GPTW Global Customer Data Processing Agreement

This DPA forms part of the agreement between the GPTW entity identified in the applicable agreement or Order ("GPTW") and the corresponding Customer (the "Agreement"). It governs the Processing of Personal Data by GPTW on behalf of Customer in connection with the Services. GPTW acts as a Processor (or equivalent role under Applicable Laws), and Customer acts as a Controller (or equivalent role under Applicable Laws).

1. Definitions

"Applicable Laws" means all laws and regulations applicable to the Processing of Personal Data under the Agreement, including, where applicable, data protection, privacy, and data security laws.
"DPA" means this Data Processing Agreement, including its Schedules 1 and 2, and any documents or materials referenced herein or made available via GPTW's website, including applicable jurisdiction-specific privacy provisions, as updated from time to time.
"Personal Data" means any information relating to an identified or identifiable individual, including "personal information" or "personally identifiable information" (PII) as defined under Applicable Laws, Processed by GPTW on behalf of Customer under the Agreement.
"Process" (and related terms such as "Processing" and "Processed") means any operation performed on Personal Data.
"Subprocessor" means any third party or GPTW Affiliate engaged by GPTW to Process Personal Data on behalf of Customer.

Capitalized terms not defined in this DPA have the meanings given to them in the Agreement or, where applicable, under Applicable Laws.

2. Processing of Personal Data

2.1 GPTW Processes Personal Data to provide the Services and as otherwise described in this DPA, in accordance with the Agreement and Customer's documented instructions, unless required by Applicable Laws, in which case GPTW, to the extent permitted, informs Customer prior to such Processing.
2.2 Customer instructs and authorizes GPTW and its Subprocessors to Process Personal Data as necessary to provide the Services, including transfers under this DPA.
2.3 Customer represents and warrants that it has all necessary rights and legal bases to provide Personal Data to GPTW for Processing in accordance with the Agreement and this DPA.
2.4 The subject matter, duration, nature, and purpose of the Processing, as well as the types of Personal Data and categories of Data Subjects, are set out in Schedule 1.
2.5 Taking into account the nature of the Processing, GPTW provides reasonable assistance to Customer in meeting its obligations under Applicable Laws, as further described in this DPA.

3. Personnel

GPTW limits access to Personal Data to personnel who require such access to provide the Services or comply with Applicable Laws, and who are bound by confidentiality obligations and receive appropriate and regular privacy and security training.

4. Security

Details of the technical and organizational measures implemented by GPTW are set out in Schedule 2. GPTW implements and maintains appropriate technical and organizational measures to protect Personal Data, taking into account the risks to individuals, and will not materially diminish the overall level of security during the term of the Agreement.

5. Subprocessing

5.1 Customer authorizes GPTW to engage Subprocessors, including those identified herein or otherwise communicated to Customer.

5.2 GPTW provides Customer with a mechanism to be notified of new Subprocessors, including details of the Processing, at least thirty (30) days in advance. Customer may object to a new Subprocessor on reasonable data protection grounds within ten (10) days of such notice by written notice to privacy@greatplacetowork.com. If GPTW is unable to reasonably address Customer's objection within thirty (30) days, Customer may terminate the affected Services, without cause, upon written notice, and GPTW will cease providing the impacted Services thirty (30) days thereafter.
5.3 GPTW requires that each Subprocessor is bound by written obligations providing a level of protection for Personal Data no less protective than those set out in this DPA and remains responsible for the acts and omissions of its Subprocessors in connection with GPTW's Processing of Personal Data.

6. Data Subject Rights

6.1 GPTW provides reasonable assistance to Customer in responding to Data Subject requests under Applicable Laws, including by enabling access to Personal Data through the Services or otherwise to the extent available.
6.2 If GPTW receives a Data Subject request, it will direct the Data Subject to Customer, as GPTW does not have a direct relationship with Data Subjects, and will not respond except on Customer's instructions or as required by Applicable Laws, in which case GPTW will, to the extent permitted, inform Customer in advance.

7. Personal Data Breach

7.1 GPTW will notify Customer without undue delay upon becoming aware of a Personal Data Breach affecting Personal Data and will provide, to the extent available, information reasonably necessary for Customer to meet its obligations under Applicable Laws.
7.2 GPTW takes reasonable steps to investigate, mitigate, and remediate the Personal Data Breach and will reasonably cooperate with Customer in connection with such breach.
7.3 GPTW will not notify Data Subjects of a Personal Data Breach without Customer's prior written authorization, unless required by Applicable Laws.

8. Data Deletion and Retention

8.1 At all times during the term of the Services, Customer may access, export, or delete Personal Data, subject to available functionality. To the extent such functionality is unavailable or otherwise limited, and upon Customer's request or termination of the Services, GPTW will (i) delete reasonably identifiable and extractable Personal Data, including backups, except to the extent retention is required by Applicable Laws or otherwise permitted under this DPA, and (ii) provide Customer with a certificate of deletion upon written request.
8.2 GPTW provides tools to support Customer's data retention and deletion requirements but does not determine Customer-specific retention obligations. Customer remains solely liable for determining and implementing its own retention obligations.

