LEADERSHIP
CIRCLE®

TERMS AND CONDITIONS

These **TERMS AND CONDITIONS** shall govern the Agreement for Services and Statement of Work (the "**Agreement**") between **Company** and **Client** and are incorporated into the Agreement by reference. Company and Client are each hereafter referred to individually as a "**Party**" and together as the "**Parties**." Capitalized terms not defined herein shall, unless otherwise indicated herein, have the meanings ascribed to such terms in the Agreement.

For the avoidance of doubt, any Statement of Work ("SOW") accepted by Client before the Effective Date of the Agreement shall continue to be governed by the previous agreement between the Parties that governed the SOW on the SOW's effective date. All future SOWs shall be governed by this Agreement.

1. Services and Affiliate Participation

1.1. Services: Company shall provide the Services (as defined herein) on a project basis. The specific services and/or goods for any given project (the "**Services**") shall be set forth on one or more mutually agreed upon SOWs. Each SOW will include (1) a description of the Services to be provided, (2) whenever possible, clear milestones and deliverables, and (3) whenever applicable, a billing schedule in which invoices are linked to milestones and deliverables. Each SOW shall be deemed to be incorporated into this Agreement by this reference and governed by the terms herein. If any provision in a SOW conflicts with this Agreement, the terms of this Agreement shall prevail. Notwithstanding the foregoing, the Parties may agree to modify the terms and conditions of this Agreement with respect to a given SOW by setting forth such modifications in a SOW under a section entitled "Modifications to Agreement Terms and Conditions."

1.2. Affiliates: This Agreement shall apply to any wholly owned subsidiary of Client or Company and may apply to any other affiliate as agreed to in writing.

2. Compensation

2.1. Compensation for Services:

(a) Client will pay Company within thirty (30) days of receiving an invoice from Company unless otherwise agreed to in an applicable SOW. All amounts set forth in each Statement of Work are exclusive of applicable taxes and Client shall be responsible for payment of applicable taxes, duties or charges imposed by any governmental entity for Services provided under this Contract. The Parties agree to cooperate with each other to enable each to more accurately determine its own tax liability and to minimize such liability to the extent legally permissible.

(b) Client will reimburse Company for travel and other out-of-pocket expenses reasonably and properly incurred by Company and authorized by Client ("Reimbursable Expenses").

2.2. Terms of Invoicing and Payment: Unless specifically stated otherwise in any applicable SOW, all invoices will quote the reference to this Agreement and payments will be sent from Client to Company at the following address:

132 East 14075 South Suite 400
Draper, Utah 84020
USA

3. Confidentiality

3.1. Definitions:

(a) "**Client Confidential Information**" means any information (i) disclosed by or on behalf of Client or its affiliates to Company, either in writing or orally, or (ii) about Client or its affiliates and obtained by Company from a third party under an obligation not to disclose such information, or (iii) created by Company or Client or its Affiliates, or (iv) observed by Company on the premises of Client or its Affiliate(s), in each case, in connection with this Agreement.

(b) "**Company Confidential Information**" means all non-public financial or business information that is disclosed by Company to Client, either in writing or orally, provided such information is (i) directly related to the Services performed by Company, and (ii) necessary for Client to obtain the benefit of the Services, and (iii) designated as confidential or that reasonably should be understood to be confidential given the nature of the information and the circumstances of disclosure. Together Client Confidential Information and Company Confidential Information shall be referred to as "**Confidential Information**." "*Leader Confidential Information*" is a subset of Company Confidential Information and means any information (i) disclosed by or in evaluation of an employee or representative of Client or its affiliates, either in writing or orally, and (ii) is about the individual's leadership style, strengths, etc., and (iii) that is entered into Company's Project Center (the online tool through which information relating to an individual's leadership strengths and styles are collected and then turned into a report) or is created by Project Center unless it has been anonymized and de-identified. Anonymized or aggregated information that is provided to Client in the form of a report is not included in Leader Confidential Information and is work product belonging to Client.

3.2. Exclusions: Confidential Information does not include information that: (i) was already in the possession of a Party before the Party obtained such information in connection with this Agreement, as evidenced by the Party's written records, (ii) is independently developed by a Party without reference to any information of the other Party, as evidenced by such Party's written records, (iii) is or becomes publicly available through no fault of a Party, or (iv) is obtained by a Party from a third party not bound by any obligation not to use or disclose such information.

3.3. Obligations: Each Party shall take precautions, to secure and protect the Confidential Information of the other Party from unauthorized use or disclosure, that are at least as stringent as those observed by Company to protect its own proprietary and valuable technologies and materials, but in any event no less than reasonable precautions. Each Party agrees not to use Confidential Information of the other Party for any purpose except (i) Company may use Client Confidential Information as necessary to perform the Services and (ii) Client and its affiliates, contractors, and collaborators may use Company Confidential Information as necessary to fully exploit any inventions or work product or the Services. Each Party agrees not to disclose to any third party any Confidential Information of the other Party without such Party's prior written consent, except as set forth in the following two cases: (a) each Party may disclose Confidential Information of the other Party to the extent required under applicable law or regulation, provided the disclosing Party uses reasonable efforts to provide the other Party with reasonable advance notice of the disclosure and the opportunity to object, narrow, or limit the disclosure, and (b) Client may disclose Confidential Information of Company to its affiliates, contractors and collaborators in furtherance of the rights granted hereunder. The Parties' obligations under this section shall survive for a period of two (2) years after the termination or expiration of this Agreement.

3.4. Publicity and Publications: Company may use the name, logo, or trademark of Client or a Client affiliate and may refer to Client or a Client affiliate without approval of Client in Company's publications, advertisements, marketing materials, or as Company otherwise deems necessary. Client agrees that Company may use its name, logo, or trademark for this limited purpose and Company shall not be required to make a payment of any kind.

3.5. Data Protection: The Parties agree to the Data Protection requirements set forth in the Data Processing Agreement attached as Exhibit A to these Terms and Conditions.

