Data Processing Agreement

This Data Processing Agreement ("DPA") is by and between (i) the GPTW entity, as the Processor of Customer Personal Data, set forth in the Order or Statement of Work that references the GPTW Master Services Agreement, or any other currently effective agreement, (the "Agreement"), ("GPTW"), and (ii) the person or entity who is named on such Order or Statement of Work on behalf of itself and Customer Affiliates, as the Controller of Customer Personal Data, ("Customer") and sets forth the terms and conditions applicable to GPTW's processing activities under the Agreement. Customer and GPTW are referred to individually as a "Party" and collectively as the "Parties".

WHEREAS, in the course of providing the Services to Customer pursuant to the Agreement, GPTW may Process Customer Personal Data on behalf of Customer, and the Parties agree to comply with the following provisions with respect to the Processing of Customer Personal Data.

NOW THEREFORE, in consideration of the mutual covenants contained herein and for other good and valuable consideration, the respective receipt and sufficiency of which are hereby acknowledged, the Parties agree as follows:

1. General

1.1 The above and foregoing recitals are true and correct and incorporated herein by reference.

1.2 This DPA consists of the terms and conditions set forth in this DPA and the following Schedules, which are attached hereto and incorporated herein by reference:

1.2.1 Schedule 1: Details of the Processing

1.2.2 Schedule 2: Technical and Organizational Security Measures

1.2.3 Schedule 3: Additional Applicable Privacy Provisions

2. Definitions

2.1 In this DPA, capitalized terms will have the meanings set out below. Capitalized terms not otherwise defined below will have the meaning given to them in the Agreement.

"**Affiliates**" means, as to GPTW, those entities that are directly or indirectly controlled by , control, or are under common control with Great Place to Work Institute, Inc., including, but not limited to, those entities who have entered into license agreements with GPTW to be able to sell and provide the Subscription Services; and as to Customer, those Customer entities that directly or indirectly control, are controlled by, or are under common control with Customer. "Control" (in this context) means the possession, directly or indirectly, of the power to direct or cause the direction of the management and operating policies of the entity in respect of which the determination is being made through the ownership of the majority of its voting or equity securities, contract, or otherwise.

"**Applicable Law(s)**" means any applicable provisions of all laws, codes, legislative acts, regulations, ordinances, rules of court, and court orders which govern the Party's respective business operations. GPTW shall comply with all Applicable Laws applicable to GPTW in its role as a Data Processor Processing Personal Data. For the avoidance of doubt, GPTW is not responsible for complying with Applicable Laws applicable to Customer or Customer's industry. Customer shall comply with all Applicable Laws to Customer as a Data Controller.

"Cross-Border Transfer Mechanism" means applicable legally valid mechanisms required for the transfer of Customer Personal Data from a Controller or a Processor in a given jurisdiction to another Processor or Subprocessor operating in a separate jurisdiction where Applicable Laws require a legal mechanism for cross-border transfer. Such mechanisms include, by way of example and without limitation, the Standard Contractual Clauses.

"Core Subscription Services" means Assess, Analyze, and Accelerate offerings identified in the Order.

"**Countries with Adequate Protection**" means the following applicable third countries, territories, or specified sectors within a third country: (1) for data processed subject to the EU GDPR: the EEA, or a country or territory that is the subject of an adequacy decision by the Commission under Article 45(1) of the EU GDPR;
(2) for data processed subject to the UK GDPR: the UK or a country or territory that is the subject of the adequacy regulations under Article 45(1) of the UK GDPR and Section 17A of the Data Protection Act 2018; and/or
(3) for data processed subject to the Swiss FDPA: Switzerland, or a country or territory that (i) is included in the list of the states whose legislation ensures an adequate level of protection as published by the Swiss Federal Data Protection and Information Commissioner, or (ii) is the subject of an adequacy decision by the Swiss Federal Council under the Swiss FDPA.

"Customer Personal Data" means any Personal Data Processed by GPTW on behalf of Customer pursuant to or in connection with the Agreement.

"GDPR" means EU General Data Protection Regulation 2016/679.

"**Pseudonymized Data**" means Data that has gone through Pseudonymization.

"Restricted Transfer" means a transfer of Customer Personal Data from Customer to a GPTW Processor, or a transfer of such data between GPTW Processors, where such transfer would be prohibited by Applicable Laws (or by the terms of data transfer agreements put in place to address the data transfer restrictions of Applicable Laws) in the absence of a Cross-Border Transfer Mechanism.

"Services" means Core Subscription Services and any other GPTW Products and Services.