9. Audit

9.1 GPTW makes available to Customer information reasonably necessary to demonstrate compliance with this DPA, including audit reports where in scope for the Subscription Services (e.g., SOC reports).
9.2 Customer may conduct an audit no more than once annually, upon reasonable notice, either directly or through a third party approved by GPTW and bound by 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. Audits are limited to review of a robust customer due diligence package consisting of details on GPTW's information security/risk practices and discussions with knowledgeable personnel.
9.3 Any additional audit requests are subject to mutually agreed scope, timing, scheduling and fees. Neither Customer nor any approved third party will be granted any access to GPTW systems, networks, security testing results or operational logs as part of any audit.

© 2026 Great Place To Work Institute, Inc. All Rights reserved.

10. Cross-Border Transfers

10.1 Customer acknowledges that GPTW may Process Personal Data globally as necessary to provide the Services.
10.2 Where Personal Data is transferred across borders, GPTW Processes such data in compliance with Applicable Laws, including through the use of appropriate transfer mechanisms.
10.3 Details of such transfer mechanisms, including Standard Contractual Clauses where applicable, as well as transfer risk assessments, are made available via GPTW's website and are incorporated by reference into this DPA.

11. Additional Assurances

11.1 In the event GPTW receives a legally binding request for disclosure of Customer Personal Data, GPTW will (i) notify Customer of such request unless prohibited by Applicable Laws; and (ii) will not respond to such disclosure request without prior notice to Customer, unless required by Applicable Laws.

11.2 In the event GPTW is not legally permitted to notify Customer of a legally binding request for disclosure of Customer Personal Data, GPTW agrees to take reasonable legal actions against the disclosure of 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.

12. General Terms

12.1 This DPA is governed by the law and jurisdiction specified in the Agreement.
12.2 In the event of any conflict between this DPA and the Agreement with respect to the Processing of Personal Data, this DPA prevails.
12.3 Any claims under this DPA are subject to the terms and limitations set forth in the Agreement.
12.4 If any provision of this DPA is held to be invalid or unenforceable, the remaining provisions will remain in full force and effect.
12.5 This DPA constitutes the complete agreement between the Parties with respect to the Processing of Personal Data and supersedes any prior or contemporaneous terms relating to such subject matter.

© 2026 Great Place To Work Institute, Inc. All Rights reserved.

Schedule 1 – Details of the Processing Activities

Category	**Description**
Subject Matter	Processing of Personal Data in connection with the Agreement or the DPA.
Duration	For the term of the Agreement and thereafter as required by Applicable Laws or the DPA.
Service Processing	To provide, operate, maintain, secure, and support the Services, including identifiable Personal Data.
Business Operations	Subject to the Key Safeguards set out herein, and limited to (i) Service monitoring, (ii) customer-specific improvements, (iii) general improvements, and (iv) development of new products and functionality, Customer instructs GPTW to Process Personal Data as reasonably necessary to provide, maintain, support, and enhance the Services, including through the use of data that has been processed in a manner such that it no longer identifies an individual.
Key Safeguards	Business Operations use data that is transformed to prevent practical linkage to individuals (as further set out in the Technical and Organizational Measures).
Restrictions	No cross-advertising; no profiling unless authorized and lawful.
Types of Data	Identification, employment, usage data, and other data submitted by Customer.
Data Subjects	Employees and Customer's other authorized users invited to take GPTW's survey.
Special Categories	Processed only where provided by Customer and in accordance with Applicable Laws.

© 2026 Great Place To Work Institute, Inc. All Rights reserved.

Schedule 2: Technical and Organizational Measures

The following Technical and Organizational Measures are applicable to Subscription Services. Consistent with GPTW's obligation to maintain its compliance programs as described above, GPTW shall continuously carry out the following security measures:

Security Policy: GPTW maintains an information security policy that is reviewed annually by GPTW, and which is published and communicated to all GPTW employees.

Employee Onboarding: To the extent permissible under Applicable Laws, all GPTW personnel are subject to a comprehensive background check and required to accept GPTW's Code of Conduct upon hire.

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

Access Controls:

a) Access to all GPTW-owned or licensed network components, servers, databases, computers, and software programs by GPTW personnel are protected by authentication procedures that require giving a unique username and complex password. GPTW enforces a password policy consisting of a minimum number of characters and complexity.
b) Privileged access by GPTW personnel involved in the provisioning of the Services is secured by means of two-factor authentication and is defined by GPTW in such a manner as to limit access authorizations only to the extent necessary to perform the assigned role. Any access to GPTW's systems used in the provision of the Services is logged and monitored.
c) GPTW terminates all credentials and access to the Services of a GPTW employee in the event of termination of his or her employment within a reasonable time frame.

Change Management: GPTW employs a change management process for configurations, software, and hardware based on industry accepted standards.

Anti-Virus and Malware Scanning: GPTW uses commercially available malicious code detection software, including virus detection and malware detectors, on GPTW systems.

Secure Coding Practices: GPTW developers are trained on secure development. Applications should be written in a secure manner to implement industry best practices.

Patch Management: GPTW reviews 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 manages the patching process prudently to apply patches in a timely manner consistent with the associated risk.