3.6 Data Control and Basis of Processing: Under this Agreement, some data will be controlled by Company and some will be controlled by Client. Any personal data entered into Company's Project Center, even if the individual is employed or contracted by Client, is controlled by Company and is processed based on that individual's, not the Client's, consent. Any information entered into Project Center by evaluators invited by those individuals to evaluate those individuals' leadership is also controlled by Company. Any other data collected directly from individuals using Project Center is controlled by Company. Any data provided to Company directly by Client such as names, titles, and email addresses of Client's employees or contractors is controlled by Client and processed based on this Agreement. Client does not have the capacity to order the change, correction, deletion, or change of processing of any data received through Project Center and may not access individual leadership evaluations or reports created by or submitted to Project Center or Certified Practitioners in regard to Client's employees or contractors. Client may only receive copies of those reports if the individual who is the data subject discloses those reports to Client directly. That Company remains the controller of the Project Center data is essential to the provision of the Services so that it can guarantee evaluators and the evaluated individuals that the feedback will be kept confidential. Any aggregated data, report, or other work product provided directly to Client is controlled by Client.

4. Intellectual Property

The following shall be owned by the Company: all intellectual property rights—including without limitation copyrights, patents, patent disclosures and inventions (whether patentable or not), trademarks, service marks, trade secrets, know-how and other confidential information, trade dress, trade names, logos, corporate names, and domain names—together with all of the goodwill associated therewith, derivative works, and all other rights (collectively, "Intellectual Property Rights") in and to all documents, work product, and other materials that are delivered to Client under this Agreement or prepared by or on behalf of Company in the course of performing the Services, including any items identified as such in any Statement of Work (collectively, the "Deliverables"), except for any Client Confidential Information or Client-owned materials. Company hereby grants Client a license to use all Intellectual Property Rights in the Deliverables free of additional charge and on a non-exclusive, worldwide, non-transferable, non-sublicensable, fully paid-up, royalty-free, and perpetual basis to the extent necessary to enable Client to make reasonable use of the Deliverables and the Services.

Notwithstanding the foregoing, nothing in this Agreement shall grant Client the right to sell, reproduce, sub-license, transfer, or otherwise distribute the Intellectual Property Rights to any third party. Client and Company may identify any Deliverables or any other materials listed on any Statement of Work which will be owned exclusively by Client, but must do so in writing on the Statement of Work prior to the development or creation of such materials. Nothing in this Agreement shall grant Client an ownership right in the Intellectual Property Rights and Client hereby acknowledges and agrees that it shall not reverse engineer, decompile, or disassemble any Intellectual Property Rights or otherwise attempt to determine the source code for computer programs or other trade secrets that constitute Intellectual Property Rights.

Because of the difficulty of valuing Intellectual Property Rights, failure to abide by the terms of this part 4 of the Agreement shall entitle the non-breaching Party to immediately seek and obtain injunctive relief under the laws, jurisdiction and venue provisions set forth in part 9.6 of this Agreement. The non-breaching Party shall be entitled to seek any other legal or equitable relief available to that Party.

5. Representations and Warranties

5.1. Each of Company and Client hereby represents and warrants that, during the term of this Agreement:

(a) Company and Client shall comply with any applicable laws in connection with the performance of the Services, and each shall have all rights, licenses, permits and consents necessary to perform the Services.

(b) Company shall perform and complete the Services in accordance with the terms and subject to the conditions set out in the respective Statement of Work and this Agreement.

(c) Company shall perform Services in a timely, workmanlike, and professional manner in accordance with generally recognized industry standards for similar services.

5.2. EXCEPT FOR THE REPRESENTATIONS AND WARRANTIES EXPRESSLY PROVIDED FOR IN THIS AGREEMENT OR IN A STATEMENT OF WORK, THE PARTIES EXPRESSLY DISCLAIM ALL OTHER REPRESENTATIONS AND WARRANTIES, WHETHER EXPRESS OR IMPLIED, ORAL OR WRITTEN, STATUTORY OR OTHERWISE, INCLUDING, BUT NOT LIMITED TO, ANY WARRANTIES OF

MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND THOSE ARISING BY STATUTE OR FROM A COURSE OF DEALING, USAGE, TRADE, PRACTICE OR CUSTOM.

6. Term and Termination

6.1. Term: The initial term of this Agreement shall be for **one** (**1**) **year** commencing on the Effective Date. After the initial term, the Agreement shall renew automatically for subsequent twelve (12) month periods, even in the absence of a SOW, unless notice of termination is provided to the other Party in accordance with this Section.

6.2. Termination for Convenience: Either Party may terminate this Agreement for any reason upon thirty (30) days prior notice, provided that such termination by Company shall not be effective until completion of all Services. If Client elects to cancel this Agreement for any reason other than in such case where Company is in material breach as outlined in Section 6.3, the matrix for Cancellation Convenience Fee in the applicable SOW will be applied.

6.3 Termination for Material Breach: Either Party may terminate this Agreement for any material breach of this Agreement by the other Party, if such breach is not cured within thirty (30) days after the non-breaching Party delivers written notice of such breach to the breaching Party.

6.4. Termination for Bankruptcy: Either Party may terminate this Agreement upon prior notice in the event the other Party makes a general assignment for the benefit of its creditors, a petition in bankruptcy is filed by or against such other Party, or a receiver is appointed on account of such other Party's insolvency.

6.5. Effect of Termination:

(a) Upon any termination of this Agreement, Client's obligations to Company shall be to pay Company for Services performed prior to the date of termination, in addition to any applicable Cancellation Convenience Fee in accordance with the applicable SOW.

(b) Upon termination notice for this Agreement, Company's obligations shall be to (i) provide the Services to Client until the date of such termination (except to the extent otherwise instructed in writing by Client), and (ii) refund to Client all amounts paid to Company in respect of any Services not performed.

