Appendices

Appendix 1: Master Services Agreement

This Master Services Agreement (this "Agreement") is made between GPTW Switzerland AG ("GPTW") and the person or entity that is named in the Offer that references this Agreement ("Customer"). CUSTOMER AGREES THAT ITS USE OF GPTW'S SUBSCRIPTION SERVICES AND GPTW'S PERFORMANCE OF PROFESSIONAL AND SUPPORT SERVICES ARE SUBJECT TO AND GOVERNED EXCLUSIVELY BY THIS AGREEMENT AND ANY ADDITIONAL TERMS STATED IN THE OFFER, INCLUDING ANY ATTACHMENTS THERETO. This Agreement is effective as of the signature date stated in the applicable Offer as "date" ("Effective Date").

1. Services

1.1 Subscription Services. The Services will be identified in the Offer. During the Initial Term and all applicable Renewal Terms defined in the Offer, GPTW will provide the Services to Customer and Customer may use such Services listed in the Offer solely for its internal business purposes, subject to and conditioned on compliance with this Agreement and the Offer.

1.2 Support Services. GPTW shall maintain a trained and knowledgeable staff capable of providing support for the Services. GPTW will use commercially reasonable diligence to correct reproducible errors when reported to GPTW and provide phone, email, or online support. GPTW will also provide periodic enhancements and modifications to the Subscription Services, including bug fixes, to correct reproducible errors reported to GPTW.

1.3 Professional Services. GPTW will provide the Professional Services listed in the Offer, in accordance with the Offer. If Customer requests additional Professional Services that were not previously identified on an Offer or Statement of Work, then Customer may need to execute an additional Offer or Statement of Work.

2. Acknowledgements

2.1 Reservation of Rights. The Services are provided with a limited right to use and are not sold, and GPTW reserves and retains all rights not expressly granted in this Agreement. GPTW has and shall maintain sole and exclusive ownership of all rights, title, and interest in the Services, and all modifications and enhancements thereof (including ownership of all trade secrets, copyrights, trademarks, brands, and other intellectual property rights pertaining thereto). There will be no "work for hire" or any deliverables owned by Customer created as part of the Services and all works, customizations, and developments created as part of the Services shall be considered a part of the Services.

2.2 Use Restrictions. Except as expressly provided in this Agreement, no other use of the Services provided by GPTW is permitted. Customer may not, and may not cause or permit others to: (a) reverse engineer, disassemble, adapt, translate, or decompile

the Subscription Services, including, without limitation, any third party components, or otherwise attempt to derive source code, trade secrets, or knowhow from the Subscription Services; (b) license, sell, transfer, assign, distribute, or outsource use of the Subscription Services, or provide service bureau, data processing, or time sharing access to the Subscription Services; (c) create Internet "links" to the Subscription Services or "frame" or "mirror" the Subscription Services on any other server, or wireless or Internet-based device; (d) access or use the Subscription Services to build or support, directly or indirectly, products or services competitive to GPTW; (e) interfere with or disrupt the integrity or performance of any Subscription Services or any data contained therein; (f) attempt to gain unauthorized access to any Subscription Services or its related data, systems, or networks; or (g) remove or alter any proprietary notices or marks on the Services.

2.3. GPTW Badges. GPTW grants to Customer a non-exclusive, revocable, limited license to use and display:

2.3.1 The Certification Badge during the Certification Period for the sole purpose of promoting Customer's designation as a Great Place To Work during the Certification Period. When displaying the Certification Badge, Customer will remain in full compliance with the Certification Badge Guidelines that can be found as appendix to the offer in the "Terms & Conditions for Great Place To Work® Certification™ and Best Workplaces™ List".

2.3.2 The Regional List Badge during the Regional List Inclusion Period for the sole purpose of promoting Customer's designation as a company that has achieved one of the top Trust Index scores within a global region, as defined by GPTW. When displaying the Regional List Badge, Customer will remain in full compliance with the International Regional List Badge Guidelines that can be found as appendix to the offer in the "Terms & Conditions for Great Place To Work® Certification™ and Best Workplaces™ List"

2.3.3. The National List Badge during the National List Inclusion Period for the sole purpose of promoting Customer's designation as a company that has achieved one of the top Trust Index scores within a designated country. When displaying the National List Badge, Customer will remain in full compliance with the National List Badge Guidelines that can be found as appendix to the offer in the "Terms & Conditions for Great Place To Work® Certification™ and Best Workplaces™ List"

2.4 Customer Feedback. Customer has no obligation to provide GPTW with any suggestion, enhancement request, recommendation, evaluation, correction, or other feedback about the Services ("Feedback"), but if it does, Customer grants to GPTW and its Affiliates a worldwide, perpetual, irrevocable, royalty-free license to use, copy, modify, distribute, disclose, create derivative works, and make and incorporate such Feedback into its Services for any purpose. GPTW has no obligation to incorporate or apply any Feedback to the Services.

2.5 Great Place to Work Institute Inc. (global umbrella organization) Licensees. Customer consents to persons or companies qualified and licensed by Great Place to Work Institute Inc. ("Licensees") to provide a portion of the Services on Great Place to

Work Institute Inc.'s behalf solely outside of the United States. Great Place to Work Institute Inc. shall be responsible for the actions of its Licensees relating to the portion of the Services the Licensee(s) provide Customer on Great Place to Work Institute Inc.'s behalf.

2.6 Compliance with Laws. GPTW shall comply with Applicable Laws in performing its obligations hereunder. Customer shall comply with Applicable Laws when using the Services and remains solely responsible for its compliance with Applicable Laws, including, but not limited to, with respect to the configuration and use of the Services and regardless of whether GPTW provides assistance with Customer compliance matters. Customer acknowledges that the specific privacy requirements established under Applicable Laws relating to Customer are the responsibility of Customer and not GPTW.

2.7 Upgrades. Customer acknowledges that the Subscription Services may change at any time as required by changes to normal business conditions. It is further understood by Customer that any changes to the Subscription Services will be applicable to all GPTW customers utilizing the Subscription Services and such changes will not materially diminish the functionality of the Subscription Services.

2.8 Access Credentials. Except as otherwise provided herein, Customer will not provide any third party with access credentials to the Subscription Services and will safeguard and compel all users to safeguard the access credentials. Customer will be responsible for all acts and omissions of its users. Customer will notify GPTW promptly if it learns of any unauthorized use of any access credentials or any other known or suspected breach of security. If Customer allows use of the Subscription Services by any of its Affiliates without requiring such Affiliate to execute a separate Offer to establish its own tenant environment, then Customer will be fully responsible and liable for all use and misuse of the Subscription Services by such Affiliate, and will fully cooperate with GPTW in enforcing all of its rights to, interests in, and protection of the Services, including in seeking equitable remedies against any Affiliate that breaches this Agreement.

2.9 Connectivity. Customer is responsible for securing, paying for, and maintaining connectivity to the Subscription Services from Customer's location(s) via the internet, including any and all related hardware, software, third party services, and related equipment and components for such connectivity. Customer agrees that GPTW will have no liability for such connectivity and Customer will not be excused from any of its obligations under the Agreement as a result of the quality, speed, or interruption of the communication lines from the Customer's location(s) to the internet.

3. Fees

3.1 Fees. Customer will pay the fees on the payment terms and in the currency indicated in the Offer. For each Offer, the billing period of the fees will start as set forth in the Offer and will continue for the time period indicated as the Initial Term on the Offer and all Renewal Terms. Customer is responsible to pay for the Services for the entire Initial Term and each Renewal Term. Except as otherwise specified in the Offer(a) subscription fees are based on Subscription Services purchased and not time

of actual usage; (b) minimum quantities purchased cannot be decreased during the relevant subscription term; (c) additional quantities may be purchased; and (d) payment obligations are non-cancelable and fees paid are non-refundable.

3.2 Taxes. The fees exclude, and Customer will be responsible for, all sales, use, excise, withholding, VAT, and any other similar taxes, duties and charges of any kind imposed by any governmental entity in connection with the Services (excluding taxes based solely on GPTW's income).

3.3 Late Payment. Any invoices not reasonably disputed in writing within thirty (30) days from the date of receipt will be deemed undisputed and due. All undisputed invoices not paid within thirty (30) days after the date such amounts are due and payable may accrue interest at a rate up to the maximum allowable by applicable law. Customer will reimburse GPTW for any additional reasonable cost incurred by GPTW in connection with collecting any amounts payable under this Agreement. If Customer is more than thirty (30) days overdue in its payment of an undisputed amount due, then GPTW reserves the right to suspend the Services provided under the applicable Offer, but only until such payment is made to GPTW and provided that GPTW gives Customer at least ten (10) business days prior written notice of the overdue amount before GPTW suspends the Services. Upon payment in full of all overdue amounts, GPTW will restore the Services.

4. Data, Security and Privacy

4.1. Ownership and License of Customer Data. Customer shall retain ownership of the entire right, title, and interest in and to Customer Data and Raw Data. Customer grants GPTW a non-exclusive, worldwide license for the term of this Agreement, to use, sample, collect, and compile the Customer Data for the purposes of providing, maintaining, improving, or operating the Services, and for benchmarking purposes.

4.2. Raw Data License. Customer grants to GPTW a non-exclusive, perpetual, irrevocable, worldwide license to use, sample, collect, and compile Raw Data in aggregated, de-identified form, that does not identify Customer Confidential Information, and that is stripped of all persistent identifiers (e.g., device identifiers, IP addresses, and cookie ID's), in a manner that does not allow the Raw Data on its own to be identified as originating from any individual survey taker, for the purposes of providing or maintenance of, improvement to, and operation of the Services, for new or different products or services, and for benchmarking purposes.

4.3. Collection of Personal Data. Services may employ applications and tools that collect and process Personal Data that may be required by GPTW to provide the requested Services or functionality included in or related to those Services. If Customer wishes to stop the collection and processing of Personal Data, Customer may need to discontinue using certain Services.

4.4. Data Privacy and Security. Each Party agrees to comply with Applicable Laws in its processing of Personal Data. GPTW and its sub-processors will process Personal Data in accordance with the Data Processing Agreement (DPA) which is incorporated in the Offer.

5. Confidentiality

5.1 Definition. "Confidential Information" is any non-public information relating to a Party that is disclosed pursuant to any Offer or this Agreement, and which reasonably should be understood by the recipient of such information to be confidential because of (a) legends or other markings; (b) the circumstances of the disclosure; or (c) the nature of the information itself.

5.2 Exceptions. Information will not be considered Confidential Information if the information was (a) in the public domain without any breach of this Agreement; (b) disclosed to the receiving Party on a non-confidential basis from a source lawfully in possession of such Confidential Information and, to the knowledge of the receiving Party, is not prohibited from disclosing such Confidential Information to receiving Party; (c) released in writing from confidential treatment by disclosing Party; or (d) is independently developed by the receiving Party without use of or reference to the Confidential Information.

5.3 Nondisclosure. Except as expressly permitted in this section, neither Party will disclose the other Party's Confidential Information to any third party.

