GREAT PLACE TO WORK® INSTITUTE, INC.
POLICY EXPLANATION

Will GPTW provide a copy of its SOC 1 and/or SOC 2 audits or other third-party security/financial audits?

GPTW considers third party security/financial audits confidential and does not release them to any company. There are several reasons for this policy. First, the audits are static in time and may not cover the entire term of the company's engagement. Second, the audits provide no legal protection to a company. Third, a company having possession of these audits places itself at serious risk for no benefit, e.g. should there be a GPTW security breach, any company in possession of these audits would be a primary litigation target and would have to prove that company's possession of the audits did not cause the GPTW breach. Instead, GPTW provides the highest standard of legal protection by warranting to the company that during the entire term of the engagement GPTW will comply with the following industry standards:

GPTW represents and warrants that during the Term it complies with Service Organization Controls (SOC) Report 1 and 2 under the Statement on Standards for Attestation Engagements (SSAE) 18 standard as well as with the International Organization for Standardization (ISO) 27001:2013 and ISO 9001:2015 standards and the National Institute of Standards and Technology (NIST 2015) cybersecurity framework. GPTW also complies with the Payment Card Industry Data Security Standard (PCI DSS). This warranty is found on the GPTW website in Section 7 (Data Security) of the of the GPTW Products and Services Agreement (PSA).

GPTW maintains a full-time Chief Data Protection Officer (CDPO) and staff to ensure compliance with these industry standards. The CDPO reports directly to the CEO of GPTW.

Does GPTW comply with all Data Protection Laws in the EU (GDPR) as well as all other countries?

Yes. GPTW will use commercially reasonable efforts consistent with industry standards to collect, transmit, store, protect and maintain the Data and Company Data obtained through the Services. GPTW represents and warrants that during the Term it complies with the European Union (EU) 2016 General Data Protection Regulation (GDPR) and any Data Protection Laws. GPTW is also certified under the US/EU and US/CH Privacy Shield. This warranty is found on the GPTW website in Section 8 (Data Privacy) of the GPTW PSA. GPTW collects Data for processing and archiving scientific and historical research purposes and statistical purposes assessing workplace culture, performance, and accreditation to assist organizations in evaluating and improving their workplaces. This exact language is found in Article 89 of the GDPR.

As advised in the GDPR, GPTW maintains a full-time Chief Data Protection Officer (CDPO) and staff to ensure compliance with all Data Protection Laws. The CDPO reports directly to the CEO of GPTW. GPTW also employs full-time Certified Information Privacy Practitioner (CIPP) and staff who is certified under the NIST standard as administered by the International Association of Privacy Professionals at www.iapp.org.

Can a Company use its Master Services Agreement?

Yes, but only after payment of a review fee of $20,000. The payment of the fee must be received before any review starts. Why the fee? GPTW has quoted to Company the lowest price for its products and services. This low price quote means accepting the GPTW Order Form and /or SOW and the GPTW Products and Services Agreement found at the website:

https://www.greatplacetowork.ca/images/documents/Products-and-Service-Agreement-06-2019.pdf. The quote does not include what GPTW needs to be compensated for the extra time and personnel required to perform the review and the documentation that must be developed just for your Company. It is important to note that because of the unique products and services being delivered by GPTW, a company's Master Services Agreement definitely will not properly address Data ownership, Data processing, compliance with all Data Protection Laws, compliance with Data security industry standards, etc.

Can a Company change the GPTW Product and Services Agreement?

Yes, but only after payment of a review fee of $15,000. The payment of the fee must be received before any review starts. Why the fee? GPTW has quoted to Company the lowest price for its products and services. This low price quote means accepting the GPTW Order Form and /or SOW and the GPTW Products and Services Agreement found at the website: https://www.greatplacetowork.ca/images/documents/Products-and-Service-Agreement-06-2019.pdf. The quote does not include what GPTW needs to be compensated for the extra time and personnel required to perform the review and the documentation that must be developed just for your Company. It is important to note that because of the unique products and services being delivered by GPTW, special care had to be taken to craft the GPTW Products and Services Agreement to address issues like Data ownership, Data processing, compliance with all Data Protection Laws, compliance with Data security industry standards, etc. It is important to note, GPTW will not make any material changes to its PSA.