6.6. Survival: Sections 3, 4, 5, 6.3, 6.5, 6.6, 7, 8, and 9 shall survive the termination of this Agreement.

7. Notices

Except as otherwise expressly provided in this Agreement, any notice required under this Agreement shall be in writing and shall specifically refer to this Agreement. Notices shall be sent via one of the following means and will be effective (i) on the date of delivery, if delivered in person; (ii) on the date of receipt, if sent by a PDF image sent by email or other electronic transmission (with delivery confirmed); or (iii) on the date of receipt, if sent by private express courier or by first class certified mail, return receipt requested (or its equivalent). Any notice sent electronically shall also be delivered by private express courier or by first class mail. Notices shall be sent to the other Party at the addresses set forth below. Either Party may change such addresses by sending notice to the other Party.

Company:
Conscious Leadership, LLC 132 East 14075 South Suite 400 Draper, Utah 84020 USA legal@leadershipcircle.com

8. Indemnification and Insurance

8.1. Indemnification: Each indemnifying Party ("**Indemnifying Party**") shall indemnify, defend and hold the other Party harmless along with the indemnified Party's directors, officers, employees, agents and affiliates (collectively, "**Indemnitees**") from and against any liabilities, claims, demands, costs, damages, expenses, penalties or fees (including reasonable attorney's fees) ("**Damages**") resulting from third party claims, actions and suits ("**Claims**") arising out of such Party's (i) gross negligence or willful misconduct in the performance of Services, (ii) improper use of Company property or Client property, (iii) breach of this Agreement, including any SOW, or (iv) any violation of law by a Party, its subcontractors, or personnel, including any infringement of any third-party intellectual property. Nothing in this clause shall restrict or limit the beneficiary of such indemnity's general obligation at law to mitigate a loss it may suffer or incur as a result of an event that may give rise to a claim under this indemnity. Company and Client agree to give the Indemnifying Party prompt notice of any Claims and shall provide reasonable assistance and cooperation at the Indemnifying Party's expense in the defense and settlement of any Claim.

8.2. Limitation of Liability: EXCEPT FOR THE INDEMNIFICATION OBLIGATIONS IN SECTION 8.1, IN NO EVENT SHALL COMPANY'S LIABILITY ARISING OUT OF OR RELATED TO THIS AGREEMENT WHETHER IN CONTRACT, TORT, OR UNDER ANY OTHER THEORY OF LIABILITY, EXCEED IN THE AGGREGATE, THE TOTAL AMOUNT PAYABLE BY CLIENT TO COMPANY UNDER THIS AGREEMENT DURING THE TWELVE (12) MONTHS IMMEDIATELY PRECEDING THE ACT OR OMISSION GIVING RISE TO THE LIABILITY. IN NO EVENT SHALL EITHER PARTY BE LIABLE FOR ANY LOST PROFITS OR REVENUE OR FOR ANY INDIRECT, SPECIAL, COVER, PUNITIVE, INCIDENTAL OR CONSEQUENTIAL DAMAGES, ARISING UNDER THIS AGREEMENT AND WHETHER OR NOT THE PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THE FOREGOING DISCLAIMER SHALL NOT APPLY TO THE EXTENT PROHIBITED BY APPLICABLE LAW.

8.3. Insurance: During the term of this Agreement, Company will obtain and maintain, at its own expense, the following coverage, under the following conditions:

(a) Commercial General Liability: Company shall maintain commercial general liability coverage (including contractual liability, personal advertising and products/completed operations coverage) for limits no less than USD 1,000,000 per occurrence and USD 2,000,000 in the aggregate. The policy form shall be an "occurrence" form. If claims made, Company shall maintain coverage including completed operations for a minimum of five (5) years following termination of the Agreement.

(b) Certificate of Insurance: Upon request by Client, Company shall provide Client with its certificate of insurance evidencing the insurance coverage set forth in this section. Company shall provide to Client at least thirty (30) days prior written notice of any cancellation, non-renewal, or material change in any of such insurance coverage.

9. Miscellaneous

9.1. Assignment and Subcontracting: Company may assign its rights under this Agreement to any subsidiary or affiliate. Client may not assign its rights under this Agreement without the express written permission of Company. Company may use Certified Practitioners to perform services under this Agreement without further written permission of Client.

9.2. Relationship of the Parties and Employment Matters:

(a) Independent Contractor: The Parties to this Agreement are independent contractors, and nothing contained in this Agreement shall be deemed or construed to create a partnership, joint venture, employment, franchise, agency or fiduciary relationship between the Parties. Company further acknowledges that any workers and/or consultants it assigns to Client are employees or independent contractors of Company and not of Client. Company assumes sole and full responsibility for withholding any and all appropriate taxes and mandatory social contributions for its employees and for complying with any applicable law, including workers compensation, unemployment insurance, social contributions and wage and hour laws.

(b) Employment Matters:

(i) For all personnel performing Services under this Agreement, Company warrants that such personnel hold the necessary work authority or work permit granted by the competent authority for the respective country in which such personnel perform Services.

(ii) For Services performed within the United States of America, Company shall also:

1. Verify the identity and work authority of each worker and/or consultant under the US immigration laws, and certifies by entering into this Agreement that all personnel performing Services or that may perform Services in the future are authorized to work legally within the US; and
2. If requested at any time, certify to Client in writing that Company is in compliance with all Employment Eligibility Verification Form (I-9) requirements; and
3. Be responsible for the creation and retention of all employment records or documents required by law, including properly completed I-9 Forms for all Company workers and/or consultants working on Client's premises or otherwise performing Services.