"Standard Contractual Clauses" or **"SCCs"** means any type or module of standard contractual clauses approved by any relevant authority such as the European Commission in Decision (EU) 2021/914 on standard contractual clauses for the transfer of personal data to third countries, the British Data Protection Authority, the Swiss Data Protection Authority or the Singapore Data Protection Authority, including those executed between GPTW Affiliates as GPTW Processors. The completed EU SCCs (Processor-to-Processor) and (Controller-to-Processor) are available on https://www.greatplacetowork.com/cross-border-transfer-mechanisms, and are deemed incorporated in this DPA, in accordance with Section 11 below.

"Subprocessor" means any person (including any third party and any GPTW Affiliate) appointed by or on behalf of GPTW to Process Customer Personal Data on behalf of Customer in connection with the Agreement, a list of which is available on https://www.greatplacetowork.com/list-of-sub-processors, and which is incorporated herein by reference.

"GPTW Processor" means GPTW or a GPTW Subprocessor.

"**GPTW Other Products & Services**" means Professional Services and GPTW products and services other than Core Subscription Services, which are subject to the specific Supplement for GPTW Other Products and Services made available to Customer.

The terms, **"Commission", "Controller", "Data Subject", "Member State", "Personal Data", "Personal Data Breach", "Personal Information", "Processing", "Processor", "Pseudonymization"** and **"Supervisory Authority"**, will have the same meaning as in the GDPR, or the equivalent meaning as set forth in Applicable Laws, and **"Processing"** shall be interpreted to include the following as applicable **"Process"**, **"Processes"** and **"Processed"**.

Where applicable, the terms, **"Service Provider" "Share"** and **"Sell"** will have the same meaning as in the California Consumer Privacy Act (**"CCPA"**).

3. Processing of Customer Personal Data

3.1 GPTW will:

3.1.1 comply with all Applicable Laws in the Processing of Customer Personal Data; and

3.1.2 not Process Customer Personal Data other than for the purpose, and in accordance with, the relevant Customer's instructions as documented in the Agreement and this DPA, unless Processing is required by the Applicable Laws to which the relevant GPTW Processor is subject, in which case GPTW to the extent permitted by the Applicable Laws, will inform Customer of that legal requirement before the Processing of that Customer Personal Data.

3.2 Customer hereby:

3.2.1 instructs GPTW (and authorizes GPTW to instruct each Subprocessor) to: (a) Process Customer Personal Data; and (b) in particular, transfer Customer Personal Data to any country or territory subject to the provisions of this DPA, in each case as reasonably necessary for the execution of the Agreement.

3.2.2 warrants and represents that it is and will at all relevant times remain duly and effectively authorized to give the instructions set out in Section 3.2.1 on behalf of each relevant Customer Affiliate; and

3.2.3 warrants and represents that it has all necessary rights in relation to the Customer Personal Data and/or has collected all necessary consents from Data Subjects to Process Customer Personal Data to the extent required by Applicable Law.

3.3 Schedule 1 to this DPA sets out certain information regarding GPTW's Processing of Customer Personal Data as required by Article 28(3) of the GDPR (and equivalent requirements of other Applicable Laws).

4. GPTW Personnel

GPTW will take steps to ensure that access to Customer Personal Data is limited to those individuals who: (a) need to know or access the relevant Customer Personal Data as necessary for the purposes of providing the Services under the Agreement or to comply with Applicable Laws in the context of that individual's duties to GPTW; and (b) are subject to

written confidentiality undertakings or professional or statutory obligations of confidentiality.

5. Security

5.1 Taking into account the state of the art, the costs of implementation and the nature, scope, context, and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, GPTW will in relation to the Customer Personal Data implement appropriate technical and organizational measures to ensure a level of security appropriate to that risk as set forth in Schedule 2 to this DPA.

5.2 In assessing the appropriate level of security, GPTW will take into account the risks that are presented by Processing, in particular from a Personal Data Breach.

6. Subprocessing

6.1 Customer generally authorizes GPTW to appoint Subprocessors in accordance with this Section 6, including without limitation those Subprocessors provided herein and any new Subprocessors. Subprocessors used for GPTW Other Products and Services may be listed under each applicable Statement of Work or Order Form or in an addendum to this DPA or other form of communication.

6.2 GPTW will provide Customer with a mechanism to obtain notification of the appointment of any new Subprocessor, including material details of the Processing to be undertaken by the Subprocessor at least thirty (30) days before said Subprocessor carries out Processing activities on Customer Personal Data on behalf of Customer. Customer may object, on reasonable data protection grounds, to any new Subprocessor by providing notice of an objection by email to GPTW at privacy@greatplacetowork.com within ten (10) days of Customer's receipt of notification of the addition of the new Subprocessor by GPTW. In the event GPTW, in its sole discretion, is unable to forego the utilization of a new Subprocessor that has been objected to for the Processing of Customer Personal Data or is otherwise unable to reasonably address the Customer's objection within thirty (30) days of GPTW's receipt of such objection from Customer, the Customer may terminate the impacted services upon written notice to GPTW. This termination right is Customer's sole and exclusive remedy if Customer objects to any new Subprocessor, and is not a termination for cause. GPTW will cease providing the impacted services thirty (30) days following the notice of termination.