5.4 Protection. Each Party will secure and protect the Confidential Information of the other Party with a reasonable standard of care commensurate with the sensitivity of such Confidential Information and using precautions that are at least as stringent as it takes to protect its own Confidential Information of like nature, but no less than reasonable precautions.

5.5 Use. Each Party will only use the Confidential Information of the other Party as expressly permitted by or as required to exercise their rights, duties, and obligations under this Agreement.

5.6 Disclosure Exceptions. Confidential Information may be shared with and disclosed to (a) any Affiliate, sub-processor, or other third party who has a need to know to enable the receiving Party to exercise its rights or perform its obligations in connection with this Agreement and have non-disclosure obligations at least as stringent as the confidentiality provisions of this Agreement that apply to the Confidential Information; or (b) any court or governmental agency of competent jurisdiction, pursuant to a subpoena, order, civil investigative demand or similar process with which the receiving Party is legally obligated to comply, and of which the receiving Party notifies disclosing Party as required by a legal process, including in connection with any proceeding to establish a Party's rights or obligations under this Agreement (provided however that, when permitted by Applicable Law, a Party will give the other reasonable prior written notice so that the disclosing Party has an opportunity to contest any disclosure required by a legal process).

6. Warranty

6.1 Mutual Warranties. Each Party hereby warrants that (a) it has the full right and authority to enter into this Agreement; and (b) the performance of its obligations and duties under this Agreement does not conflict with or result in a breach of any other

agreement of such Party or any judgment, order, or decree by which such Party is bound.

6.2 Subscription Services Warranty. GPTW warrants that the Subscription Services will substantially conform with the Offer and that the functionality of the Subscription Services will not be materially diminished or adversely modified. In the event of a breach of the warranty described in this Section, as Customer's exclusive remedy and GPTW's sole obligation, GPTW will make commercially reasonable efforts to remedy such breach without additional cost to Customer, provided that if GPTW cannot substantially remedy such breach, then Customer may terminate the affected Subscription Services in accordance with Section 7.2. Customer agrees to report any non-conformance of the Subscription Services within thirty (30) days of its discovery and provide GPTW with reasonable information and assistance to enable GPTW to reproduce or verify the non-conforming aspect of the Subscription Services.

6.3 Professional and Support Services Warranty. GPTW warrants that the Professional Services and Support Services will be performed by qualified personnel in a good and professional manner. In the event GPTW breaches the warranty described in this Section, as Customer's exclusive remedy and GPTW's sole obligation, GPTW will reperform the deficient Professional or Support at GPTW's cost, provided that if GPTW cannot substantially remedy such breach, then GPTW will refund any fees prepaid by Customer for the affected Services. Customer must report any deficiencies in such Professional or Support Services, within thirty (30) days of the completion of the non-compliant Professional or Support Services.

6.4 Disclaimer. TO THE EXTENT PERMITTED UNDER APPLICABLE LAW, GPTW DISCLAIMS ALL OTHER WARRANTIES NOT SET FORTH IN THIS AGREEMENT, EITHER EXPRESS OR IMPLIED, INCLUDING ALL WARRANTIES OF MERCHANTABILITY, QUALITY, PERFORMANCE, FITNESS FOR A PARTICULAR PURPOSE, NON- INFRINGEMENT, TITLE, AND ANY WARRANTIES ARISING FROM COURSE OF DEALING, USAGE, OR TRADE PRACTICE, IN CONNECTION WITH THIS AGREEMENT AND THE SERVICES. GPTW DOES NOT REPRESENT, WARRANT, OR COVENANT THAT THE SERVICES OR ANY OTHER PRODUCT OR SERVICE PROVIDED HEREUNDER WILL BE UNINTERRUPTED, ERROR-FREE, VIRUS-FREE, OR SECURE. THIS DISCLAIMER OF WARRANTY MAY NOT BE VALID IN SOME JURISDICTIONS AND CUSTOMER MAY HAVE WARRANTY RIGHTS UNDER LAW WHICH MAY NOT BE WAIVED OR DISCLAIMED. ANY SUCH WARRANTY RIGHTS EXTEND ONLY FOR THIRTY (30) DAYS FROM THE EFFECTIVE DATE OF THIS AGREEMENT (UNLESS AND ONLY TO THE EXTENT SUCH LAW PROVIDES OTHERWISE).

6.5 Customer Warranty. Customer warrants that it has all rights and required consents to provide Customer Data to GPTW.

7. Term & Termination

7.1 Term of the Agreement. The Term of this Agreement commences on the Effective Date and continues until the stated term in each applicable Offer has expired or has otherwise been terminated as provided in this Agreement. At the expiration of the Initial Term, and at the expiration of each Renewal Term (if mentioned in the Offer),

each as indicated on the Offer, the Services will automatically renew for the duration indicated on the Offer as the Renewal Term.

7.2 Types of Termination

7.2.1 For Cause. Either Party may terminate this Agreement, or any Service identified in an Offer, if the other Party fails to perform any material obligation under this Agreement, and such Party is not able to cure the non- performance within thirty (30) days of written notice of such default with reasonably sufficient detail regarding the alleged breach, provided that GPTW may immediately terminate or suspend Customer's access to the Services if Customer is in breach of the "Use Restrictions" or "Confidentiality" sections of this Agreement. Either Party may immediately terminate this Agreement and all Offers if the other Party has a receiver or similar party appointed for its property, becomes insolvent, acknowledges its insolvency in any manner, ceases to do business, makes an assignment for the benefit of its creditors, or files a petition in bankruptcy. Other than as expressly permitted in this Agreement, or an Offer, neither party may terminate this Agreement and remains fully obligated to the terms and conditions herein.

7.3 Effects of Termination. If the Agreement is terminated for any reason:

7.3.1 Fees. All fees will be paid by Customer for amounts owed through the effective date of termination, and, if the Agreement is terminated for GPTW's breach of the Agreement, any fees prepaid by Customer for the Service not rendered prior to the effective date of termination will be credited against Customer's account, with any remaining amounts refunded to Customer within thirty (30) days of the effective date of termination.

7.3.2 Cessation of Services. GPTW will cease to provide the Services to Customer and Customer's right to use and access the Subscription Services will end as of the effective date of termination. If Customer requires access to the Subscription Services after the effective date of termination or transition assistance, such access and assistance will be subject to mutual agreement and additional fees under a separate Offer, and will be subject to the terms and conditions of this Agreement.

7.3.3 Deletion of Customer Data. GPTW will delete Customer Data which is not Raw Data after Customer's rights to access the Subscription Services and retrieve Customer Data have ended, unless otherwise provided under this Agreement, an Offer, or another document. GPTW will delete Customer Data in a series of steps and in accordance with GPTW's standard business practices for destruction of Customer Data and system backups. GPTW has no obligation to retain Customer Data and Customer Data may be permanently deleted as part of GPTW's data management program(s) or practice(s), and in accordance with Applicable Laws.

8. Indemnification

8.1 Claims Against Customer. GPTW will defend Customer and Customer's respective directors, officers, and employees, who are acting on behalf of Customer ("Customer Indemnified Parties"), from and against any and all Claims to the extent alleging that the permitted uses of the Subscription Services infringe or misappropriate any

legitimate copyright or patent. GPTW will indemnify and hold harmless the Customer Indemnified Parties against any liabilities, obligations, costs, or expenses (including, without limitation, reasonable attorneys' fees) actually awarded to a third party by a court of applicable jurisdiction as a result of such a Claim, or as a result of GPTW's settlement of such a Claim.

8.2 Mitigation. In the event that a final injunction is obtained against Customer's use of the Subscription Services by reason of infringement or misappropriation of any such copyright or patent, or if in GPTW's opinion, the use of the Subscription Services is likely to become the subject of a successful Claim of infringement or misappropriation, GPTW (at its option and expense) will use commercially reasonable efforts to either (a) procure for Customer the right to continue using the Subscription Services as provided in the Agreement; or (b) replace or modify the Subscription Services so that they become non-infringing but remain substantively similar to the affected Subscription Services. Should neither (a) nor (b) be commercially reasonable, either Party may terminate the Agreement and the rights granted hereunder upon written notice, at which time GPTW will provide a refund to Customer of any fees paid by Customer for the infringing elements covering the period of their unavailability.

8.3 Exceptions. GPTW will have no liability to indemnify or defend Customer to the extent the alleged infringement or misappropriation of the Subscription Services is based on (a) a modification undertaken by Customer, or on behalf of Customer; (b) use other than as authorized by this Agreement; or (c) use in conjunction with any equipment, service, or software not provided by GPTW, where the Subscription Services would not otherwise infringe, misappropriate, or become the subject of the Claim.

8.4 Qualifications. Customer will provide written notice to GPTW promptly after receiving notice of a Claim. If defense of such Claim is materially prejudiced by a delay in providing notice, GPTW will be relieved from providing such indemnity to the extent of the delay's impact on the defense. GPTW will have sole control of the defense of any indemnified Claim and all negotiations for its settlement or compromise, provided that GPTW will not enter into any settlement which imposes any obligations on Customer without the prior written consent of Customer. Customer will cooperate fully (at GPTW's request and expense) with GPTW in the defense, settlement, and compromise of any such action. Customer may retain its own counsel at its own expense, subject to GPTW's rights above. This "Indemnification" section states GPTW's sole liability and Customer's exclusive remedy for all third party claims and damages.

8.5. GPTW Intellectual Property. Customer will defend, hold harmless, and indemnify GPTW and GPTW's respective directors, officers, and employees, who are acting on behalf of GPTW ("GPTW Indemnified Parties"), from and against any and all liabilities, obligations, costs, or expenses (including, without limitation, reasonable attorneys' fees) arising out of either (a) Customer's use of GPTW's Certification Badge, Regional List Badge, or National List Badge, in violation of the Certification Badge Guide or (b) Customer's use of other GPTW Intellectual Property which infringes or misappropriates any legitimate GPTW copyright, trademark, trade secret, or patent.

9. Limitations of Liability

9.1 Monetary Cap. DURING ANY TWELVE (12) MONTH CONTRACT TERM (BEGINNING ON THE EFFECTIVE DATE OF THE APPLICABLE OFFER), A PARTY'S TOTAL AGGREGATE LIABILITY FOR ANY AND ALL CLAIMS IN CONNECTION WITH ANY SERVICE SHALL IN NO EVENT EXCEED THE AMOUNT PAID OR PAYABLE BY CUSTOMER TO GPTW DURING SUCH TWELVE (12) MONTH CONTRACT TERM FOR THE SERVICE GIVING RISE TO SUCH CLAIM(S).

9.2 Exclusion of Damages. NEITHER PARTY WILL BE LIABLE FOR ANY INDIRECT, CONSEQUENTIAL, INCIDENTAL, SPECIAL, OR PUNITIVE DAMAGES; FOR THE COST OF ACQUIRING SUBSTITUTE OR REPLACEMENT SERVICES; OR FOR ANY LOST OR IMPUTED PROFITS OR REVENUES, BUSINESS INTERRUPTION, LOST GOODWILL, OR LOST DATA RESULTING FROM OR RELATED TO THE SERVICES OR THIS AGREEMENT, HOWEVER CAUSED; OR ANY DAMAGES TO THE EXTENT CAUSED BY CUSTOMER'S DATA OR APPLICATIONS, OR UNAUTHORIZED THIRD PARTY ACCESS OR INTRODUCTION OF MALICIOUS CODE.