(c) Equal Opportunity: Company agrees that, unless otherwise specifically exempted, this Agreement shall be performed in full compliance with all applicable equal opportunity affirmative action requirements, including, but not limited to, the requirements of Title VII of the Civil Rights Act of 1964, the American with Disabilities Act and the Vietnam Era Veteran's Readjustment Assistance Act of 1974. The provisions of the Equal Opportunity Clauses of Executive Order 11246, (41 CFR 60-1.4), section 503 of the Rehabilitation Act of 1973, (41 CFR 60-741.5(a)), section 402 of the Vietnam Era Veterans Readjustment Act of 1974, (41 CFR 60-250.5(a)), and, the Jobs for Veterans Act of 2003, (41 CFR 60-300.5(a)), are hereby incorporated by reference and made a part of this Agreement.

9.3. Amendment; Waiver: Except as otherwise expressly provided in this Agreement, no amendment to this Agreement shall be effective unless made in writing and executed by an authorized representative of each Party. In no event shall any terms and conditions set forth in any subsequent writing or document issued by Company in connection with the Services (including terms and condition of sale and invoices) have any effect except as otherwise expressly provided in this Agreement. A Party's failure to exercise, or delay in exercising, any right, power, privilege, or remedy under this Agreement shall not (i) operate as a waiver thereof or (ii) operate as a waiver of any other right, power, privilege, or remedy. A waiver will be effective only upon the written consent of the Party granting such waiver.

9.4. Severability: If any of the provisions of this Agreement are held to be illegal, invalid or unenforceable, such illegal, invalid or unenforceable provisions shall be replaced by legal, valid and enforceable provisions that will achieve to the maximum extent possible the intent of the Parties, and the other provisions of this Agreement shall remain in full force and effect.

9.5. Remedies: The rights and remedies of each Party provided by this Agreement are cumulative and are not exclusive of any rights and remedies provided by law or equity.

9.6. Governing Law, Jurisdiction, and Venue: This Agreement shall be governed by and construed under the laws of Utah, United States of America, regardless of the laws that might otherwise govern under applicable Utah principles of conflicts of law. Any dispute which may arise under this Agreement shall be litigated, if at all, exclusively in the federal or state courts of the State of Utah located in Salt Lake City. The prevailing party in any such litigation shall be entitled to reimbursement of its reasonably incurred attorney fees and costs.

9.7. Entire Agreement: This Agreement contains the entire understanding between the Parties with respect to the Services and supersedes and terminates all prior agreements, understandings and arrangements between the Parties with respect to such subject matter, whether written or oral. In no event shall any terms and conditions set forth in any subsequent writing or document issued by Company in connection with the Services (including terms and condition of sale) have any effect except as otherwise expressly provided in this Agreement.

9.8. Caption; Construction: Capitalized terms defined in the singular shall include the plural and vice versa. Titles, headings and other captions are for convenience only and shall not affect the meaning or interpretation of this Agreement. The terms "includes" and "including" mean "includes, without limitation," and "including, without limitation," respectively.

9.9. Counterparts: This Agreement may be executed in one or more counterparts, each of which together shall constitute one and the same Agreement. The delivery of a signed facsimile or other electronic copy of this Agreement or any SOW shall have the same binding effect as delivery of an original signed copy of this Agreement or SOW.

9.10. Force Majeure: Neither Party shall be deemed to have breached this Agreement for failure to perform its obligations under this Agreement to the extent such failure results from acts of God, earthquakes, fires, floods, embargoes, wars, acts of terrorism, insurrections, riots, civil commotions and similar events. If a force majeure event occurs, the Party unable to perform shall promptly notify the other Party of the occurrence of such event, and the Parties shall meet (in person or telephonically) promptly thereafter to discuss the circumstances relating thereto. The Party unable to perform shall (i) provide reasonable status updates to the other Party from time to time, (ii) use commercially reasonable efforts to mitigate any adverse consequences arising out of its failure to perform and (iii) resume performance as promptly as possible.

9.11. Change in Circumstances: Company agrees to promptly inform Client in writing of any event or change in circumstances which could reasonably affect its ability to perform the Services hereunder in a manner contemplated by the Parties.

EXHIBIT A

DATA PROCESSING AGREEMENT

The additional data processing terms in this data processing agreement ("DPA"), effective as of the date of the Agreement, shall govern this DPA between **Company** and **Client**. Company and Client are hereinafter collectively referred to as "**Parties**" or individually as a "**Party**."

WHEREAS, the Parties have entered into an Agreement for Services and Statement of Work (the "**Agreement**"); and

WHEREAS, in the course of providing the Services to Client pursuant to the Agreement, Client may disclose Personal Data (as defined herein) to Company; and

WHEREAS, to ensure adequate safeguards with respect to the Processing of Personal Data, the Parties agree to comply with the following provisions with respect to any Personal Data, each acting reasonably and in good faith;

NOW, THEREFORE, in consideration of the foregoing premises and of the mutual promises and covenants set forth below, Company and Client hereby agree as follows:

1. Definitions

All capitalized terms not defined herein shall have the meaning set forth in the Agreement.

(a) "**Applicable Data Protection Laws**" means all applicable laws, regulations, regulatory guidance, or requirements in any jurisdiction relating to data protection, privacy, or confidentiality of Personal Data including but not limited to (a) the GDPR together with any transposing, implementing or supplemental legislation, and (b) the CCPA.

(b) "**Business**" means a sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners, that Processes the Personal Data of Data Subjects, or on the behalf of which such information is collected and that alone, or jointly with others, determines the purposes and means of the processing of a Data Subject's Personal Data. For the avoidance of doubt, Client is a Business.

(c) "**CCPA**" means the California Consumer Privacy Act, Cal. Civ. Code § 1798.100 *et seq.*, and its implementing regulations.

(d) "**Contractor**" means a party to whom a Business makes available a Data Subject's Personal Data for a Business Purpose pursuant to a written contract with the Business, provided that the contract prohibits the Contractor from retaining, using, or disclosing the Personal Data for any purpose other than for the specific purpose of performing the services specified in the contract or as otherwise permitted by the CCPA. The terms "Business Purpose" and "Commercial Purpose" have the same meaning as those terms as defined by the CCPA. For the avoidance of doubt, Company is a Contractor.