6.3 With respect to each Subprocessor, GPTW will:

6.3.1 verify that the arrangement between GPTW and the Subprocessor is governed by a written contract including terms which offer at least equivalent level of protection for Customer Personal Data as those set out in this DPA and meet the requirements of article 28(3) of the GDPR; and

6.3.2 if that arrangement involves a Restricted Transfer, confirm that the Standard Contractual Clauses, or other legally valid Cross-Border Transfer Mechanism, are at all relevant times incorporated into the relevant agreement(s) between GPTW and the Subprocessor.

7. Data Subject Rights

7.1 Taking into account the nature of the Processing, GPTW will assist Customer by implementing commercially reasonable technical and organizational measures for the fulfilment of the Customer's' obligations, as reasonably understood by Customer, to respond to requests to exercise Data Subject rights under the Applicable Laws.

7.2 If GPTW receives a request from a Data Subject under any Applicable Law(s) in respect of Customer Personal Data ("Data Subject Request"), GPTW will:

7.2.1 promptly redirect the Data Subject to its Controller; and

7.2.2 ensure that GPTW does not respond to that Data Subject Request except on the documented instructions of Customer or as required by Applicable Laws to which GPTW is subject, in which case GPTW, to the extent permitted by Applicable Laws, shall inform Customer of that legal requirement before GPTW responds to the Data Subject request.

8. Personal Data Breach

8.1 GPTW will notify Customer without undue delay and in accordance with Applicable Laws upon GPTW or any Subprocessor becoming aware of a Personal Data Breach affecting Customer Personal Data, providing Customer with sufficient information to allow Customer to meet its obligations to report or inform Data Subjects of the Personal Data Breach under the Applicable Laws.

8.2 In the event of a Personal Data Breach, the Parties will reasonably cooperate with each other, and GPTW shall take commercially reasonable steps to keep Customer informed as to the investigation, mitigation, and remediation of any such Personal Data Breach.

8.3 Except as may be required by Applicable Laws, GPTW will not notify Customer's affected Data Subjects about a Personal Data Breach without Customer's prior written consent.

9. Deletion or return of Customer Personal Data

9.1 Subject to Sections 9.2 and 9.3, following the latter of either (i) termination or expiration of the Agreement or (ii) cessation of the Processing of Customer Personal Data, (the "Cessation Date"), GPTW will, in accordance with the terms of the Agreement, promptly return or delete Customer Personal Data that can be reasonably identified and extracted in accordance with the requirements of the relevant Applicable Laws.

9.2 Notwithstanding Section 9.1 above, each GPTW Processor may retain Customer Personal Data to the extent and for such period as required by Applicable Laws, provided that GPTW will ensure the confidentiality of all such Customer Personal Data and will ensure that such Customer Personal Data is only Processed as necessary for the purpose(s) specified in the Applicable Laws requiring its storage.

9.3 Upon receipt of written request from Customer, GPTW will provide written certification to Customer that it has complied with this Section 9.

10. Audit rights

GPTW shall demonstrate appropriate technical and organizational measures to Customer throughout the term. Customer may exercise such audit right either personally or by appointing a third party, so long as said third party is acceptable to GPTW and bound to confidentiality and non-disclosure obligations at least as stringent as Customer's obligations with respect to GPTW Confidential Information as set forth in the Agreement. Customer is responsible and liable for any and all acts or omissions of any such third party. Customer may exercise such audit right on an annual basis with reasonable notice. Any such audits shall be limited to a robust customer due diligence package consisting of details on GPTW's information security/risk practices, examination of the results of the annual AICPA SSAE 18 SOC 1 and if available, SOC 2 Type I and Type II audits conducted by an independent third party, executive summaries of the annual penetration test results or verification of such testing through the SOC 2 report for Core Subscription Services, and reasonable access to knowledgeable personnel to discuss the controls in place, including a meeting at GPTW corporate headquarters. In the event Customer requests support or information beyond the content described above, then, upon Customer's audit request, the Parties will mutually agree on the terms of the audit plan, which shall include details regarding the scope, duration, fees, and scheduling of the audit. In no event shall Customer or its designees be permitted to access GPTW systems, network servers, scan summaries or activities logs.

11. Restricted Transfers and Cross-Border Transfer

11.1 Customer is fully aware and acknowledges that GPTW operates as a global company with locations across the world. In order for GPTW to provide customers with service level continuity and to optimize both organization and management of the quality of its products and services, GPTW reserves the right to have Customer Personal Data processed by other GPTW Affiliates or by Subprocessors and that may be located in a different region than where the original Processing took place, which Customer accepts.