9.3. Exclusions. THE LIMITATIONS OF LIABILITY CONTAINED IN SECTIONS 9.1 AND 9.2 SHALL NOT APPLY TO LIABILITIES ARISING FROM (A) A PARTY'S INDEMNITY OBLIGATIONS; (B) CUSTOMER'S PAYMENT OBLIGATIONS; OR (C) A PARTY'S GROSS NEGLIGENCE, FRAUD, OR WILLFUL MISCONDUCT.

9.4 Applicability of Limitations. THESE LIMITATIONS APPLY FOR ANY REASON, REGARDLESS OF ANY LEGAL THEORY AND FOR WHATEVER REASON LIABILITY IS ASSERTED, EVEN IF GPTW HAS KNOWLEDGE OF THE POSSIBILITY OF SUCH DAMAGES AND WHETHER OR NOT SUCH DAMAGES ARE FORESEEABLE. NOTWITHSTANDING ANYTHING TO THE CONTRARY IN THIS AGREEMENT, NOTHING IN THIS SECTION OR ELSEWHERE IN THIS AGREEMENT SHALL OPERATE TO EXCLUDE OR LIMIT THE LIABILITY OF ANY PARTY TO THE EXTENT SUCH LIABILITY CANNOT LAWFULLY BE SO LIMITED OR EXCLUDED UNDER APPLICABLE LAW. INSOFAR AS APPLICABLE LAW PROHIBITS ANY LIMITATION ON LIABILITY HEREIN, THE PARTIES AGREE THAT SUCH LIMITATION WILL BE AUTOMATICALLY MODIFIED, BUT ONLY TO THE EXTENT SO AS TO MAKE THE LIMITATION COMPLIANT WITH APPLICABLE LAW. THE PARTIES AGREE THAT THE LIMITATIONS ON LIABILITIES SET FORTH HEREIN ARE AGREED ALLOCATIONS OF RISK AND SUCH LIMITATIONS WILL APPLY NOTWITHSTANDING THE FAILURE OF ESSENTIAL PURPOSE OF ANY LIMITED REMEDY.

10. General

10.1 Jurisdiction & Dispute Resolution. This Agreement is governed by and is to be interpreted solely in accordance with the laws of Switzerland, without regard to any conflict of law provision that would result in the application of a different body of law, and each Party agrees to submit to exclusive venue in the courts of Switzerland in any dispute arising out of or relating to this Agreement. IF NOT OTHERWISE PROHIBITED BY APPLICABLE LAW, EACH PARTY AGREES THAT ANY CLAIM RELATED TO THIS AGREEMENT WILL BE RESOLVED ONLY ON AN INDIVIDUAL BASIS AND NOT IN A CLASS, CONSOLIDATED, OR REPRESENTATIVE ACTION, SUIT, OR OTHER SIMILAR PROCESS. The United Nations Commission on International Trade Law, the United Nations Convention on Contracts for the International Sale of Goods, will not apply to this Agreement.

10.2 Export. Each Party shall comply with the export laws and regulations of the United States and other applicable jurisdictions in providing and using the Services. Without limiting the generality of the foregoing, Customer represents that it is not on any U.S. government denied- party list and it shall not make the Services available to any person or entity that (a) is located in a country that is subject to a U.S. government embargo; (b) is listed on any U.S. government list of prohibited or restricted parties; or (c) is engaged in activities directly or indirectly related to proliferation of weapons of mass destruction.

10.3 Severability & Waiver. The invalidity or illegality of any provision in this Agreement will not affect the validity of any other provision. All unaffected provisions remain in full force and effect. The waiver of any breach of this Agreement will not constitute a waiver of any subsequent breach or default and will not negate the rights of the waiving Party.

10.4 Surviving Provisions. Provisions in this Agreement which by their nature are intended to survive in the event of a dispute or because their obligations continue past termination of the Agreement, including provisions relating to acknowledgements, reservation of rights, use restrictions, fees, confidentiality, limits of liability, indemnification, and termination, will so survive.

10.5 Assignment. This Agreement cannot be assigned by a Party, whether by operation of law or otherwise, without the prior written consent of the other Party; provided, however, that either Party may assign this Agreement in its entirety (including all Offers and Statements of Work) as part of a merger, acquisition, transfer, or sale of all or substantially all of its assets, stock or business, including to an Affiliate, so long as the assignee agrees to be bound by all of the terms and conditions of this Agreement, the Offers, and Statements of Work. This Agreement shall be binding on and inure to the benefit of all permitted predecessors, successors, and assigns of each Party.

10.6 Force Majeure. If an unforeseeable event reasonably beyond the control of either of the Parties arises to prevent a Party from performing its obligations under this Agreement, including, but not limited to, acts of war, terrorism, uprising, acts of nature like earthquakes or floods, outbreak of infectious disease, civil unrest, embargoes, riots, sabotage, labor shortages, changes in laws or regulations, the failure of the internet or communications via common networks, power or system failure, or a delay in transportation (collectively "Force Majeure"), each Party will be excused from performance of its obligations under this Agreement, except payment of fees, for the duration of the Force Majeure affecting such Party, provided that the affected Party will use reasonable efforts to mitigate the impact of the Force Majeure. Notwithstanding the foregoing, GPTW remains obligated to provide disaster recovery portions of the Services to the extent not also prevented by the Force Majeure.

10.7 Publicity. GPTW may refer to the Customer as a GPTW customer and use Customer's name and Customer's logo, on public platforms that include, but are not limited, to lists of GPTW's customers, and on GPTW's website. Where required under Applicable Law, the Parties will agree to the specific use of the name and logo in writing.

10.8 Notice. When either Party needs to provide notification or consent under this Agreement, those notices and consents must be in writing and considered delivered upon actual receipt. All notices to GPTW must be sent to the following: Attention: GPTW Switzerland AG, Schiffbaustrasse 7, 8005 Zurich, Switzerland All notices to Customer will be sent to the contact listed on the applicable Offer. Any cure period required under this Agreement will begin on the date the notice is received.

10.9 eSignature. Each Party agrees that an eSignature (or a facsimile signature by the authorized representative) is evidence of acceptance of a valid and enforceable agreement.

10.10 No Third Party Beneficiaries. The provisions of this Agreement are for the sole benefit of the Parties and they will not be construed as conferring any rights on any third party nor are there any third party beneficiaries to this Agreement.

10.11 Relationship of the Parties. The Parties are independent contractors. Nothing in this Agreement shall be deemed to constitute a partnership or joint venture between the Parties or constitute any Party to be the agent of the other Party for any purpose.

10.12 Entire Agreement. This Agreement (and any information in referenced herein, including in an exhibit, schedule, attachment, annex, or at any URL) along with any corresponding Offer, SOW, and Services Description constitute the entire agreement between the Parties pertaining to each Offer. This Agreement supersedes all prior and contemporaneous representations, negotiations, and communications between the Parties relating to the Services and its subject matter. This Agreement may only be amended in writing signed by each of the Parties. If Customer uses its own purchase order or similar document, any terms or conditions in such purchase order are null and void. In the event of a conflict between the provisions contained in this Agreement and those contained in an Offer, SOW, or Services Description, the following order of precedence shall apply: (1) the Offer, (2) this Agreement, (3) the DPA, and (4) the SOW.

11. Definitions

11.1 "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 Great Place to Work Institute, Inc., 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.

11.2 "Applicable Law(s)" means any applicable provisions of all laws, codes, legislative acts, regulations, ordinances, administrative rules, rules of court, and court orders which govern a Party's respective business.

11.3. "Certification Period" means the 13month period beginning upon the date the Customer receives the designation as a Great Place To Work. The Certification Period does not automatically renew.

11.4 "Claim(s)" means any and all notices, charges, claims, proceedings, actions, causes of action and suits, brought by a third party.

11.5 "Customer Data" means all content, information, and data Customer inputs into the Subscription Services or collected by GPTW while providing Professional Services, including but not limited to Personal Data.

11.6 "Data Protection Laws" means (a) GDPR if Personal Data of European Union Data Subjects will be processed by GPTW, (b) FADP (Federal Act on Data Protection) if Personal Data of Swiss Data Subjects will be processed by GPTW and (c) any other Applicable Laws regarding protection of Personal Data.

11.7 "Offer" means an Offer agreed by both Parties, which is subject to this Agreement or otherwise references this Agreement, setting out, among other things, the type Subscription Services or Professional Services, the quantity of employees that may be surveyed using the Subscription Services, the term of the Offer, price and payment terms of the Services to be provided by GPTW, and the fees to be paid by Customer.

11.8 "Party" or "Parties" means GPTW or Customer, or both, as the context dictates.

11.9 "Personal Data" means "personal data" as defined under the GDPR and FADP; "personal information" as defined under the CCPA; and as similar terms, such as "personally identifiable information," are defined under other applicable Data Protection Laws.

11.10 "Professional Services" means the deployment, launch, configuration, implementation, integration, delivery, consulting, managed, and other similar services provided hereunder.

11.11 "Raw Data" means the responses received by GPTW from Customer's employees in connection with Trust Index Survey(s) and/or one-to-one interviews administered by GPTW to support the Subscription Services.

11.12 "Services" means the (a) Subscription Services; (b) Support Services; (c) Professional Services; and (d) other services or offerings as set forth in an Offer.

11.13 "Subscription Services" means those GPTW software-as-a-service ("SaaS") applications set forth in the Offer and made available to Customer via a hosted multi-tenant environment to use on a subscription basis.

11.14 "Support Services" means support and maintenance services provided by GPTW for the Subscription Services, as described in this Agreement.

Appendix 2: Data Processing Agreement (DPA) according to Article 28 GDPR and Article 9 FADP

Between Customer (Controller)

and

GPTW Switzerland AG, Schiffbaustrasse 7, 8005 Zürich, Switzerland (Processor)

§ 1 Subject matter and duration of the order

Details on the subject matter and duration of the order are set out in the assignment of GPTW Switzerland AG to conduct a survey of the Controller's employees. In case the controller only conducts a survey of the apprentices (Great Start! survey) or additionally to the employee survey conducts a survey of the apprentices (Great Start! apprentices survey) and/ or vocational and practical trainers (Great Start! trainer survey) the term "employees" also refers to "apprentices" and/or "vocational and practical trainers" hereinafter.

The Processor processes personal data on behalf of the Controller in the context of a Great Place To Work® survey within the meaning of Article 4 and Article 28 General Data Protection Regulation (GDPR) and Article 9 Federal Act on Data Protection (FADP) on the basis of this contract.

The contract begins with the access to Emprising™ and ends when the Emprising™ license expires.