(e) "**Controller**" means the entity which determines the purposes and means of the Processing of Personal Data.

(f) "**Data Breach**" means a breach of security leading to the accidental, unauthorized, or unlawful destruction, loss, alteration, disclosure of, or access to Personal Data transmitted, stored, or otherwise Processed for the purposes of providing the Services.

(g) "**Data Protection Authority**" means any representative or agent of a government entity or agency who has the authority to enforce Applicable Data Protection Laws.

(h) "**Data Subject**" means a natural person to whom Personal Data relates.

(i) "**GDPR**" means the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

(j) "**Personal Data**" means any information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with an identified or identifiable natural person or with a particular household. An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.

(k) "**Process**," "**Processing**," "**Processed**" shall mean any operation or set of operations which is performed upon Personal Data by the Parties or in connection with and for the purposes of the provision of the Services, whether or not accomplished by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction; and as defined by Applicable Data Protection Laws.

(l) "**Services**" means the provision of the services to be provided by the Company pursuant to the Agreement.

2. Processing of Personal Data

2.1. Roles of the Parties. The Parties are Controllers. The subject matter, duration, purpose of the Processing, and the types of Personal Data and categories of Data Subjects Processed under this DPA are further specified in Schedule 1.

2.2. Company's Obligations. Company's instructions for the Processing of Personal Data shall comply with Applicable Data Protection Laws.

2.3. Client's Obligations. Client will ensure that all Personal Data is accurate and up to date at the time of transfer of Personal Data to Company and will provide a secure mechanism for the transfer of Personal Data between Client and Company.

2.4. Joint Obligations. All Personal Data Processed by the Parties pursuant to the Agreement is Confidential Information and the Parties will Process Confidential Information only in accordance with documented instructions set forth in Schedule 1 or as otherwise provided by the other Party in writing. The Parties shall adhere to all Applicable Data Protection Laws about Processing Personal Data. Where a Party believes that compliance with any instructions by the other Party would result in a violation of any Applicable Data Protection Laws, the Party shall notify the other Party thereof in writing without delay. The Parties shall make available to each other all information necessary to demonstrate their compliance with their obligations under this DPA.

(a) Assistance Requirements. The Parties shall assist each other with the following: compliance with Applicable Data Protection Laws when required by Applicable Data Protection Laws; notifications to, or inquiries from a Data Protection Authority; notifications to, and inquiries from, Data Subjects; and Company's obligation to carry out data protection impact assessments and prior consultations with a Data Protection Authority.

2.5. Company Use. Company is permitted to access, collect, analyze, and use the data, information, or insights generated or derived from the provision, use, and performance of the Services to deliver the Services and for its own purposes, such as improving its products and services, analytics, and industry analysis. Company will ensure that Personal Data is in an anonymized, de-identified, or aggregate form that does not identify individuals associated with the usage of the Services.

3. Notification Obligations

3.1 Notification Obligations. In relation to the Personal Data Processed under this DPA, the Parties shall immediately notify each other, in writing, of the following:

(a) A Data Subject's request to exercise their privacy rights such as accessing, rectifying, erasing, transporting, objecting to, or restricting their Personal Data;

(b) Any request or complaint received from a Party or its employees;

(c) Any question, complaint, investigation, or other inquiry from a Data Protection Authority;

(d) Any request for disclosure of Personal Data; and

(e) Where the Personal Data becomes subject to search a seizure, an attachment order, confiscation during bankruptcy or insolvency proceedings, or similar events or measures by third parties while being Processed.

4. Confidentiality

4.1. Confidential Information. All information pursuant to the Agreement and all information defined as confidential by the Agreement is Confidential Information.

4.2. Personnel. The Parties shall ensure that their personnel engaged in the Processing of Personal Data are informed of the confidential nature of the Personal Data, have received appropriate training on their responsibilities, and have executed written confidentiality agreements. The Parties shall ensure that such confidentiality obligations survive the termination of the Parties' respective employment relationships with such individuals.

4.3. Limitation of Access. The Parties shall ensure that access to Personal Data is limited to those personnel performing Services in accordance with the Agreement.

5. Security and Documentation

5.1. Protection of Personal Data. The Parties shall maintain appropriate technical and organizational measures for protection of the security (including protection against unauthorized or unlawful Processing and against accidental or unlawful destruction, loss, alteration, damage, unauthorized disclosure of, or access to, Personal Data), confidentiality, and integrity of Personal Data.

5.2. Documentation. The Parties shall be able to demonstrate compliance with their obligations under this DPA and shall be able to make such documentation available to a Data Protection Authority upon request.

6. Data Breaches

6.1. Data Breach Notification. Company shall notify Client in writing without undue delay after becoming aware of a suspected Data Breach. In no event shall such notification be made more than 72 hours after Company's discovery of the Data Breach.

6.2. Data Breach Management. Company shall make reasonable efforts to identify the cause of such Data Breach and take those steps it deems necessary and reasonable to remediate the cause of the Data Breach to the extent the remediation is within Company's reasonable control.

7. Termination and Storage Limitation

7.1. Termination. This DPA shall terminate automatically upon the later of (a) the termination or expiry of the Agreement or (b) a Party's deletion or return of Personal Data. A Party shall further be entitled to terminate this DPA for cause if the other Party is, in the sole opinion of such Party, in a material or persistent breach of this DPA which, in the case of a breach capable of remedy, shall not have been remedied within ten (10) days from the date of receipt by the other Party of a notice from a Party identifying the breach and requesting its remedy.

7.2. Storage Limitation. Company shall retain Personal Data no longer than necessary for the purpose(s) for which it is Processed under Schedule 1.

8. CCPA

8.1 CCPA Certification. Company certifies that Company can comply with the privacy requirements set out for Contractors under the California Consumer Privacy Act, Cal. Civ. Code § 1798.100 et seq., as amended from time to time, and its implementing regulations ("CCPA").