Segregation of Customer Data: GPTW provides appropriate security controls and segmentation methods to protect and isolate Customer Data from other tenants.

Encryption:

a) Customer Data input into the Services is secured using an industry standard protocol, such as Transport Layer Security (TLS).
b) GPTW encrypts Customer Data using industry standard technology, such as AES-256 encryption standard for data at rest.

Firewalls: Network connections to the Services are protected with industry standard firewalls. GPTW updates its firewall software regularly and on a scheduled basis.

Intrusion Detection: GPTW implements and maintains an intrusion detection monitoring process to protect the Services and detect unwanted or hostile network traffic. GPTW updates its intrusion detection software regularly and on a scheduled basis.

© 2026 Great Place To Work Institute, Inc. All Rights reserved.

Systems Hardening and Secure Configuration: GPTW follows industry standards for platform hardening and securing configuration. GPTW removes or disables unnecessary utilities from operating system configurations and restricts access rights to least privilege.

Testing:

a) GPTW contracts with an independent third party to conduct a penetration test on a regular basis.
b) GPTW performs scanning of the infrastructure using an industry recognized automated scanning tool designed to detect security flaws and security vulnerabilities within the operating systems. GPTW assesses scan results and remediates relevant security vulnerabilities within a reasonable amount of time based on the risk to the Services.

Physical Access Control: GPTW requires that its data center subprocessor uses industry standard technology such that only the appropriately authorized staff have access to those systems of GPTW that are used to provide the Services.

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 mobile number, email address, IP address, and other unique verification identifiers, 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 enhancing the customer and/or user experience with new functionalities.

Incident Response: GPTW maintains security incident management policies and procedures, including security incident escalation, mitigation and remediation procedures.

Disaster Recovery: GPTW maintains a Disaster Recovery plan and tests the plan regularly to verify that the planned measures are effective, reviewed by management, and updated as necessary. GPTW maintains disaster recovery and backup processes intended to achieve a Recovery Time Objective of up to 72 hours and a Recovery Point Objective of up to 12 hours.

Business Continuity: GPTW maintains a plan for returning to operation in the event of a disaster. Upon GPTW's declaration of disaster, GPTW implements said plan to return the Services to operation. GPTW regularly tests and reviews its business continuity plan and updates it as necessary.

Key Safeguards: GPTW applies technical, organizational, and statistical safeguards designed to reduce the risk of identifying individuals or specific Customers from resulting datasets and outputs.

a) **Identifier Controls.** GPTW removes, excludes, or transforms direct employee identifiers prior to cross-customer Business Operations Processing activities where such identifiers are not required. Information used to support customer classification, benchmark generation, and related processing is maintained separately and subject to access restrictions.
b) **Statistical Disclosure Controls.** GPTW applies aggregation, suppression, and other disclosure-risk controls designed to reduce the risk that Business Operations outputs identify, single out, or reveal information about an individual data subject or a specific Customer. Such controls are calibrated to the nature of the processing activity, the relevant dataset, and the intended output. Outputs may be withheld, restricted, modified, aggregated, or suppressed where appropriate to mitigate disclosure risk.
c) **Access and Segregation Controls.** GPTW restricts access to Business Operations datasets through role-based access controls, least-privilege principles, segregation of duties, logging, monitoring, encryption, and other appropriate safeguards. Access to source datasets is limited to authorized personnel with a legitimate business need. Cross-customer processing activities are conducted within logically segregated environments with separate processing resources and access controls appropriate to the processing activity.

© 2026 Great Place To Work Institute, Inc. All Rights reserved.

d) **Data Minimization and Dataset Design**. Business Operations Processing is limited to data reasonably necessary for the applicable purpose. Cross-customer datasets are designed to exclude direct employee identifiers and incorporate measures intended to reduce attribution, singling-out, and disclosure risks, including restrictions on benchmark granularity and retained linkage information. Benchmark outputs are designed to reflect aggregated populations rather than individual persons or specific Customers.

e) **Governance Controls.** Materially new cross-customer Business Operations use cases are subject to privacy, security, compliance, and governance reviews appropriate to the processing activity prior to implementation.

f) **Retention and Linkage Controls**. Temporary mappings, identifiers, or linkage mechanisms used to support a processing activity may be retained only as long as reasonably necessary for the applicable purpose and are not maintained as part of benchmark outputs. GPTW does not maintain or provide, as part of benchmark outputs, information designed to link benchmark results to specific source records, individuals, or Customers.

g) **Purpose Limitation.** Customer Data processed for Business Operations is used solely for the Business Operations purposes described in this DPA and as otherwise permitted under the Agreement. Customer Data is not sold and is not used for purposes unrelated to the Business Operations purposes described in this DPA.

Program Adjustments. GPTW monitors, evaluates, and updates its security program, as appropriate, in light of: (a) relevant changes in technology and internal or external threats to GPTW or Personal Data; (b) applicable security and data privacy requirements; and (c) changes in GPTW's business operations, including mergers and acquisitions, alliances and joint ventures, outsourcing arrangements, and changes to information systems.

© 2026 Great Place To Work Institute, Inc. All Rights reserved.