Irrespective of the foregoing provisions regarding the terms of the contract, the obligations to maintain confidentiality, secrecy and agreed storage periods shall apply beyond the end of the contract.

§ 2 Nature and purpose of the processing, nature of personal data and categories of data subjects

The purpose of processing personal data is to conduct the employee survey on Emprising™. Emprising™ is a so-called "Software as a Service" (SaaS) solution. The tool consists of the survey platform (=Emprising™) and the customer portal. The latter is the administration portal and the portal where the Culture Brief™ and the Culture Audit™ are completed. The customer portal can be accessed via the link: login.greatplacetowork.com. The customer portal and the Emprising™ survey platform are technically linked. The Emprising™ web application is provided, maintained and further developed by the global umbrella organization - the Great Place to Work® Institute, Inc. based in Oakland, USA. Great Place to Work® Institute, Inc. acts as a sub-processor for GPTW Switzerland AG.

The survey on Emprising™ is conducted using business e-mail address and/ or codes. The employee data file (EDF) containing the data will be uploaded to Emprising™ by the customer.

Type of processing (Article 4(2) GDPR):

Collection, recording, organization, storage, consultation, comparison, anonymization and erasure of personal data uploaded in the Emprising™ platform within the framework of the employee survey.

Type of personal data (Article 4(1), Articles 13, 14 and 15 GDPR, as well as Articles 19(3) and 25 FADP):

For the **employee survey** with e-mail address: (business) e-mail address, IP address, Session ID (temporarily), user survey opened and completed date and time, survey languages chosen, browser user agent information for troubleshooting purposes.

For the **employee survey** with codes: same as for survey with e-mail address plus an individual code. The code letters contain access data for the website together with an individual access code for the survey.

In the survey (answering is voluntary):

- age group (25 years or younger 26-34 years, 35-44 years, 45-54 years, 55 years and older)
- gender group (female, male, another gender not listed)
- managerial level group (Employee/Individual Contributor (no people management responsibility); Frontline Manager or Supervisor (first tier manager; supervises other employees, not other managers), Mid-Level Manager (runs major departments or divisions, but not part of executive team); Executive/C-Level Leader (Highest level leaders; CEO/President and the C-suite executives who report to CEO)
- Tenure (less than 2 years, 2-5 years, 6-10 years, 11-15 years, 16-20 years, over 20 years)
- work status group (full-time, part-time)

There are 2 open- ended questions in the Swiss questionnaire

a) If you could change one thing about this company to make it a better place to work, what would it be?

b) Is there anything unique or unusual about this company that makes it a great place to work? Please give examples.

By default, responses to open-ended questions are forwarded to the client exactly as written by the survey participants, without removing names or other personal information, if added, that could identify individuals. GPTW Switzerland AG recommends to adding this information to the pre-survey communication to the employees.

For the **apprentices survey** Great Start! with e-mail address: (business) e-mail address, IP address, Session ID (temporarily), user survey opened and completed date and time, survey languages chosen, browser user agent information for troubleshooting

purposes.

For the **apprentices survey** Great Start! with codes: same as for survey with e-mail address plus an individual code. The code letters contain access data for the website together with an individual access code for the survey.

The apprentice survey will be set up as a separate pulse survey within the client's Emprising™ license.

In the survey (answering is voluntary):

- age group (Under 18 years of age, 18 - 21 years of age, older than 21 years of age)
- gender group (female, male, another gender not listed)
- year of apprenticeship group (First training year, Second training year, Third training year, Fourth training year)
- planned degree group (Federal vocational certificate (EBA), Swiss certificate of proficiency (EFZ), Swiss certificate of proficiency (EFZ) with vocational baccalaureate)

There are 2 open- ended questions in the Great Start! questionnaire:

a) What do you particularly like about your training company? Please give specific examples.

b) What would you change about your training company, if you could? Please give specific examples.

There is one pre-coded demographic in the apprentices list:

- Official training profession according to SERI (State Secretariat for Education, Research and Innovation)

By default, responses to open-ended questions are forwarded to the client exactly as written by the survey participants, without removing names or other personal information, if added, that could identify individuals. GPTW Switzerland AG recommends to adding this information to the pre-survey communication to the employees.

For the Great Start! **trainer survey**: (business) e-mail address, IP address, Session ID (temporarily), user survey opened and completed date and time, survey languages chosen, browser user agent information for troubleshooting purposes.

For the Great Start! **trainer survey** with codes: same as for survey with e-mail address plus an individual code. The code letters contain access data for the website together with an individual access code for the survey.

In the survey (answering is voluntary):

- age group (25 years or younger, 26-34 years, 35-44 years, 45-54 years, 55 years or older)
- gender group (female, male, another gender not listed)
- years of service ((less than 2 years, 2-5 years, 6-10 years, 11-15 years, 16-20 years,

over 20 years)
- education level (No school-leaving certificate, Compulsory school-leaving certificate (secondary level), Apprenticeship with Federal vocational certificate (EBA) or Swiss certificate of proficiency (EFZ), Apprenticeship with Swiss certificate of proficiency (EFZ) with vocational baccalaureate, Matura (Swiss baccalaureate) from a high school, Bachelor / higher college, Master, PhD)

There are 2 open- ended questions in the Great Start! questionnaire:

a) What do you particularly like about your role as a trainer? Please give specific examples.

b) What would you change about your role as a trainer if you could? Please give specific examples.

By default, responses to open-ended questions are forwarded to the client exactly as written by the survey participants, without removing names or other personal information, if added, that could identify individuals. GPTW Switzerland AG recommends to adding this information to the pre-survey communication to the employees.

Sensitive data/special categories of data (Article 9 GDPR/Article (5)(c) FADP):

No sensitive or special categories of data are included in the Swiss employee survey questionnaire.

No sensitive or special categories of data are included in the Great Start! apprentices survey and in the Great Start! trainer survey.

For clients conducting the employee survey **outside Switzerland** additional questions may need to be included in the questionnaire if the client wants to be certified in the respective country. Depending on the country the following questions (see table below) need to be included in the questionnaire answering these questions is, however, **voluntary and the questions will only be asked to employees who have an employment contract with one of the countries listed in the table.**

	Australia	Brazil	USA
What is your racial/ethnic identity?		x	x
Do you identify as LGBTQ+? (Lesbian, Gay, Bisexual, Transgender, Queer, +)		x	x
Do you have any chronic physical, mental, or emotional health problems, illnesses or other disabilities?		x	x
Do you identify as an Aboriginal and/or Torres Strait Islander person?	x		

Categories of persons concerned (Article 4(1) GDPR and Article 5 FADP):

Survey participants (employees of the Controller)

Recipients or categories of recipients to whom the data may be transferred:

Internal departments of GPTW Switzerland AG that are involved in achieving the purposes of data processing.

External entities engaged in contract data processing, as per Article 24 GDPR and Article 19 FADP, that meet security requirements under Article 32 GDPR and Articles 7 and 8 FADP and are commissioned by GPTW Switzerland AG. Examples include platform hosts for online surveys, scan service providers, IT service providers (maintenance and user support), and data disposal companies.

The Controller only receives survey evaluations in aggregated form ensuring no individual participants can be identified.

For this purpose, an evaluation threshold i.e. a minimum number of respondents is set, below which no results will be presented. The default evaluation threshold is defined as five responses or individuals. The evaluation (reporting) is based exclusively on de-identified data sets ("raw data") that do not contain any personal data.

This evaluation limit is also observed when different demographic or organizational characteristics are combined for an evaluation, e.g., the results for all men of a certain age group or for all managers in a certain organizational unit.

The Processor does not, as a matter of principle, provide any raw data to the Controller to carry out its own evaluations and thus potentially circumvent the specified evaluation threshold of at least five individuals.

Transfer of raw data to Great Place To Work Institute Inc.

Once a year the raw data from all organizations is fed into an aggregated database and made available to Great Place To Work Institute® Inc. (global umbrella organization in the USA) for benchmarking and the creation of supraregional lists. In this database, for each organization, only the company name and the aggregated responses of all participants to the 60 survey questions are displayed. Demographic data is only ever available as a group of data sets.

Standard periods for the deletion of data:

Personal data within the employee data (EDF) file will be deleted within five (5) working days after the survey ends, which means that personal data such as e-mail address or individual code is replaced with survey taker 1,2,3 etc. and thus it is not possible to trace individual answers anymore.

Some clients conduct a leadership feedback survey within Emprising™. In these cases, the report may be named after the respective manager (e.g. direct report Lara Croft). For the underlying survey data, the same rules as for all other reports apply: individual responses are deleted after 5 days, and results are only displayed to the client if at least 5 answers are provided. Result reports may be retained for potential comparison with future surveys; however, beyond the report name (e.g.

direct report Lara Croft), no personal data is stored. Such reports are only deleted upon the client's request.

§ 3 Responsibility of the Contracting Parties

The Processor is responsible for complying with the relevant data protection regulations within the framework of this contract, in particular those relating to the lawfulness of data processing.

In connection with the processing of personal data on behalf of the Controller, the Processor is also obliged to observe the data protection regulations applicable to him and to ensure that he and his employees comply with them.

Both contracting parties undertake to oblige their employees to maintain data secrecy, to sensitize them to the importance of the personal data processed and to instruct them about their obligations in connection with compliance with the relevant data protection regulations.

§ 4 Rights and Obligations of the Controller

The Controller shall be solely responsible for assessing the admissibility of processing in accordance with Article 4 No.7 GDPR and Article 6 FADP and for the selection of the rights of the data subjects in accordance with Articles 12 to 22 GDPR and Articles 25 to 29 FADP. Nevertheless, the Processor is obliged to forward all such enquiries to the Controller without delay, insofar as they are exclusively addressed to the Controller in a recognizable manner.

Changes to the object of processing and procedural changes shall be agreed between the Controller and the Processor and specified in a written or in a documented electronic format.

The Controller generally issues all orders, partial orders and instructions in writing or in a documented electronic format. Verbal instructions must be confirmed immediately in writing or in a documented electronic format.

Add-On 1 represents the standards for confidential participation of all survey participants/respondents (employees of the Controller). The Controller fully agrees with the listed standards.

The Controller shall be entitled to convince himself of the observance of the technical and organizational measures taken by the Processor and of the obligations stipulated in this contract, as stipulated under §5, prior to the commencement of processing and so on a regular basis and in an appropriate manner. Corresponding checks are generally carried out after prior notice and with a lead time of five working days. The Controller shall inform the Processor without delay if he finds errors or irregularities in the examination of the results of the contract.

The Controller is obliged to treat confidentially all knowledge of business secrets and data security measures of the Processor acquired within the framework of the contractual relationship. This obligation remains in effect even after termination of this contract.

§ 5 Duties of the Processor

The Processor shall process personal data exclusively within the framework of the agreements made and in accordance with the instructions of the Controller, unless he is obliged to do so by law of the Union or of the member states or the FADP to which the Processor is subject (e.g., investigations by prosecution or state protection authorities). In such a case, the Processor shall inform the person responsible of these legal requirements prior to processing, unless the law in question prohibits such notification on account of an important public interest (Article 28(3)(a) GDPR and Article 9 FADP).