11.2 In connection with Restricted Transfers, GPTW will only operate cross-border transfer of Customer Personal Data either to Countries with Adequate Protection or based on a Cross-Border Transfer Mechanism.

11.3 In connection with Customers operating in countries where no Restricted Transfers are occurring, no transfer mechanism shall be applicable.

12. Additional Assurances

12.1 GPTW shall maintain the following additional safeguards with respect to Customer Personal Data that is transferred pursuant to the Standard Contractual Clauses:

12.1.1 GPTW agrees to notify Customer of any request from law enforcement authority or other governmental authority with competent authority and jurisdiction over GPTW for disclosure of Customer Personal Data processed under this DPA ("Disclosure Request") to the extent permitted by applicable law. GPTW shall not respond to Disclosure Requests without notifying Customer and receiving written authorization from Customer to respond to such Disclosure Request, except as required under Applicable Laws or order of court or governmental authority with competent authority and jurisdiction over same;

12.1.2 In the event GPTW receives a Disclosure Request for disclosure of Customer Personal Data processed under this DPA and Data Processor is not legally permitted to notify Customer of the Disclosure Request, GPTW agrees to take reasonable legal actions against the disclosure of the Customer Personal Data and to refrain from disclosure of the Customer Personal Data to the respective authorities until a court of competent jurisdiction orders GPTW to disclose such Customer Personal Data. In such event, GPTW agrees to provide the minimum amount of information required when responding to the Disclosure Request, based on GPTW's reasonable interpretation of the Disclosure Request; and

12.1.3 GPTW can make available to Customer a Transfer Risk and Impact Statement to assist Customer in carrying out its own transfer impact assessment related to Customer's use of the Services.

13. General Terms

13.1 Governing Law. Without prejudice to clauses 17 (Governing Law) and 18 (Choice of Forum and Jurisdiction) of the Standard Contractual Clauses:

13.1.1 the Parties to this DPA hereby submit to the choice of jurisdiction stipulated in the Agreement with respect to any disputes or claims howsoever arising under this DPA, including disputes regarding its existence, validity or termination or the consequences of its nullity; and

13.1.2 this DPA and all non-contractual or other obligations arising out of or in connection with it are governed by the laws of the country or territory stipulated for this purpose in the Agreement.

13.2 DPA Priority. Nothing in this DPA reduces GPTW's obligations under the Agreement in relation to the protection of Customer Personal Data or permits GPTW to Process (or permit the Processing of) Customer Personal Data in a manner which is prohibited by the Agreement. With regard to the subject matter of this DPA, in the event of inconsistencies between the provisions of this DPA and the Agreement, the provisions of this DPA will prevail.

13.3 Claims. Any claims brought under this DPA shall be subject to the terms and conditions of the Agreement, including but not limited to, the exclusions and limitations set forth in the Agreement.

13.4 Severability. Should any provision of this DPA be invalid or unenforceable, then the remainder of this DPA will remain valid and in force. The invalid or unenforceable provision will be either (i) amended as necessary to ensure its validity and enforceability, while preserving the Parties' intentions as closely as possible or, if this is not possible, (ii) construed in a manner as if the invalid or unenforceable part had never been contained there.

13.5 This DPA supersedes all prior and contemporaneous representations, negotiations, and communications between the Parties relating to processing Customer Personal Data, including without limitation, any terms that may be imposed upon GPTW by means of any "click-through", forms, applications, or any other terms and conditions which are presented to GPTW in the course of GPTW's engagement with Customer.

Schedule 1: Details of Processing of Customer Personal Data

This Schedule 1 includes certain details of the Processing of Customer Personal Data as required by Article 28(3) GDPR.

Subject matter and duration of the Processing of Customer Personal Data

The subject matter and duration of the Processing of the Customer Personal Data are set out in the Agreement and this DPA.

The nature and purpose of the Processing of Customer Personal Data

Provision of the Services are set out in the Agreement and this DPA, where GPTW acts as a data processor, and for business operations, as an independent controller.

GPTW will use and otherwise process Customer Data only as described and subject to the limitations provided below (a) to provide Customer the Services in accordance with Customer's documented instructions and (b) for business operations incident to providing the Services to Customer.

Processing to Provide Customer the Services

For purposes of this DPA, "to provide" a Service consists of:

- Delivering functional capabilities as licensed, configured, and used by Customer and its users;
- Troubleshooting (preventing, detecting, and repairing problems); and
- Keeping Services up to date and operational, and enhancing user productivity, reliability, efficacy, quality, and security.

When providing Services, GPTW will not use or otherwise process Customer Data or Personal Data for: (a) user profiling, (b) advertising or similar business purposes, or (c) sell or share Personal Data.

Processing for Business Operations Incident to Providing the Services to Customer

For purposes of this DPA, "business operations" means the processing operations authorized by Customer in this section.