8.2 Company CCPA Obligations. Company is acting solely as a Contractor with respect to Personal Data. Company agrees that it:

(a) shall not sell or share Personal Data provided by Client;

(b) shall not collect, retain, use, disclose or otherwise Process Personal Data outside of the direct business relationship between Company and Client or for any purpose (including a commercial purpose) other than for the specific purpose of performing the services, obligations, or actions for the benefit of Client or Client employees and Client contractors as specified in the Agreement and this DPA;

(c) shall comply with all applicable laws and regulations in connection with its receipt, use, handling, Processing, access to and storage of Personal Data (e.g., the CCPA);

(e) shall promptly refer to Client any requests with respect to Personal Data received from individuals, including requests to access, delete, or change Personal Data and Company shall cooperate with and assist Client in responding to and fulfilling such requests;

(f) shall not combine Personal Data provided by Client with Personal Data that it receives from other sources;

(g) shall allow Client to take reasonable measures to review Company's compliance with the requirements under the CCPA;

(h) shall allow Client to take steps to remediate unauthorized use of Personal Data;

(i) shall enter into agreements at least as restrictive as this CCPA section with entities, engaged by Company, that help Process Personal Data provided by Client to Company;

(j) and shall notify Client if Company decides it can no longer meet its obligations under the CCPA.

9. Mechanisms for International Transfers

9.1 Transfers Outside of the EU/UK/Switzerland to a Country with an Adequacy Decision**.** Company shall rely on an adequacy decision to transfer Personal Data when such adequacy decision has been granted under Applicable Data Protection Laws. For the avoidance of doubt, if Company is certified under the Data Privacy Framework Program, granted by the Commission Implementing Decision of 10.7.2023 on the Adequate Level of Protection of Personal Data Under the EU-US Data Privacy Framework ("DPF"), the UK Extension to the EU-U.S. DPF ("UK DPF"), or the Swiss-U.S. Data Privacy Framework ("Swiss-U.S. DPF"), the DPF, UK DPF, or Swiss-U.S. DPF shall apply and supersede the applicable transfer mechanism(s) set forth in Section 9.2 of this DPA as a valid transfer mechanism to Personal Data transferred to the United States.

9.2 Transfers Outside of the EU/UK/Switzerland to a Country without an Adequacy Decision**.** In the course of the provision of Services under the DPA, it may be necessary for Client to transfer Personal Data from the European Union, the European Economic Area and/or their member states, Switzerland, or the United Kingdom, to Company in a country that does not have an adequacy decision or is not located in the European Economic Area.

(a) In relation to Personal Data that is subject to the GDPR (i) Company will be deemed the "data importer" and Client is the "data exporter"; (ii) the Module One terms shall apply where Client is a Controller and where Company is a separate Controller; (iii) in Clause 7, the optional docking clause shall be deleted; (iv) in Clause 11, the optional language shall be deleted; (v) in Clause 17, Option 1 shall apply and the Standard Contractual Clauses shall be governed by the member state of Spain; (vi) in Clause 18(b), disputes shall be resolved before the courts of Spain; (vii) Annex I and Annex II shall be deemed completed with the information set out in Schedule 1 of this DPA respectively; and (viii) if and to the extent the Standard Contractual Clauses conflict with any provision of the Agreement (including this DPA) the Standard Contractual Clauses shall prevail to the extent of such conflict. For this section, the Standard Contractual Clauses from the Commission Implementing Decision (EU) 2021/914 are incorporated by reference and available here: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc/standard-contractual-clauses-international-transfers_en.

(b) In relation to Personal Data that is subject to UK Data Protection Laws, the International Data Transfer Agreement ("IDTA") shall apply with the following modifications: (i) the contact information about the parties to the Agreement is the contact information for the IDTA; (ii) Client is the data exporter and Company is the data importer; (iii) the laws that govern the IDTA and the location where legal claims can be made is England and Wales; (iv) the UK GDPR applies to the data importer's processing of transferred data; (v) the Parties do not use the additional security or commercial clauses from the IDTA; and (vi) the information in this DPA and Schedule 1 can be used for Tables 1-4. For this section, the Standard Contractual Clauses from the Information Commissioner's Office are incorporated by reference and available here: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-data-transfer-agreement-and-guidance/.

(c) In relation to Personal Data that is subject to the Swiss DPA, the Standard Contractual Clauses referenced in Section 9.1.1 shall apply with the following modifications: (i) references to "Regulation (EU) 2016/679" shall be interpreted as references to the Swiss DPA; (ii) references to "EU", "Union" and "Member State law" shall be interpreted as references to Swiss law; and (iii) references to the "competent supervisory authority" and "competent courts" shall be replaced with the "the Swiss Federal Data Protection and Information Commissioner " and the "relevant courts in Switzerland".

9.3 Alternative Data Transfer Mechanisms**.** The Parties acknowledge that the laws, rules and regulations relating to international data transfers are rapidly evolving. In the event that Company adopts another mechanism authorized by applicable laws, rules or regulations to transfer Personal Data (each an "Alternative Data Transfer Mechanism"), the Parties agree to work together in good faith to implement any amendments to this DPA necessary to implement the Alternative Data Transfer Mechanism.

10. Miscellaneous Provisions

10.1. Amendments**.** This DPA may not be amended or supplemented, nor shall any of its provisions be deemed to be waived or otherwise modified, except through a writing duly executed by authorized representatives of both Parties.

10.2. Governing Law**.** This DPA shall be governed by the governing law set forth in the Agreement.

EXHIBIT B

SCHEDULE 1

Description of the Processing

Contact Information

Company: Conscious Leadership, LLC
Address: 132 East 14075 South Suite 400
Draper, UT 84020
Representative/DPO/Privacy Office Email: legal@leadershipcircle.com

Subject-Matter

The subject-matter of the Processing:
The subject-matter of the Processing is for the purpose of evaluating the leadership styles and skills of Client's employees (and contractors, if applicable) and providing them with coaching to improve those skills, as outlined more completely in the Agreement. In order to perform these Services, Company must process Personal Data to interact and communicate with the individuals Client wishes to invite to participate in the evaluation process. Such interaction, communication, and processing of Personal Data may occur beyond Client's engagement with Company and Company's delivering of the Services to Client.