The Processor shall not use the personal data provided for processing for any other purposes, in particular not for his own purposes. Copies or duplicates of personal data will not be made without the Controller's knowledge.

In the area of the processing of personal data in accordance with the order, the Processor assures the execution of all agreed measures in accordance with the contract. He assures that the data processed for the Controller will be strictly separated from other data sets.

In fulfilling the rights of the persons concerned in accordance with Articles 12 to 22 GDPR and Articles 25 to 29 FADP by the Controller, in drawing up lists of processing activities as well as in the event of necessary data protection impact assessments by the Controller, the Processor shall cooperate to the extent necessary and shall provide the Controller with appropriate support (Article 28(3)(e) and (f) GDPR).

The Processor will inform the Controller immediately if he believes that an instruction issued by the Controller violates legal regulations (Article 28(3) 3rd sentence GDPR). The Processor shall be entitled to suspend the execution of the corresponding notification until it has been confirmed or changed by the person responsible at the Controller after verification.

The Processor shall correct, delete or restrict the processing of personal data from the contractual relationship if the Controller requests this by means of an instruction and if this does not conflict with legitimate interests of the Processor.

The Processor may provide information about personal data from the contractual relationship with third parties or those affected by the contract only after prior instruction or approval by the Controller.

The Processor agrees that the Controller – in principle by appointment and with a lead time of five working days – is entitled to monitor compliance with the provisions on data protection and data security as well as the contractual agreements to the appropriate and necessary extent himself or by third parties commissioned by the Controller, in particular by obtaining information and inspecting the stored data and the data processing programs as well as by means of checks and local inspections (Article 28(3) 2nd sentence (h) GDPR). The Processor guarantees that he will cooperate, as far as necessary, in supporting these inspections.

The processing of personal data in private residences of employees of the Processor (e.g., via tele/mobile working or working from home) is permitted. Insofar as data is processed in a private residence, access to the employee's home for control purposes of the employer is guaranteed. Additionally, data privacy measures according to Article 32 GDPR and Articles 7 and 8 FADP are guaranteed.

The Processor confirms that he is aware of the relevant data privacy regulations according to GDPR and FADP applicable to processing of personal data. The Processor is obligated to maintain confidentiality in the processing of the Controller's personal data in accordance with the order. This obligation remains in effect even after termination of this contract.

The Processor guarantees that he will familiarize employees involved in carrying out the work with the relevant data protection provisions prior to commencement of the work and that he will commit them to secrecy in a suitable manner for the time of their work as well as after the termination of the employment relationship (Article 28(3) 2nd sentence (b) and Article 29 GDPR). The Processor monitors compliance with data protection regulations in his company. The Processor has appointed a Data Protection Officer (DPO) as representative in the EU according to Article 27 GDPR.

Daniel Schwaiger
isdacom GmbH
Forsbachstrasse 19
51145 Cologne
Germany
dsc@isdacom.de

The Processor must notify the Controller immediately in case of a change of the appointed DPO.

The Processor is obligated to inform the Controller without any delay about the exclusion of approved rules of conduct pursuant to Article 41 GDPR and the revocation of a certification pursuant to Article 42 GDPR.

§ 6 Notification obligations of the Processor in the event of processing disruptions and breaches of the protection of personal data

The Processor shall notify the Controller without delay of any disturbances, violations by the Processor or persons employed by him, as well as of data protection regulations or the stipulations made in the order, and of any suspicion of data protection violations or irregularities in the processing of personal data.

This shall also apply in particular with regard to any reporting and notification obligations on the part of the Controller pursuant to Articles 33 and 34 GDPR and Article 24 FADP. The Processor undertakes to provide the Controller with appropriate support, if necessary, for his obligations under Articles 33 and 34 GDPR (Article 28(3) 2nd sentence (f) GDPR) and Article 24 FADP.

The Processor may carry out notifications pursuant to Articles 33 and 34 GDPR and Article 24 FADP for the customer only in accordance with the instructions given in advance pursuant to § 5 of this contract.

§ 7 Sub-processing

The Processor shall be entitled to appoint third parties for the fulfilment of the contract, insofar as he informs the Controller immediately in writing and the Controller does not object to the use of the third party within a period of 30 working days.

The Processor must ensure that he carefully selects the sub-processor with particular regard to the suitability of the technical and organizational measures taken by the sub-processor within the meaning of Article 32 GDPR and Articles 7 and 8 FADP. The relevant test documents shall be made available to the Controller upon request.

The contractually agreed service is provided by the Processor and its sub-processors both in a member state of the European Union (EU) or in a signatory state of the Agreement on the European Economic Area (EEA, EU states plus Iceland, Liechtenstein, Switzerland, Norway) as well as additionally in the United States of America (USA). The Processor ensures the appropriate level of data protection by agreeing the standard contractual clauses in the processor-to-processor variant (with module 3) in accordance with Art. 46(2)(c) GDPR and Article 16 FADP.

A sub-processor may be engaged in third countries only if the special requirements of Articles 44 et seq. GDPR are fulfilled (e.g., adequacy decision by the European Commission, SCC, approved codes of conduct). Upon request, the Processor shall provide the Controller with evidence of the conclusion of the aforementioned agreements with its sub-processors.

The Processor shall ensure that the agreed provisions between the Controller and Processor shall also apply to all sub-processors. In the contract with the sub-processors, the details must be specified in such a way that the separate responsibilities of the Processor and the sub-processor are clearly defined.

If several sub-processors are used, this also applies to the responsibilities between these sub-processors. In particular, the Controller must be entitled to carry out appropriate checks and inspections, including on-site inspections, at sub-processors' premises or have them carried out by third parties commissioned by him.

The contract with the sub-processor(s) must be prepared in written form, which can also be done in an electronic format (Articles 28(4) and (9) GDPR). The forwarding of data to the sub-processor is permissible only if the sub-processor has fulfilled the obligations according to Articles 29 and 32 GDPR and Articles 7 and 8 FADP with regard to its employees.

The Processor shall verify compliance with the obligations of the sub-processor(s). The results of the tests shall be documented and made available to the Controller upon request. The Processor shall be liable vis-à-vis the Controller for ensuring that the sub-processor complies with the data protection obligations which have been

contractually imposed on him by the Processor in accordance with this section of the contract.

At present, the following sub-processors designated by name and contract content are engaged in the processing of personal data to the extent specified therein. The Controller agrees to their assignment:

Name of sub-processor	**Purpose of processing**	**Contact details**	**Legal basis for data transfer**
Great Place to Work® Institute, Inc.	Provision of the customer portal and the Emprising™ survey platform	Legal form: Company under American law. Registered office: 1999 Harrison Street, Suite 2070, Oakland CA 94612, USA Contact details: https://www.greatplacetowork.com Phone: +1 415 844 2500	SCC module 3 (processor-to-processor)
GPTW Switzerland AG ensures the appropriate level of data protection by agreeing the standard contractual clauses (SCC) in the processor-to-processor variant (with module 3) with Great Place To Work Institute Inc. in accordance with Article 46(2)c GDPR and Article 16 FADP. The SCC also contain the Swiss specific Add-ons regarding reference to Swiss data protection law, supervisory authority, terminology (member state also refers to Switzerland) and governing law and jurisdiction. Great Place to Work® Institute Inc. uses the following sub-processors:			
MICROSOFT AZURE	Cloud host in the EU data center (Netherlands) of customer data processed through Emprising™. OR Cloud host in the US data center Region East of customer data processed through Emprising™.	Legal form: Company under American law. Registered office: Microsoft Corporation, One Microsoft Way, Redmond, Washington 98052, USA Contact details: HR privacy askHR@microsoft.com Phone: (+1) 425 882 8080	SCC module 3 (processor to processor)
HTEC GROUP - High Tech Engineering Center d.o.o.	Maintenance of the Emprising™ software platform.	Legal form: Company under Serbian law. Registered office: Bulevar Milutina Milankovica 11B, 11000 Belgrade, Serbia Contact details: Aleksandar Cabrilo, President, aleksandar.cabrilo@htec.rs	SCC module 3 (processor-to-processor)

Microsoft 365	Provider of the Office 365 services.	Legal form: Company under American law. Registered office: Microsoft Corporation, One Microsoft Way, Redmond, Washington 98052, USA Contact details: HR privacy, askHR@microsoft.com Phone: (+1) 425 882 8080	SCC module 3 (processor to processor)
UKG, Inc. (GPTW's parent company)	Service for joint clients (if applicable), audit of GPTW's security controls, maintain back-end infrastructure that's used to support the services.	Legal form: Company under American law. Registered office: 900 Chelmsford Street, Lowell, MA 01851 Contact details: privacy@greatplacetowork.com	SCC module 3 (processor to processor)
Twilio	Provider of email delivery services.	Legal form: Company under American law. Registered office: 101 Spear Street, First Floor, San Francisco, CA 94105 Contact details: privacy@twilio.com	SCC module 3 (processor to processor)
MongoDB	Provider of database management and storage services.	Legal form: Company under American law. Registered office: 1633 Broadway, 38th Floor, New York, NY 10019 Contact details: privacy@mongodb.com	SCC module 3 (processor to processor)
MavenAGI	Provider of AI customer support services	Legal form: Company under American law. Registered office: 501 Boylston Street, Flr 9, Boston, MA 02116 Contact details: security@mavenagi.com	SCC module 3 (processor to processor)

Special case:

Normally the below listed sub-processors are not involved, as the employee data file (EDF) is handled and uploaded to Emprising™ by the customer. If required, GPTW Switzerland AG will support the customer in setting up the EDF. If the customer requires this support, the EDF will be uploaded by the customer to the Insight-tool (sub-module of the OneManyAny, which is an online-platform, provided by Trust Lab Limited). The server location of Trust Lab Limited is Poland. After the client has uploaded the EDF GPTW Switzerland AG can download the EDF from the Insight-tool

and save it on its own cloud (Synology) for editing. The server location of this Open Circle AG is in Switzerland.

The revised version of the EDF is made available to the customer again via upload to the Insight-tool and the client will then upload then by themselves to Emprising™ or the revised version is uploaded to Emprising™ by GPTW Switzerland AG for the customer.

If the above-described approach is applicable to the client the following sub-processors designated by name and contract content are engaged by GPTW Switzerland AG in the processing of personal data to the extent specified therein. The Controller agrees to their assignment:

Name of sub-processor	**Purpose of processing**	**Contact details**	**Legal basis for data transfer**
Trust Lab Limited	Exchange of the employee list (EDF) between the customer and GPTW Switzerland AG to support the customer in setting up the EDF Server location: Poland	Registered office: Trust Lab Limited, 235 Charlemont, Griffith Avenue, Dublin D09X4E0, Ireland Contact details: wojciech@thetrustlab.com jaroslaw@thetrustlab.com	Adequacy decision pursuant to FADP
Open Circle AG	System administration for GPTW Switzerland AG EDF downloaded from Insight tool will be stored on Synology (server managed by OpenCircle AG) Server location: Switzerland	Registered office: Freilagerstrasse 32, 8047 Zurich Contact details: support@open-circle.ch	FADP

Not to be understood as subcontracting relationships within the meaning of this regulation are those services provided by third parties which the Processor uses as ancillary services to support the fulfilment of the contract (e.g., telecommunications services). However, the Processor is obliged to take appropriate and legally compliant contractual agreements and control measures even in the case of outsourced ancillary services.