Customer authorizes GPTW:

- to create aggregated statistical, non-personal data from data containing Pseudonymized identifiers (such as usage logs containing unique, Pseudonymized identifiers);
- to calculate statistics related to Customer Data; and
- to de-identify Customer Data to enhance and create new functionalities.

in each case limited to providing the Services, such as billing and account management; internal reporting and business modeling, and product strategy; and enhancing Customer's experience.

When processing for these incident business operations, GPTW will apply principles of data minimization, confidentiality and will not use or otherwise process Customer Data or Personal Data for: (a) user profiling, (b) advertising or similar commercial purposes, (c) any other purpose, other than for the purposes set out in this section or (d) Sell or Share Personal Data.

The types of Customer Personal Data to be Processed

All Customer Personal Data required by GPTW to correctly provide the Services to Customer pursuant to the Agreement which may include, without limitation: employee first and last name, race, ethnicity, email, employee ID number, department code, badge number, job title, identification and contact information of Customer data subjects, employment and education details of Customer data subjects.

The categories of Data Subject to whom the Customer Personal Data relates

Customer's employees, contractors, or other individuals authorized or invited by Controller to take GPTW's survey.

Special categories of Customer Personal Data to be Processed

None unless provided by Customer to GPTW .

The obligations and rights of Customer

The obligations and rights of Customer are set out in the Agreement and this DPA.

Privacy related contact:

GPTW: privacy@greatplacetowork.com

Customer: As specified in this DPA, in the Order Form or in the Statement of Work.

Schedule 2: Technical and Organizational Measures

1. ISAE3402 /SSAE 18 (SOC 2) Audit: GPTW shall ensure compliance with ISAE3402/SSAE 18 AICPA Trust Principles for Security, Confidentiality, and Availability (and, where in scope, Privacy and Processing Integrity), and will undergo an audit each year for the purposes of examining the relevant controls with respect to the Services. Such audits shall be carried out by an independent, certified third party and the resulting reports shall be provided to Customer upon request. GPTW shall ensure the data center carries out its own SOC 2 audits and provide such reports to Customer upon request.

2. Audit by Customer: GPTW shall demonstrate appropriate technical and organizational measures to Customer throughout the term. Customer may exercise such audit right either personally or by appointing a third party that is bound by appropriate obligations of confidentiality and acceptable to GPTW. Customer may exercise such audit right on an annual basis with reasonable notice. Any such audits shall be limited to a robust customer due diligence package consisting of details on GPTW's information security/risk practices, examination of the results of the annual AICPA SSAE 18 SOC 2 Type audits conducted by an independent third party, executive summaries of the annual penetration test results or verification of such testing through the SOC 2 report, and reasonable access to knowledgeable personnel to discuss the controls in place, including a meeting at GPTW corporate headquarters. In the event Customer requests support or information beyond the content described above, then, upon customer's audit request, the Parties will mutually agree on the terms of the audit plan, which shall include details regarding the scope, duration, fees, and scheduling of the audit. In no event shall Customer or its designees be permitted to access GPTW systems, network servers, scan summaries or activities logs.

a) ISO 27000 Series Audits: GPTW shall also ensure the datacenter used to provide the Services will continue to have its IT security management certified according to ISO 27001 or comparable industry standard security framework.

3. Entity Controls: Consistent with GPTW's obligation to maintain its compliance programs as described above, GPTW shall continuously carry out the following security measures:

a) Security Policy: GPTW shall maintain an information security policy that is reviewed annually by GPTW and published and communicated to all GPTW employees. GPTW shall maintain a dedicated security and compliance function to maintain and monitor security controls across GPTW.

b) Employee Onboarding: All GPTW personnel shall be subject to a comprehensive background check and agree to accept GPTW's Code of Conduct upon hire.

c) Employee Termination: GPTW shall terminate all credentials and access to the Services of a GPTW employee in the event of termination of his or her employment within a reasonably timely manner.

d) Access Controls by GPTW Personnel: Access to all GPTW owned or licensed network components, servers, databases, computers, and software programs by GPTW personnel shall be protected by an authentication procedure that requires giving at least a unique username and complex password. GPTW shall implement technical controls to enforce a password policy consisting of a minimum number of characters and complexity, including requirements of alpha, numeric, upper case, lower case and/or special characters. Lockout periods shall be in effect for inactivity and unsuccessful password attempts. Passwords shall expire after a fixed amount of time.

e) Security Awareness Training: GPTW employees shall participate in security awareness and privacy training, upon hire and annually thereafter.

f) Change Management: GPTW shall employ a change management process based on industry accepted standards for change management in configurations, software, and hardware.