Will GPTW fill out a Company's security survey/document?

Yes, but only after payment of a review fee of $10,000. The payment of the fee must be received before any review starts. All of the answers to any security survey is found on the GPTW website at https://www.greatplacetowork.ca/images/documents/GPTW-External-Security-Policy-10012018.pdf. The Company can use the GPTW External Security Policy to fill out its own security survey. Why the fee? GPTW has quoted to Company the lowest price for its products and services. This low-price quote means accepting the answers provided in the above GPTW External Security Policy. Otherwise, GPTW needs to be compensated for the extra time and personnel required to answer the survey. Furthermore, a company's security survey provides no legal protection. A survey is static in time and may not cover the entire term of the company's engagement. Instead, GPTW provides the highest standard of legal protection by warranting to the company that during the entire term of the engagement GPTW will comply with the following industry standards:

GPTW represents and warrants that during the Term it complies with Service Organization Controls (SOC) Report 1 and 2 under the Statement on Standards for Attestation Engagements (SSAE) 18 standard as well as with the International Organization for Standardization (ISO) 27001:2013 and ISO 9001:2015 standards and the National Institute of Standards and

Technology (NIST 2015) cybersecurity framework. GPTW also complies with the Payment Card Industry Data Security Standard (PCI DSS). This is found on the GPTW website in Section 7 (Data Security) of the GPTW PSA.

Will GPTW provide Certificates of Insurance (COI)?

Yes, but only after payment of a retrieval fee of $4,000. The payment of the fee must be received before retrieval begins. Why the fee? GPTW has quoted to Company the lowest price for its products and services. This low-price quote means accepting the quote without further involvement of GPTW personnel. Otherwise, GPTW needs to be compensated for the extra time and personnel required to retrieve the COI. Furthermore, a Certificate of Insurance provides no legal protection. A COI is static in time and may not cover the entire term of the company's engagement. Instead, GPTW provides the highest standard of legal protection by warranting to the company that during the entire term of the engagement GPTW will carry the insurance coverage itemized in Section 12.8 (Insurance) of the GPTW PSA found on the GPTW website.

What Data Does GPTW Collect?

The nature and purpose as well as the subject matter and duration of the Processing of the Company Personal Data is to collect Company employee survey data for processing and archiving scientific and historical research purposes and statistical purposes assessing workplace culture, performance, and accreditation to assist organizations in evaluating and improving their workplaces. This exact language is found in Article 89 of the GDPR. The types and categories of Company Personal Data to be processed is found in the demographic section and Trust Index questions of the survey.

How does Emprising™ comply with Data Security and data Privacy laws?

The GPTW Emprising™ survey and analytics software platform operates by uploading to Emprising an email address list for the Company's Employees taking the survey and, optionally, other information such as pre-coded demographics etc. by either GPTW or the Company. The email list is stored encrypted in a separately partitioned area from the Company Employee Data. When the Company survey opens, the email list is used to generate a personalized invite to each Company Employee which is a log-in identifier unique to each Company Employee. When the Company survey closes, the email list used to link to the Company Employee Data is deleted. As a result, the Company Employee Data is immediately de-identified and made anonymous.

To protect the confidentiality of the Company Employee Data, GPTW uses a suppression algorithm. GPTW will not report on Assessment results in which fewer than five (5) people in a Company demographic group have responded.

A unique identifier for Data Subjects may be kept as long as it is assigned randomly at the time of survey (e.g. as a sequential number generated by a database upon the insertion of a new record) and is not associated with external data that create a re-association with the Data Subject's Personal Data; the unique identifier is only used as required within a relational database for Survey responses and associated data for a given year.

October 1, 2018