Storage location of data

The access for the controller in Emprising™ will be set up on the either on the EU-Server or the US-Server

For customers who conduct the survey with Emprising™ for the firsttime , access is always set up on the EU-server. Clients that did the first survey with Great Place To Work before January 1st 2024 were setup on the US-Server but have the option to move their data to the EU-Server before they do the follow-up survey.

The domain for the Emprising™ web application and access to the live dashboards for the US- server is app.emprising.com. The domain for the Emprising™ web application and access to the live dashboards for the EU-server is eu-appsurvey.emprising.com. The customer portal can be accessed via the link login.greatplacetowork.com. Access to the customer portal is managed via the authentication server (identity server) of Great Place to Work® Institute, Inc. which forms the basis for the distribution of roles and authorizations for the customer portal. There is no such secondary identity server in the EU data center. This means that when a new account is created for an administrator or for a manager who wants to access the survey results, an account is created on the identity server in the USA for the purpose of authentication, regardless of whether the customer account itself was set up on the EU or US server. As soon as a manager logs in via the identity server, they are forwarded to the relevant data center, which contains the survey results. The e-mail address is stored on the identity server in the USA.

The following table shows which personal data always flows via the US-Server, regardless of the server on which the customer access was set up.

Process step	**Customer-Portal /Emprising™**	**Storage Location**	**What is stored?**	**Purpose of storage**
Setup access for customer by GPTW Switzerland AG	Customer-Portal	US-Server Region East	e-mail address of the administrator	Setting up the survey by customers
Completion of Culture Brief™/ Culture Audit™ (by customer)	Customer-Portal	US-Server Region East	For customers who survey in multiple countries, the Culture Brief™ asks for the name and email address of the person who should be notified if the organization is recognized on one of the international lists. If the person completing the Culture Audit™ is another than the administrator, a login is also created for this person and the email address is stored.	Complete Culture Brief™ (relevant for certification) and Culture Audit™ (relevant for participation in the Best Workplaces list if organization has more than 250 employees)
Manager Access (Access is set up by the customer's administrator)	Customer-Portal	US-Server Region East	e-mail address of managers	Access to the results of the respective organizational unit
Certification-Badge and toolkit	Customer-Portal	US-Server Region East	e-mail address of the administrator	Access to the certification badge and tips & tricks for certification

The following table shows which personal data is stored in connection with the survey.

Process step	Customer-Portal /Emprising™	Storage Location	What is stored?	Purpose of storage
Prepa-ration of survey by customer	Emprising™	EU-Server if customer access was created on EU-Server Netherlands eu-appsurvey.emprising.com US-Server Region East, if customer access was created on US-Server app.EMPRISING.com/	E-mail addresses and access codes of employees that are uploaded to Emprising™ by the customer via the EDF	Sending invitations e-mails to employees to take part in the survey / The e-mail addresses/codes are optionally linked with information on the organizational affiliation, so that survey results can be evaluated on the basis of the linked organizational units
Survey period	Emprising™	EU-Server if customer access was created on EU-Server Netherlands eu-appsurvey.emprising.com US-Server Region East, if customer access was created on US-Server app.EMPRISING.com/	E-mail addresses and access codes of employees that are uploaded to Emprising™ by the customer via the EDF	Reminder e-mail to employees
Survey results: Presen-tation of the survey results as live dash-boards (incl. filters)	Emprising™	EU-Server if customer access was created on EU-Server Netherlands eu-appsurvey.emprising.com US-Server, if customer access was created on US-Server Region East app.EMPRISING.com/	Until 5 days after completion of the survey: E-mail addresses and access codes of employees uploaded to Emprising™ by the customer via the EDF	Ensuring the accuracy of the evaluation and the possibility of any corrections

§ 8 Technical and organizational measures - Article 32 GDPR (Article 28(3) 2nd sentence (c) GDPR) and Articles 7 and 8 FADP

A level of protection commensurate with the risk to the rights and freedoms of the natural persons concerned by the processing operation shall be ensured for the specific processing operation. To this end, the protection objectives of Article 32 (1) GDPR and Articles 7 and 8 FADP, such as confidentiality, integrity and availability of the systems and services as well as their resilience with regard to the type, scope, circumstances and purpose of processing, are taken into account in such a way that

the risk is permanently contained by appropriate technical and organizational remedial measures.

A risk assessment is carried out for the processing of personal data in accordance with instructions, taking into account the probability of occurrence and severity of the risks to rights and freedoms.

The data protection concept described in Add-On 2 specifies the selection of the technical and organizational measures in accordance with the determined risk, taking into account the protection objectives in accordance with state-of-the-art technology, in detail and in accordance with the current state of the art.

Decisions on the organization of data processing and the procedures used for security reasons are to be agreed between the Processor and the Controller. Insofar as the measures taken by the Processor do not meet the requirements of the Controller, he shall notify the Controller without delay.

The measures at the Processor's premises may be adapted to technical and organizational developments during the course of the contractual relationship, but may not fall below the agreed standards.

The Processor must agree on any substantial changes with the Controller in a documented form (written, electronic). Such reconciliations are to be kept for the duration of this contract.

§ 9 Obligations of the Processor after Contract Termination, Article 28(3) 2nd sentence (g) GDPR

After completion of the contractual work, the Processor shall delete or have destroyed all data, documents and processing or usage results that have come into his possession and to sub-processors in accordance with data protection regulations.

Agreements on technical and organizational measures as well as inspection and testing documents (including sub-processors) must be kept by both contract parties for the duration of their validity and subsequently for three full calendar years.

§ 10 Liability

Reference is made to Article 82 GDPR.

§ 11 Miscellaneous

Supplementary agreements generally require written form or a documented electronic format.

Should the property or the personal data of the Controller to be processed by the Processor be endangered by measures of third parties (e.g., by seizure or confiscation), by insolvency or composition proceedings or by other events, the Processor shall inform the Controller immediately.

§ 12 Severability clause

Should individually provisions of this contract be ineffective or unenforceable or become invalid or unenforceable after the contract has been concluded, this shall not affect the validity of the remaining parts of the contract.

The invalid or unenforceable provision shall be replaced by a valid and enforceable provision the effects of which come closest to the economic objective pursued by the contract parties with the invalid or unenforceable provision. The above provisions shall apply mutatis mutandis in the event that the contract proves to be incomplete.

§ 13 Governing law

This Agreement, and any dispute or claim (including non-contractual disputes or claims) arising out of or in connection with it or its subject matter or formation, shall be governed by, and construed in accordance with, the laws of Switzerland.

§ 14 Contact person in Switzerland for questions regarding data protection

GPTW Switzerland AG
Mrs. Ulrike Preissner
Schiffbaustrasse 7
8005 Zürich
Switzerland
CH_privacy@greatplacetowork.com

Attachments:

Add-On 1: Standards for confidential participation

Add-On 2: Technical and organizational measures of the Processor

Add-On 1:
Standards for confidential participation

Emprising™ is a dynamic tool for analyzing the results of the Great Place To Work® survey. Great Place To Work® does everything technically possible to ensure the confidentiality of survey participants/ respondents. However, these technical possibilities have their limits if users make mistakes when setting up the survey – and in particular when uploading the e-mail addresses or access codes of the potential survey participants/respondents, or if they do not observe the following standards.

#1 – The e-mail addresses are the only personal data in the employee list (EDF)

If the results are differentiated according to organizational units (e.g. locations, teams), no personal data such as first and last name, personnel number or similar may be uploaded within the employee list (EDF). The identification feature may only be the business e-mail address to which the invitation e-mail for questioning is sent, or an individual access code.

Reason: If names are uploaded with, the results can be filtered by name. This contradicts the promise of confidentiality.

#2 - Standards for designing access codes for the code letter survey

You can create random access codes in Emprising™, as an alternative to the use of e-mail addresses. Do not use attributes as access codes that are uniquely assigned to specific employees (e.g., personnel numbers or names) or are easy to guess (e.g. sequential numbers). The codes should be printed and distributed individually in sealed envelopes.

#3 - Avoid small organizational units as far as possible

Great Place To Work® recommends a minimum size of ten (10) employees per unit, so that you get statistically usable and at the same time confidential results. Emprising™ prevents columns containing uniquely identifiable information such as serial numbers or similar from being uploaded with the EDF.

Reason: The minimum number of participants for results to be displayed in Emprising™ is five (5). No group results will be displayed unless at least five people have responded. This applies to both demographic as well as organizational units. Therefore, if you want to capture your organizational structure in order to get more detailed results, it is essential to create sufficiently large units. In addition, organizational units and demographic data can be combined for evaluation (e.g. all women in Division A). It cannot be ruled out that the confidentiality of individual participants/respondents is no longer fully ensured when matching units just above the evaluation limit. This risk increases if many small units are included in the e-mail list.

Add-On 2:
Technical and organizational measures of the Processor

General

The following catalog of measures describes the individual technical and organizational measures taken in the context of commissioned processing in accordance with Article 24 (1) GDPR.

Confidentiality (Article 32(1)(b) GDPR)

Site Access control (Measures must be taken which are designed to prevent unauthorized persons from gaining access to data-processing facilities with which personal data is processed or used.)

Type of building

The building used by GPTW Switzerland AG is a multi-level building. On the lower floor there are offices which are used by various business tenants. The building also has a basement. The floors above the offices are occupied by private flats. GPTW Switzerland AG shares the sanitary facilities with the business tenants on the ground floor. The connecting door between the sanitary facilities and the offices of GPTW Switzerland AG is always closed. A key is required to re-enter the office from the sanitary facilities. The main entrance is secured by a safety lock and can therefore only be entered with the help of a key. To enter the office, visitors must ring the bell and are identified and admitted by the staff via an intercom system with camera.

Site access adequately secured

The identification of visitors by staff ensures that visitors must register and cannot enter the building without authorisation.

Entry Authorization

In the office, there is a separation of processing and public zones. Before closing time, the premises are checked to prevent unauthorised persons from being locked in the office.

Key regulations

All keys are recorded in a key register. The issue and return of keys are documented and receipted by a member of staff responsible for this. If a key is not returned by a staff member who has left, the locks will be changed promptly. The same applies if a key is lost.

Access-controlled zones

The server is locked in a special server cabinet. Appropriate internal measures ensure that only authorised persons have access to the server.

System Access controls (Measures must be taken to prevent data-processing systems from being used by unauthorized persons.)

System Access

Devices are secured against unauthorized use by entering a user ID and password.