4. Application and Network Controls:

a) Privileged Access by GPTW Personnel: Privileged access to GPTW owned or licensed network components, servers, databases, computers, and software programs by GPTW personnel that are used in the provision of the Services shall be secured by means of a two-factor authentication and shall be defined by GPTW in such a manner as to ensure that the access authorizations are granted only to the extent necessary to perform the assigned role. Any access to GPTW's systems used in the provision of the Services shall be monitored.

b) Infrastructure of the Data Center: GPTW and/or its sub-processor(s) shall monitor the infrastructure in order to identify any security vulnerabilities.

c) Anti-Virus and Malware Scanning: GPTW uses commercially available malicious code detection software, including virus detection and malware detectors, on GPTW systems. Anti-virus definition files shall be updated regularly, on a scheduled basis, following the availability of such updates by the software provider.

d) Secure Coding Practices: GPTW developers shall be trained on secure development. Applications should be written in a secure manner to implement industry practices, such as input validation, session management, SQL injection, and cross site scripting mitigation. These practices shall be tested as part of the annual penetration testing described below.

e) Patch Management: GPTW shall review all patches, updates, and upgrades of operating systems, middleware, or applications to all relevant components of the Services after they have been released by the manufacturer and tested by GPTW. GPTW shall manage the patching process prudently to assure that critical patches are applied in a timely manner consistent with the associated risk.

f) Segregation of Customer Data: GPTW shall provide appropriate security controls and segmentation methods to protect and isolate Customer Data from other tenants.

g) Encrypted Data Transfers: Customer Data input into the Services shall be secured using an industry standard protocol, such as Transport Layer Security (TLS).

h) Encrypted Data Storage: GPTW shall encrypt Customer Data using industry standard technology, such as AES-256 encryption standard for data at rest.

i) Firewalls: Connections to the Services networks, shall be protected with industry standard firewalls. GPTW shall update its firewall software regularly, on a scheduled basis, following the availability of updates by the software provider.

j) Intrusion Detection: GPTW shall implement and maintain an intrusion detection monitoring process at the network and/or host level to protect the Services and detect unwanted or hostile network traffic. GPTW shall update its intrusion detection software regularly, on a scheduled basis, following the availability of updates by the software provider or a heuristic analysis shall be used.

k) Systems Hardening and Secure Configuration: GPTW shall follow industry standards for platform hardening and secure configuration. GPTW shall remove or disable unnecessary utilities from operating system configurations and restrict access rights to least privilege.

l) Penetration Testing: GPTW shall contract, as part of its security program and on at least an annual basis, with an independent third party to conduct a network and application penetration test. The penetration test will include, but is not limited to, the potential for unauthorized internet access, compromise of roles, and escalation of privileges for the Services. Upon request, GPTW will provide an executive summary of said penetration test including the scope and methodology of the test and confirmation that critical and high-risk findings have been remediated or provide an independent third-party audit report attesting to such testing and remediation. Penetration testing includes the web application vulnerabilities defined by the Open Web Application Security Project (OWASP) Top 10 and those listed in the SANS 25 (as applicable) or its successor current at the time of the test.

m) Vulnerability Management: GPTW shall implement commercially reasonable processes designed to protect Customer Data from system vulnerabilities. GPTW shall perform scanning of the infrastructure using an industry recognized automated scanning tool designed to detect security flaws and security vulnerabilities within the operating systems. GPTW shall assess scan results and remediate relevant security vulnerabilities within a reasonable amount of time based on the risk to the Services.

n) Audit Logging: GPTW shall log GPTW personnel's access to the Services to maintain an audit trail that includes, but is not limited to, web server logs, system logs, and network event logs.

5. Physical Access Control: GPTW shall ensure that its data center sub-processor uses industry standard technology to ensure that only the appropriately authorized staff have access to those systems of GPTW that are used to provide the Services. This shall include at least the following measures: visitor sign-ins, role-based access controls, limited access to the server rooms and to the alarm systems which report any unauthorized access.

6. Security Monitoring: GPTW may monitor and analyze the use of its Subscription Services, which may record information concerning security controls and compliant use of the application, the events that occur within the application, aggregated usage, performance data, and access locations. The Subscription Services will collect usage statistics, telemetry, and other data from Customer, such as email address, IP address, and other unique verification identifier, for the purposes of enabling multifactor authentication; benchmarking, modelling, and training; providing, operating, maintaining, customizing, and improving the Subscription Services and its security, including by developing new or different functionalities for such purposes.

7. Incident Response and Notification:

a) GPTW shall maintain security incident management policies and procedures, including security incident escalation procedures. In the event GPTW confirms unauthorized access or acquisition, disclosure or use of Customer's Personal Data has occurred, GPTW agrees to notify Customer, in accordance with the terms of the Agreement or per Applicable Laws.

b) GPTW shall (i) investigate such information security incident and perform a root cause analysis; (ii) remediate the effects of such information security incident; and (iii) provide Customer with assurances that such information security incident is not likely to recur.

