server-side antivirus programs that include up-to-date antivirus definitions. In addition, Supplier must install all critical patches or security updates within thirty (30) days of release or provide a detailed remediation plan not exceeding ninety (90) days.

11. Supplier must maintain a vulnerability management program in place that outlines the process to apply critical security patches in line with industry best practices, that is risk-based and has mitigating controls when needed.

12. Supplier must maintain documented change management procedures that provide a consistent approach for controlling, implementing and documenting changes (including emergency changes) for Supplier Information Systems that includes appropriate segregation of duties.

13. Unless otherwise expressly agreed in the contract document, development and testing environments must be physically and/or logically separated from production environments and must not contain GEA data unless specified in the contract document. Production changes must be approved by the Supplier’s appropriate system owner, as such person is designated in the contract document, and such changes must not be made by any Supplier developers.

14. Change Management: Requires segregation of duties, so all production changes are approved by the designated system owner, and not development resources.

15. Any back-up media containing GEA data stored at Supplier’s site must be kept in a secure location (e.g., locked office or locked file cabinet) and be encrypted to a standard consistent with industry practice. If off-site media storage is used, Supplier must have a media check-in/check-out process with locked storage for transportation. Back-up information must be given the same level of physical and environmental protection as the level of control applied at the main site.

16. Workstations must not be left authenticated when unattended and must be password protected when not in use. An inactivity lockout must be implemented on workstations.

17. Network layer security devices must allow only authorized connections and rule sets must be reviewed at minimum semi-annually.

18. Mobile devices used to Process GEA data (including emails) must have strong mobile device security controls which include required passcode or PIN, inactivity lock, encryption, jail break detection, and remote wipe.

**Physical security controls shall include the following at a minimum on all Supplier facilities where GEA data may be Processed:**

19. Physically secure perimeters and external entry points must be suitably protected against unauthorized access (e.g. barriers such as walls, card controlled entry gates). Access to all locations must be limited to Supplier personnel and authorized visitors only. Reception areas must be manned or have other means to control physical access.

20. Visitors must be required to sign a visitor’s register (maintained for at least one year) and be escorted or observed at all times, upon each entry to and exit from the premises.

21. A clear desk policy must be enforced throughout the Supplier facilities. Documents that contain GEA data must be kept secured (e.g. locked office or file cabinet) when not in use.