Network and Servers

Each user has his or her own user ID plus a password, without which access to the network is not possible (RADIUS authentication). In addition, there are instructions to shut down the devices or personal computers after finishing work or when leaving the workplace, or to lock them against unauthorized use. The internal network is protected against unauthorized access from outside by means of a hardware and software firewall. Employees are instructed to store data exclusively on the server.

Passwords

There are instructions for secure passwords. Passwords are never displayed or stored unencrypted. In addition, passwords are stored in encrypted form, thus preventing access by unauthorized third parties. The default passwords of all relevant systems are explicitly disabled.

Multi-Factor-Authentication (MFA)

To secure access to critical systems and applications, the company uses two-factor authentication (2FA). In addition to a password, a second factor, which is a time-based one-time, is required for login.

Firewall

Both a hardware firewall and a software firewall are used. Hardware firewall updates are installed manually by the IT service provider, software firewall updates are installed automatically when they appear.

System administration

System administration is outsourced to Open Circle AG, Freilagerstrasse 32, 8047 Zurich as part of commissioned data processing in accordance with the requirements of Article 28, GDPR. The administrators have separate user accounts for system administration and processing.

Vulnerability management und penetration tests

The network & security solutions of Open Circle AG include state-of-the-art vulnerability management using the Wazuh Security and Vulnerability Detection Framework whereever applicable. The network & security solutions of Open Circle AG are regularly maintained and continuously updated (automatic update for the NAS once a week and for firewalls on a regular basis when new releases are available availability). Security Assessments like Penetration tests can be discussed and planned on request.

Access logging

Access logging is activated on the NAS/Synology drive, so you can see who is creating, reading, changing or deleting files. It is not possible to see which data within a file has been changed. However, this can be reconstructed via the backup (every 3 hours) if required. Access rights are assigned at user level.

Data Access control (It is necessary to take measures which are capable of ensuring that persons entitled to use a data-processing system are only able to access data covered by their access authorization and that personal data is not read, copied, modified, altered or removed without authorization during processing, use and storage.)

General protection

The organization protects itself against malware and unauthorized access from outside. This is done by means of anti-virus software, a hardware firewall and a software firewall. Updates of the hardware firewall are installed manually by the IT service provider, updates of the anti-virus software and the software firewall are installed automatically when they appear. State-of-the-art encryption procedures are used.

Data-processing system(s) (DP systems)

User IDs must be entered for the use of the DP systems with which personal data are collected, processed or used. These are set up by the IT service provider. In this regard, guidelines exist for the assignment of user IDs. This ensures that each user can only access those services that are needed to fulfil the tasks.

During the survey, only data is collected that is necessary for the purpose of processing (data minimisation) and that has been agreed upon with the person in charge in order to interfere as little as possible with the protection rights of the voluntary participants in surveys. A deletion concept (data avoidance) applies. Data is transmitted and stored in encrypted form in accordance with the state of the art.

Passwords

There are instructions for secure passwords. Passwords are never displayed or stored unencrypted. In addition, passwords are stored in encrypted form, thus preventing access by unauthorized third parties. The default passwords of all relevant systems are explicitly disabled.

Networks and servers

Each user has his or her own user ID plus a password, without which access to the network is not possible (RADIUS authentication). In addition, there are instructions to shut down the devices or personal computers after finishing work or when leaving the workplace, or to lock them against unauthorized use. The internal network is protected against unauthorized access from outside by means of a hardware and software firewall. Employees are instructed to store data exclusively on the server.

Fault diagnosis/remote maintenance

Security measures are taken for fault diagnosis, maintenance and remote maintenance so that it is recognizable who has accessed what and when.

Access via remote maintenance is only carried out by company computers that have the same security standard as local, company PCs.

Paper documents

The principle of the "clean desk" and the empty screen is practised so that neither personal information in paper form nor information stored on data carriers remains on employees' desks for a longer period of time.

Separation requirement (Measures are to be taken to ensure that data collected for different purposes can be processed separately.)

Data bases

GPTW Switzerland AG does not maintain data bases containing personal data. Existing data bases only contain raw data from different clients.

Integrity (Article 32(1)(b) GDPR)

Controls on transfer (Measures must be taken to ensure that personal data cannot be read, copied, altered or removed without authorization electronically during electronic transmission or during its transport or storage on data carriers, and that it can be reviewed and determined which persons are intended to transmit personal data by means of data transmission facilities.)

Type of data transmission

Data is sent/data is transmitted by letter post, e-mail, telephone, Internet, Voice over IP (VoIP), sFTP and https. As a matter of principle, state-of-the-art encryption procedures are used during transmission.

Data security

Data manipulation by malware is prevented by means of anti-virus software.

Disposal and destruction of data carriers

Data (carriers) to be destroyed are transported to the disposal company in sealed containers. The disposal company has been carefully selected and committed in writing to Article 28 GDPR. Data carriers are disposed of in accordance with data protection regulations.

E-mail

No e-mail servers are used that can be reached unencrypted via the Internet, as otherwise the passwords for SMTP and/or POP3 could be intercepted.

Mobile device and mobile data carriers

Notebooks and smartphones are used. The notebooks as such and the respective operating systems are fully encrypted.

WiFi

There is in-house WiFi access. WiFi accesses are protected according to the state of the art (WPA2). The default password for the configuration of the access point/router has been changed. A physically separate WiFi is also available for guests and external staff.

Remote Maintenance

Remote maintenance is carried out by the external IT service provider and the access to personal data is not excluded. The remote maintenance includes both the installed software applications and the user administration along with the helpdesk. Access is controlled by user ID and password. The transmission path is secured by SSL encryption. The remote maintenance is logged.

Remote maintenance is carried out exclusively via computers that have the same security standard as the local company computers.

Procedures for regular review, assessment and evaluation (Article 32(1)(d) GDPR; Article 25(1) GDPR)

Verification/inspection of mandate compliance (Measures are to be taken which are capable of ensuring that personal data processed by contract can only be processed in accordance with the instructions of the Controller.)

Review of the Sub-processor

Sub-processors are carefully selected with particular regard to Article 28 GDPR and thus the suitability of the technical and organizational measures taken by them. Orders are always placed in writing.

The data protection responsible of GPTW Switzerland AG is involved in all contracts as well as in the verification of the proper implementation of the commissioned processing. In this context, the client is aware of the declaration of commitment to confidentiality and disclosure in the context of the processing of personal data (in accordance with Article 28(3) (b) GDPR).

Contractual content

Each data processing contract shall be concluded in writing. The technical and organizational measures to be taken by the sub-processors are part of the agreement. The competences and obligations between the client and the sub-processor are also clearly delineated.

Availability and resilience (Article 32(1)(b) GDPR), as well as availability control and rapid recoverability (Article 32(1)(c) GDPR)

Availability control (Measures are to be taken which are capable of ensuring that personal data is protected against accidental destruction or loss.)

Emergency concept

If a malfunction occurs, the employee who detects the malfunction immediately reports it to the IT service provider, who immediately remedies the weak point. In mutual agreement, system analyses are carried out by IT.

Data backup

Responsibilities for central data backup are regulated. The backup is done automatically and is thus de facto enforced; in the event of an error, the IT service provider is informed immediately via monitoring service. The backups are stored at a safe distance, protected from access and encrypted ("spatial and logical separation"). The data can be restored quickly even if backup readers fail. The server hard disks are mirrored in a RAID system. The central and uniform procurement of hardware and software is regulated.

Virus protection

Virus protection programs are used. The virus protection programmes are updated automatically when they appear or several times a day. As an additional protective measure, SPAM filters are used for e-mail traffic.

Fire protection of the PC workrooms

There is a strict ban on smoking in the offices. In addition, fire extinguishers are located in the PC workrooms.

Incident Response and obligation to report breaches

The company has implemented an incident response process that includes the protection, detection, recovering, documentation, internal reporting, and timely notification of personal data breaches in accordance with applicable legal requirements, such as the 72-hour notification period under the GDPR.

Appendix 3: General Terms and Conditions

Status September 2025

Scope

These general terms and conditions apply to all contractual relationships between the customer and GPTW Switzerland AG. With the commissioning of GPTW Switzerland AG, they become an integral part of the contractual relationship between the customer and GPTW Switzerland AG.

Deviating or additional contractual, delivery, or purchasing conditions of the customer do not become part of this contractual relationship. Something else shall only apply if the inclusion of the deviating or additional conditions is expressly agreed in writing.

Execution of the contract

GPTW Switzerland AG shall perform the agreed services to the best of its ability and on the basis of the methodological principles developed by GPTW. It is agreed between the contracting parties that GPTW Switzerland AG does not guarantee the achievement of specific results, outcomes, rankings, business objectives, or other successes.

Rights of use

The contractual brands, titles, logos, and methods are the intellectual property of Great Place To Work Institute Inc. (global umbrella organization) and/or GPTW Switzerland AG as its licensee. All industrial property rights thereto, in particular trademark and/or copyright usage rights, shall remain with Great Place To Work Institute Inc. and/or GPTW Switzerland AG. The customer is not entitled to use, reproduce, distribute, edit, and/or redesign these rights for himself or to transfer any rights or authority to third parties.

Certification and Award

The certifications will be granted by GPTW Switzerland AG in accordance with the current competition conditions integrated in the offer (Terms & Conditions for Great Place To Work® Certification™ and Best Workplaces™ List). There is no legal entitlement to certification.

The customer undertakes to comply with the competition conditions. Any violation of the terms and conditions that results in not all employees being fairly reflected in the results, that encourages positive rather than open responses, or that results in employees feeling that the confidentiality of their data has been compromised may result in disqualification.

In the event of indications of a violation of the competition conditions GPTW Switzerland AG reserves the right to carry out random samples at the client in order to verify the facts.
In addition, in the event of violations of the competition conditions, certifications

already issued by GPTW Switzerland AG may be declared invalid, which also means that the use of the certification badge provided is no longer permitted.

GPTW Switzerland AG may use the information collected as part of the Culture Audit™ or training concept in anonymous form (i.e. without mentioning the organization name and without using the logo).

Prices and payment

Subject to other offers, all prices are quoted in Swiss francs (CHF). All prices are exclusive of any applicable value added tax (VAT).

Usually, services are invoiced at the start of the survey or at the start of the service provided.

Invoices will be issued exclusively to contractual partners with registered office and invoice address in Switzerland or Liechtenstein. The services shall be invoiced exclusively to a single invoice recipient and the invoice shall not be divided among several invoice recipients. Exceptions must be agreed upon prior to the conclusion of the contract and the additional expenses for this will be charged to the customer. As a matter of principle, GPTW Switzerland AG reserves the right to charge the customer for extraordinary effort in invoicing (e.g. due to late payments).

GPTW Switzerland AG shall provide the customer with all documents necessary for the provision of the service. Should the client require GPTW Switzerland AG to consider amending the Master Service Agreement (MSA), reviewing a different client agreement, completing a risk assessment questionnaire or reviewing a client specific data processing agreement, the client agrees to be billed for costs on a time and material basis. GPTW Switzerland AG will notify the client of the applicable fees prior to completing any work.