8. Disaster Recovery: GPTW shall maintain a Disaster Recovery plan and present verification of this plan (via the SOC 2 reporting) at the request of Customer. GPTW shall test this plan once a year and verify that the planned measures are effective, reviewed by management and updated as necessary.

9. Business Continuity: GPTW shall maintain a plan for returning to operation in the event of a disaster and present a summary of this plan at the request of Customer. Upon GPTW's declaration of disaster, GPTW shall implement said plan to return the Services to operation. GPTW shall annually test and review its business continuity plan and update as necessary.

Schedule 3: Additional Applicable Privacy Provisions

The following provisions will apply if and to the extent applicable to the Processing of Customer Personal Data by GPTW.

1. U.S. Privacy Laws

"U.S. Privacy Laws" have the same meaning as in Applicable Laws and regulations concerning the privacy and security of information reasonably identifying or linked to an individual, including, without limitation, the California Consumer Privacy Act, Cal. Civ. Code § 1798.100 et seq. or its successor the California Privacy Rights Act, Cal. Civ. Code § 1798.100 et seq., and their accompanying regulations as promulgated by the California Attorney General or California Privacy Protection Agency, as then applicable (collectively the "CPRA"); the Colorado Privacy Act, Colo. Rev. Stat. § 6-1-1309 et seq. (the "CPA") the Connecticut Data Privacy Act, Public Act No. 22-15 (the "CTDPA"); the Utah Consumer Privacy Act, Utah Code § 13-61-101 et seq. (the "UCPA "); and the Virginia Consumer Data Protection Act, Virginia Code § 59.1-571 et seq. (the "VCDPA").

Obligations. To the extent GPTW is a Service Provider or Processor and receives Personal Information from Customer and processes Personal Information on behalf of Customer in connection with GPTW's provision of the Services to Customer, GPTW in its role as a Service Provider or Processor, will not: (i) Sell or Share such Personal Information; (ii) shall not retain, use, or disclose such Personal Information for any purpose other than performing the Services or Business Purpose under the Agreement or as otherwise permitted by the U.S. Privacy Laws; (iii) retain, use, or disclose the Personal Information for a commercial purpose other than providing the Services unless otherwise permitted under the Agreement; or (iv) retain, use, or disclose such Personal Information outside of the direct business relationship between Customer and Service Provider unless otherwise permitted under the Agreement; (v) combine the Personal Information that the Service Provider receives from, or on behalf of, the Business with personal information that it receives from, or on behalf of, another person or persons, or collects from its own interaction with the consumer, provided that the Service Provider may combine personal information to perform any Business Purpose. GPTW, in its role as a Service Provider or Processor, agrees to comply with the US Privacy Laws as applicable to Service Provider in its provision of the Services to Customer under the Agreement. For clarity, GPTW shall notify Customer if it makes a determination that it can no longer meet its obligations under the CPRA and Customer may take reasonable and appropriate steps to stop and remediate the unauthorized Processing of Personal Information.

Consumer Requests. To the extent applicable, and subject to the nature of the Processing and the information available to GPTW, GPTW will reasonably assist Customer with the fulfilment of Customer's obligation to respond to consumer requests for exercising the data subject's rights as set out under the U.S. Privacy Laws.

2. United Kingdom ("UK") International Data Transfer Addendum to the EU Commission Standard Contractual Clauses

The UK International Data Transfer Addendum to the EU SCCs is available on https://www.greatplacetowork.com/cross-border-transfer-mechanisms, and is deemed incorporated in this DPA, in accordance with Section 11 of the DPA.

In connection with transfers of Customer Personal Data to which UK GDPR applies, GPTW will only operate cross-border transfer of Customer Personal Data either to Countries with Adequate Protection or based on a Cross-Border Transfer Mechanism.

If the Processing of Customer Personal Data involves any transfers to a country that is not a Country with Adequate Protection, then:

If GPTW's billing address is in an Adequate Country, the appliable UK IDTA (Processor-to-Processor) will apply with respect to all Restricted Transfers that are subject to the UK GDPR from GPTW to Subprocessors and GPTW Affiliates;

If GPTW's billing address is not in a Country with Adequate Country, appliable UK IDTA (Controller to Processor) will apply with respect to Restricted Transfers between GPTW and Customer.