Duration

Duration of the Processing:
As set forth in the Agreement between the Parties.

Extent, Type and Purpose of the Processing

The extent, type and purpose of the Processing is as follows:
As set forth in the Agreement between the Parties.

Frequency of Transfer

Continuous

Data Subjects

Personal Data Processing may relate to the following categories of Data Subjects:
Client's employees and/or contractors

Categories of Data

The Personal Data Processed may concern the following categories of data:
Contact information, e.g., names, titles, business or personal email, etc.

Technical and Organizational Measures (TOMs) to Secure Data

Company TOMs:

Preamble

The protection of personal data serves to safeguard the interests, fundamental rights and freedoms of the data subjects. Appropriate technical and organizational measures (TOM) must be defined and implemented in accordance with the General Data Protection Regulation (GDPR).

Objective of the TOM definition

According to Article 32 (1) GDPR, appropriate TOM must be established for each processing activity to ensure an appropriate level of protection. The TOM are not, however, specified in the GDPR. Just warranty objectives or protection goals are listed there. To this extent, the TOM must be defined and documented in relation to the processing activities.

This document is intended to be a supporting document for the definition and documentation of TOM. Typical examples of TOM with which the protection goals can be achieved are listed for the respective protection goals.

Terms/Definitions

Technical Measures relate to the process of data processing itself. They describe all measures that can be physically implemented, for example, by installing access control systems or by creating user accounts that are password-protected.

Organizational Measures refer to the framework conditions of the data processing operation. They comprise rules, specifications and instructions for action that serve to ensure that the persons acting comply with data protection laws.

Requirements for TOM

Confidentiality

Confidentiality means that personal data must only be accessible to authorized persons. Not only the personal data itself is threatened, but also e.g., systems and configurations. An attack on confidentiality represents the unauthorized acquisition of information (e.g., by an unauthorized person spying on the login data).

Access control

An access control system is designed to prevent unauthorized persons from gaining access to rooms or places where personal data are archived or processed.

Technical measures:

x Alarm system
x Automatic access control systems
x Biometric access control systems
x Chip cards / transponder systems
x Bell system with camera
x Video surveillance of entrance areas
x Building security concepts
x Separation systems
x Fencing of the factory sites

Organizational measures:

x Key Management
x Testing of protective measures
x Visitor control procedures
x Employee / visitor badges
x Visitors accompanied by our own staff
x Access logs

Access control

Measures suitable to prevent data processing systems from being used by unauthorized persons. Access control describes the prevention of unauthorized use of systems.

Typical measures:

x Technical measures
x Network Isolation/Segmentation
x Securing external Access (authentication, connection setup from outside)
x Protection of Devices (encryption, login, lock)
x Automatic Screen Lock
x Mobile Device Management
x Intrusion Detection Systems
x Anti-Virus Software (Server)
x Anti-Virus Software for Mobile Devices

Organizational measures:

x Rules for the use of network services
x Mobile Device Policy
x We do not allow VPN access or remote access to office systems.
x Instruction "Documents Handling”

Access control

Measures to ensure that those authorized to use a data processing system can only access the personal data according to their access authorization and that personal data cannot be read, copied, changed or removed without authorization during processing, use and after storage.

Typical measures:
(if available/implemented, please mark with a cross)

Technical measures
x Login with username and password
Login with biometric data
Automatic screen lock with password protection
x Shredder (at least level 3, cross cut)
x Collection container. f. ext. destruction
x Physical deletion of data media
x Logging of accesses

Organizational measures
x Use of role and authorization concepts
x Manage user permissions
x Allocation of rights to enter, change and delete data based on the authorization concept
x Creating User Profiles
x Administration Admin user rights
x Minimum number of administrators
x Central password assignment
x Instruction for secure passwords
x Instructions for the disposal of data media and documents
x Instruction "Delete / Destroy"
x Clean Desk policy

Separation Control

Measures to prevent that data collected for different purposes can be combined.

Typical measures:
(if available/implemented, please mark with a cross)

Technical measures:
x Separation of functions (D-Q-P)
x Multi-Client Capability

Organizational measures:
x Regulated change of purpose procedures
x Records with purpose attributes

Pseudonymization and Anonymization

Measures intended to exclude or significantly complicate the identification of the person concerned.
Anonymization requires that personal data is modified so the individual details cannot be attributed to a natural person or can only be attributed to a natural person with disproportionate effort. In contrast, pseudonymization means a disassociation of personal data by replacing the name and other identification features so that the identity can be traced and reversed by means of the list of clear names and the list of identification features.

Technical measures:
x Restrict access to assignment data to the necessary persons

Encryption

Encryption is a procedure that converts a plain text into an unreadable text by means of a key so that the source information can only be made readable again by using the appropriate key. This minimizes the risk of a data protection incident during data processing since encrypted content is generally not readable by third parties without the corresponding key. Encryption is considered as the best option to protect personal data in transit and is one way of securing stored personal data. The risk of misusing personal data is minimized by restricting access to authorized persons with the correct key.

Technical measures:
x Use of state-of-the-art encryption methods
x Encryption of files and directories.
x Encryption of data carriers
x Encryption of mobile data media
x Encryption of notebooks / tablets

Integrity
The term "integrity" means that the undetected modification of personal data should not be possible. In contrast to confidentiality, which is concerned with the authorization of data modification, integrity is about the correctness of personal data and the correct functioning of the system. Thus, the focus of integrity is on the traceability of data changes.

Input control
Measures to ensure that it can be subsequently checked and established whether and by whom personal data have been entered, modified, or removed from data processing systems. Input control is achieved by monitoring the system usage (monitoring) and storing log files (logging), which can take place at various levels (e.g., operating system, network, firewall, database, application).