Confidentiality and data protection

The parties undertake to comply with data protection regulations and to maintain confidentiality. Supplementary and overriding provisions on data protection, secrecy, and confidentiality, are set out in the Master Service Agreement (MSA) concluded between the parties, which is attached as an appendix to the respective offer.

Final provision

Unless otherwise specified in the Master Service Agreement (MSA), the place of performance and exclusive place of jurisdiction for disputes is the registered office of GPTW Switzerland AG. The legal relationship between the contracting parties shall be governed exclusively by Swiss law. If a Master Service Agreement (MSA) exists between the parties, its provisions regarding applicable law and jurisdiction shall take precedence over these General Terms and Conditions.

Appendix 4: Terms & Conditions for Great Place To Work® Certification™ and Best Workplaces™ List

All Great Place To Work® Assessment packages (Analyze, Accelerate) are non-refundable and have a one-year term from the initial purchase date in which to utilize all included components, including survey(s), report packages, online data analytics and manager access.

1. Certification Eligibility Requirements

Each Certification eligible Assessment package (Analyze, Accelerate) includes one(1) Certification attempt. To participate in Certification, Company must:

1.1 Have 10 or more country-based full-and/or part-time employees (do not include per diem, temporary or contract employees).

1.2 Ensure that the survey is accessible online to all employees.

1.3 Administer a Certification-eligible Trust Index™ Survey to all employees if total country-based employee count is 5,000 or fewer. If Company has more than 5,000 country-based employees, depending on the details of the package ordered (i.e., Assess, Analyze or Accelerate), Company must, at a minimum, survey 5,000 employees (generated as a random sample from the entire country's employee population) or may contract to conduct a full census.

1.4 Receive enough Trust Index Survey responses to meet or exceed the current Certification threshold with less than 10.5% margin of error at a 90%confidence level in the results.

1.5 Submit a culture assessment that reflects employee demographics and company programs at the time of distributing the survey.

1.6 The Certification-eligible Trust Index Survey and culture assessment must reflect the entire entity within the country, including the parent, all subsidiaries, divisions, and departments in that country. Company can only be awarded Certification independently of their parent organization and related subsidiaries if Company can show, prior to initial purchase, that they operate as a distinct and separate business, brand, and culture.

2. Certification, Profiles, and Best Workplaces Lists Consideration

2.1 Once Company has completed all the required steps, should the average of all Great Place To Work® Model© statements meets the Certification threshold, Company will be awarded the designation as Great Place To Work®-Certified™ and a Great Place To Work® Profile™ will be published, as applicable. Any Company that appears on a Great Place To Work® Best Workplaces™ List is selected primarily based on their employees' responses to the Great Place To Work Trust Index Survey which is a proprietary employee survey developed by Great Place To Work. The specific criteria and methodology for each Best Workplaces List is managed by and at the discretion of Great Place To Work and is subject to change.

2.2 Certification is valid for 13 months from the date awarded ("Certification period"). Companies awarded Certification can use the country-specific Certification badge, royalty free, during the Certification Period according to the guidelines found here: Certification Badge Usage Guideline https://www.greatplacetowork.com/certification-brand-guide

2.3 Company will be then considered for all Best Workplaces Lists that they are eligible for during the Certification Period. To be considered for Great Place To Work Best Workplaces Lists, the rules are as follows:

2.3.1 Enough survey responses must be received by Company to meet or exceed the Best Workplaces List threshold of less than a 5.5% margin of error at a 95% confidence level in the results.

2.3.2 Company must be Great Place To Work-Certified at the time of any deadline for any Best Workplaces List and meet specific criteria. Deadlines and criteria are subject to change.

2.3.3 Company must have a published Great Place To Work Profile. The Great Place To Work Profile is published online by Great Place To Work and may highlight Company facts and high-level positive results from the survey.

2.3.4 Companies selected for a Best Workplaces List can use the country-specific List badge according to the guidelines found here: https://www.greatplacetowork.com/national-list-badge-guide

3. Integrity of Our Selection Process

Great Place To Work will not consider personal relationships, gifts, or any other influences (or attempted influences) in the selection of Company for Certification and/or a Best Workplaces List. Engaging Great Place To Work® for services (e.g., Consulting) does not help Company obtain Certification or appear on a Best Workplaces List. Evaluators involved in the selection of Company for a Best Workplaces List sign non-disclosure agreements and are screened for potential conflicts of interest.

4. Confidentiality: Data, Materials, and other Company Information

4.1 Great Place To Work will only provide Company data to approved media and research "partners" who have been authorized in advance by written agreements with Great Place To Work for purposes of developing and publishing a list and/or related findings. This data may include selected data points gathered in the culture assessment, specific Trust Index Survey results and employee comments.

4.2 Great Place To Work may use aggregate data to publish reports, articles, research, or books in addition to Best Workplaces Lists and Great Place To Work Profiles.

4.3 Great Place To Work may cite examples of Company's best practices in presentations and speeches, media interviews, articles, and other communications, but only in accordance with the Positive Recognition Guidelines.

4.4 This Agreement does not apply to any information of Company that (a) is or becomes available in the public domain; (b) becomes available to Great Place To Work on a non-confidential basis from a third party or (c) is consented to disclosure by Company.

5. Positive Recognition Guidelines

5.1 Positive Recognition will be provided to Company named in publicity and findings distributed by Great Place To Work and its media partners. Company will not be negatively critiqued for its efforts, policies, programs, or practices.

5.2 Great Place To Work may publish findings on Company without prior approval from Company, provided this use is in accordance with these Positive Recognition Guidelines.

5.3 Company irrevocably authorizes and grants to Great Place To Work® Institute, Inc. the right to use the data, information and other material it and its representatives provide (collectively, the "Material") as part of the Great Place To Work Certification & Great Place To Work Best Workplaces Lists Terms, at its discretion for purposes of developing and publishing Best Workplaces Lists or related findings. This Material may include selected data points gathered in the culture submission, specific Trust Index© Survey results and employee comments. Company waives any inspection or approval of any such Material or the use thereof and it acknowledges and agrees that this Consent includes the right of Great Place To Work to copy, cut, crop, edit, revise, alter, adapt, modify or otherwise change and use the Material, in whole or in part, without any further approval by or consideration. Company waives any legal claim to any compensation or receipt of consideration of any kind for the rights granted by this Consent.

5.4 Company consents to the publication of the Great Place To Work Profile created by Great Place To Work, as applicable, including the publication of any information, any Company logos or trademarks, or any photographs or graphics, that have been submitted to Great Place To Work by Company or its employees in order for Great Place To Work to evaluate Company or prepare a Great Place To Work Profile. From time to time, Great Place To Work may enter into agreements with third parties for publication of the Great Place To Work Profile in print and other forms of media, and Company agrees that it has no objections to such third parties printing Company's Great Place To Work Profile.

6. Suspension

If Company is in breach of this Supplement, Great Place To Work may suspend the eligibility immediately if it reasonably deems that Company's breach may put the GPTW Intellectual Property at risk. Great Place To Work will promptly communicate with Company to assess if Company may remedy such breach and if such breach is not remedies within thirty (30) days, Great Place to Work may terminate the eligibility of the Company.

Appendix 5: Privacy Policy for participants taking part in the Great Place To Work® employee survey

We generally market and sell our Product to businesses, not consumers. Our commitments regarding the personal information we collect, use, and disclose about the end users of the Product are largely driven by our contracts with business customers. The information provided below is intended to help our business customers understand our privacy practices. If you are an end user of one of our products or services, you are encouraged to contact your employer with questions about how your personal information is being collected, used, and disclosed.

Information We Collect

In most instances, GPTW customers are the controllers of the personal information they collect, create, communicate, and store in our Product. The types of personal information that can be stored in our Product are listed in the Data Processing Agreement (DPA). Data subjects will find comprehensive information about which data is collected and how it is processed on the Great Place To Work website of Switzerland.

Use of Information We Collect

When we act as a processor, the personal information we collect is used to deliver our products and services to Customers. Any personal information we use is done in accordance with our contracts with our Customers.

Because our business Customers are data controllers, it is primarily them who must undertake efforts regarding how information is collected and processed in accordance with data-protection laws. Therefore, if you have questions or concerns about the processing of your information as an end user, you should contact your employer directly or refer to its separate privacy policies.

GPTW does not give anyone access to the personal information maintained in the Product unless:

- It is permitted to do so in its contract with the Customer.
- The Customer instructs GPTW to do so;
- The Customer consents (e.g., subprocessors used by GPTW);
- If GPTW is legally obligated to do so; or
- If GPTW has a legitimate interest (as defined under GDPR, FADP and other applicable laws) to do so.

Data Retention

GPTW will only retain personal information for the length of time necessary to fulfill the purpose(s) for which the information was collected or as required or permitted by applicable laws, (including the resolution of disputes) and in accordance with our Customer contracts.

To determine the appropriate retention period for personal information, we consider the amount, nature, and sensitivity of the personal information, the potential risk of harm from unauthorized use or disclosure of the personal information, the purposes for which we process your personal information, and whether we can achieve those purposes through other means, and the applicable legal requirements.

When we no longer require your personal information, we will either delete or deidentify it or, if this is not possible, we will securely store it in accordance with this policy and cease use of the personal information until deletion is possible. If we deidentify your personal information (so that it is no longer associated with you), we may retain this information for longer periods. To support our research and enable historical comparisons, we retain deidentified data indefinitely.

Disclosure of Personal Information

We do not sell your personal information to third parties. We may, however, share your information with:

- **Affiliates, Licensees, and Subsidiaries:** We might share personal information with our affiliates, licensees, and subsidiaries in order to deliver a product or service or to complete a task requested by our customer.

- **Third Party Suppliers or Service Providers:** We might engage with third parties (suppliers and/or service providers) in order to deliver a product or service, perform certain functions such as enhancing the Product, or complete a task requested by our customer.

We have contracts with our Third-Party Suppliers or Service Providers to perform certain functions on our behalf, and only at our direction. Our third parties are bound by confidentiality agreements, only have access to personal information to the extent necessary to provide these contracted services, and are only permitted to process personal information in accordance with our instructions (and for the purposes we disclose).

In addition, GPTW might disclose personal information if we in good faith believe that it is necessary:

- To comply with the law or with a legal process;
- To protect or defend our rights and property;
- To protect against misuse or unauthorized use of our website;
- To protect the personal safety or property of our users or the public (among other things, this means that, if you provide false information or attempt to pose as someone else, information about you may be disclosed as part of any investigation into your actions);and
- In connection with, or during negotiations for, an acquisition, merger, asset sale, or other similar business transfer that involves all or substantially all of our assets or

functions where personal information is transferred or shared as part of the business assets (provided that such party agrees to use or disclose of personal information consistent with our Privacy & Security Notice or gains your consent for other uses of disclosures).

We will not cross-reference your personal information with that of any other customer or entity. GPTW does not support "back door" access to any of its products, services, or operations (including our data stores) by any government or third party. GPTW does not share its encryption keys or provide the ability to break our encryption keys with any government or third party.