3. Switzerland

Where Applicable Laws of Switzerland requires sufficient safeguards for the adequate protection of Personal Data transferred to a third country, the EU SCCs shall apply. In case of a transfer from Switzerland subject to the Applicable laws of Switzerland, the terms below will have the following substituted meanings for the purposes of the EU Clauses: (i) "GDPR" means the FADP and the Revised FADP. (ii) "European Union", "Union" or "Member States" means Switzerland, provided that the term "member state" must not be interpreted in such a way as to exclude data subjects in Switzerland from the possibility of suing for their rights in their place of habitual residence, provided it is in Switzerland in accordance with Clause 18 c. (iii) "Supervisory Authority" means the FDPIC. The EU SCCs shall also protect the data of legal entities until the entry into force of the Revised FADP

In connection with transfers of Customer Personal Data to which FADP applies, GPTW will only operate cross-border transfer of Customer Personal Data either to Countries with Adequate Protection or based on a Cross-Border Transfer Mechanism.

If the Processing of Customer Personal Data involves any transfers to a country that is not a Country with Adequate Protection,

then:

- If GPTW's billing address is in an Adequate Country, the applicable EU SCCs (Processor-to-Processor) will apply with respect to all Restricted Transfers that are subject to the GDPR from GPTW to Subprocessors and GPTW Affiliates;

- If GPTW's billing address is not in a Country with Adequate Country, appliable EU SCCs (Controller to Processor) will apply with respect to Restricted Transfers between GPTW and Customer.

4. APEC / Australia

"APEC" means the Asia Pacific Economic Cooperation, a regional economic forum established in 1989 to leverage the growing interdependence of the Asia-Pacific. See www.apec.org for more information.

"APEC Member Economy" means the 21 members of APEC: Australia, Brunei Darussalam, Canada, Chile, China, Hong Kong-China, Indonesia, Japan, Republic of Korea, Malaysia, Mexico, New Zealand, Papua New Guinea, Peru, Philippines, Russia, Singapore, Chinese Taipei, Thailand, United States, and Vietnam.

GPTW shall not transfer Personal Data outside of the jurisdiction where the Personal Data is obtained unless permitted under Applicable Laws. Where GPTW Processes Personal Data from an APEC Member Economy on behalf of Customer, GPTW shall perform such Processing in a manner consistent with the APEC Cross Border Privacy Rules Systems requirements ("CBPRs") (see www.cbprs.org) to the extent the requirements are applicable to GPTW's Processing of the Personal Data. If GPTW is unable to provide the same level of protection as required by the CBPRs, GPTW shall promptly notify Customer and cease Processing. In such event, Customer may terminate the Agreement with respect only to those Products and/or Services for which GPTW is unable to provide the same level of protection as required by the CBPRs by written notice within 30 days.

Any reference to Personal Data Breach is deemed to include Notifiable Data Breaches under the Australian Privacy Act 1988.

5. Argentina

Argentine Model Clauses: means the Model Agreement of International Transfer of Personal Data for the case of Provision of Services (Contrato modelo de transferencia internacional de datos personales con motivo de prestación de servicios) (reference: EX-2016-00311578- -APN-DNPDP#MJ- Anexo II) approved by the Dirección Nacional de Protección de Datos Personales on 2 November 2016 ("Argentinian Clauses").

In connection with transfers of Customer Personal Data to which Argentinian laws applies, GPTW will only operate cross-border transfer of Customer Personal Data either to Countries with Adequate Protection, or based on the Argentinian Clauses, which are deemed incorporated herein by reference. For the avoidance of doubts, any information required under the Argentinian Clauses are deemed provided under the Cross Border Mechanisms incorporated herein by reference.

6. China

Should Customer choose to use GPTW Services in China, Customer acknowledges that:

a) GPTW cannot guarantee the availability of GPTW Services in China;

b) Access to GPTW Services solution from China is not guaranteed, and therefore some provisions in the Agreement that governs the provision of GPTW's Services may not apply; and

c) In the event that parties engage in cross-border transfers of data outside of China and the Chinese Standard Contract for Export of Personal Information ("Chinese Standard Contractual Clauses" or "Chinese SCCs") is required by applicable Chinese laws to such cross-border transfer, the parties (or their applicable affiliates) agree to execute such separate Chinese SCCs to govern the cross-border transfers of data.

7. Brazil

The Parties shall handle Customer Personal Data in accordance with the Lei Geral de Proteção de Dados ("LGPD") and only for the purposes that are compatible with those described in the Main Agreement.

GPTW shall notify Customer in writing of (a) a confirmed Personal Data Breach, or (b) any notification, complaint, consultation or request made by the Brazilian National Data Protection Authority due to the processing of Customer Personal Data.

GPTW shall, in accordance with the terms of Article 18 of the LGPD, provide Customer with reasonable assistance when necessary to respond to a complaint, consultation or request from a data subject regarding the processing of Customer Personal Data (including, without limitation, any request for access, rectification, deletion, portability or restriction of processing of Customer Personal Data).

GPTW shall only transfer Customer Personal Data to another jurisdiction in accordance with the terms of the LGPD, and GPTW shall offer guarantees and compliance aligned with the regime of data protection provided in the LGPD for any transfer of Personal Data outside of Brazil.