Technical measures

x Technical logging of the input, modification and deletion of data
x Manual or automated control of the protocols

Organizational measures

x Overview with which software which data can be entered, changed or deleted
x Traceability of entry, modification, and deletion through individual usernames
x Retention of forms from which data have been taken over in automated processing operations
x Definition of access authorizations for protocols and logs
x Specifications for the storage and analysis of logs (purpose, evaluation in case of violations/suspicion)
x Clear responsibilities for deletions

Data Transmission Control
Measures to ensure that personal data cannot be read, copied, changed, or removed by unauthorized persons during electronic transmission or during their transport or storage on data carriers, and that it is possible to check and establish to which points personal data are to be transmitted by data transmission equipment.

Technical measures

x Encrypted storage
x Logging of accesses and retrievals
x Safe transport containers
x Use of secure courier services
x Provision of encrypted connections e.g., https
x 2-factor authentication
x Use of encryption methods

Organizational measures

x Obligation of data secrecy
x Verification of the correct addressee
x Overview of regular retrieval and transmission processes
x Personal delivery with protocol

Order Control
Order control takes effect when personal data is processed on behalf of/by third parties. The objective is that personal data which are transmitted to an authorized subcontractor is processed in accordance with the conditions of the responsible controller and with the data protection regulations.

Technical measures

x Restriction of logical access and authorizations
x Logging of the system usage

Organizational measures

x Documentation of the selection procedure
x Contractual obligation of the processor
x Control of order processing and documentation of the control (supplier audits)
x Confidentiality agreement/ NDA and commitment to data secrecy

Availability
Availability means the requirement that personal data can be accessed and processed without delay and that the data can be used properly in the intended process. For this purpose, they must be accessible by authorized persons, and it must be possible to apply the intended methods for processing them.

Availability control
Personal data must be protected against loss and accidental destruction.

Technical measures

- x Redundancy of SW, HW and infrastructure
- x Ensuring the transferability of data
- x Creation of reserve capacity, e.g.
  - Ensuring connectivity in emergencies,
  - Contingency rooms and backup data center
- x Update Management

Organizational measures

- x Substitution regulation for absent employees
- x Storage/archiving instructions
- x Support concept including, among others, responsibilities, authorities and interfaces between IT and specialist departments

Contingency plan
The emergency concept covers two main functions: On the one hand, the business processes should be stabilized in such a way that the probability of a damaging incident is minimized, and on the other hand, the company or practice should be prepared for an incident or emergency in the best possible way to reduce the consequences as much as possible.

The emergency concept can be divided into two components: The first component is the Disaster Prevention Concept, which contains the basic conditions, such as the Business Process Overview or the Master Data of the company. Furthermore, all information and personal data that is not directly required for Emergency Management is collected in the Disaster Prevention Concept.

The second component is the Emergency Manual, which describes information for Emergency Management. This information includes, for example, contact information or instructions for action to be taken in case of an emergency.

Technical measures

- x Uninterruptible power supply
- x Fire and smoke detection systems
- x Fire extinguishers and flooding systems in the server room
- x Hard disk mirroring
- x Overvoltage protection for the power supply
- x Air-conditioned server room
- x Temperature and humidity monitoring in the server room

Organizational measures

- x Emergency planning/manual (e.g. BSI Basic Protection)
- x Designation of an emergency response team
- x Alarm chains and alarm systems
- x Checklists for error containment and problem analysis
- x Regulations on workarounds/emergency operating procedures
- x Storage of the backup media in a safe place outside the server room
- x Obsolescence management for the required SW programs

Restoration of availability
The security of the processing of personal data in accordance with the GDPR includes the ability to promptly restore the availability of and the access to personal data in the event of a physical or technical incident.

Technical measures

- x Use of backup systems
- x Emergency power supply
- x Separate/mirrored data storage
- x Redundant servers
- x Hourly/Daily/Weekly snapshots

Organizational measures

- x Contingency planning
- x Substitution plans for personnel
- x Test of the Emergency Concept
- x Backup Concept

x Business Continuity Management
x Service contracts with IT service providers
x Instruction on the data backup obligation

Resilience of systems

Data processing systems and services must also be resilient. This means: IT must be robustly set up to withstand heavy use without collapsing completely. For example, too many simultaneous access requests to a web server can put too much strain on the systems (Denial of Service). Often they are even part of a cyber-attack that needs to be withstood.

Typical measures:
(if available/implemented, please mark with a cross)

Technical measures
x Firewall
x Virus scanner
x Spam Filter
x Security Updates

Organizational measures
x Regulations on monitoring procedures (ticket system on faults)
x Regulations for evasion processes
x Generation of incidents from monitoring events (malfunction tickets)

Measures for security zones

Technical and organizational measures to take into account special requirements for computing and archive rooms.

Technical measures
x Network protection
x Premises: Conditions and equipment
x Supply engineering: air conditioning, USV, overvoltage/lightning protection
x Fire protection
x Burglary protection
x Access protection and controls for security zones

Organizational measures
x Specifications for adequate behavior in computer rooms
x Specifications for archive rooms

Procedures for review, evaluation, and improvement of TOM

The TOM for ensuring data protection and data security must be regularly reviewed in accordance with Art. 32 para. 1 lit. d) to ensure that they still fulfil their purpose and are state of the art. To this end, organizational procedures and processes must be developed, defined and implemented.

The legislator does not prescribe a specific cycle for review. However, experts recommend that TOM should be checked at least once a year - or more frequently depending on the level of risk. However, if a security gap in a system in use becomes known, immediate action must be taken.

Technical measures
x Employee Security Training Testing System

Organizational measures
x Data protection/data security directive
x Data protection and information security organization
x Data classification incl. deletion concept
x Regular training of employees (awareness)
x Guidelines
x Review and evaluation of TOM using checklists and audit questionnaires
x Auditing of the internal participants