DATA PRIVACY TERMS AND CONDITIONS

LIFE TIME
HEALTHY WAY OF LIFE

Last Updated: April 23rd 2018.

These Data Privacy Terms and Conditions govern your agreement with Life Time. "We", "our", and "Life Time" mean Life Time, Inc. and our affiliates; "you" and "your" mean the Vendor identified in the Vendor Agreement (the "**Agreement**"). The Agreement identifies the Vendor benefits, the quantities, charges, and other details of your order. The Agreement also refers to documents which may apply to the products or professional services you selected. The Agreement, the Vendor Terms and Conditions, any applicable referenced documents, and these Data Privacy Terms and Conditions constitute the complete agreement and supersede any prior discussions or representations regarding your order. If the terms of the Agreement are different from these Data Privacy Terms and Conditions, the Agreement will have priority. Other terms and conditions you incorporate into a purchase order or similar document do not apply.

1. **Personal Data Definition**. References to "Personal Data" means information relating to an identified or identifiable person that Life Time provides to Vendor or that Vendor otherwise acquires from or on behalf of Life Time in connection with the Agreement. Personal Data includes contact information, such as first and last names, emails, postal addresses, and phone numbers; usernames and passwords; date of births; social media account(s) information; payment and billing information; geo-location; emergency contact information; images, videos, photographs, sounds and other materials in public forums; member interest groups, member numbers, classes, programs, events, and club activities, and/or information included in public forums, messages, comments, searches, or queries through the Services.

2. **Vendor Use**. All Personal Data and other information given by Life Time to the Vendor ("**Life Time Data**") will be held in trust solely for the benefit of Life Time. This information remains the exclusive property of Life Time and the information provided is for no other purpose than to help Vendor perform the Services outlined in the Agreement. Vendor will not disclose, transfer, duplicate, reproduce, retain, re-sell, or use Life Time Data in any way without the prior written consent of Life Time. Vendor will exercise due care not to disclose any data, with exception to employees and agents to whom disclosure is necessary to perform the duties of the Agreement.

3. **Data Security**. To ensure its security and integrity against any anticipated or actual hazards, Vendor will act to prevent unauthorized access, acquisition, destruction, use, modification and disclosure of Life Time Data. Vendor agrees that its collection, use, storage, and disposal of Life Time Data and other confidential information will comply with all applicable foreign, federal, state, and local laws, rules, and regulations. Vendor will implement and maintain appropriate administrative, technical, and physical safeguards, including a written information security plan; information access controls that require appropriate authorization, generate audit trails of approvals and require periodic reviews by asset owners; systems protections (e.g., intrusion protection); physical security measures; and a security awareness program, including employee training. To the extent that any Personal Data relates to a resident of Massachusetts and constitutes "Personal Information" as defined in 201 CMR 17.02, Vendor will also comply with the obligations of 201 CMR 17.00 et. seq., entitled "Standards for the Protection of Personal Information of Residents of the Commonwealth", with respect to such Personal Data. Without limiting the foregoing, Vendor will implement the following safeguards:

   (i) General Safeguards:
      1. Vendor shall not store any Life Time Data on a mobile device, for example any laptop computer, tablet, smartphone, PDA, jump drives, CD, DVD, or other electronic device unless the data is encrypted;
      2. All Life Time Data must be encrypted while being transmitted between networks, including e-mail, whether public or private;
      3. All Life Time Data maintained on backup tapes or other backup media must be encrypted;
      4. Software firewalls must be installed on all laptops and other devices containing Life Time Data if connected to public networks or unsecure private networks;
      5. Background checks must be performed on all personnel with access to Life Time Data;
      6. Prior to loading any Life Time Data onto any application that is Internet facing, application vulnerability testing must be performed and any findings must be appropriately remediated;
      7. Security tools required by this Amendment, such as encryption tools, must be monitored to

determine whether they are installed, updated and active;
8. Access rights to Life Time Data maintained on any system must be promptly terminated when personnel no longer need access to such Life Time Data;
9. Security-related patches must be applied in a timely manner in relation to the criticality of the patch, but not later than ten (10) days after the date such patches become available to Vendor for critical patches and thirty (30) days for other patches.

(ii) Safeguards That Apply to Laptops Containing Life Time Data:
1. Anti-virus and anti-spyware software must be installed and updated in a timely manner;
2. All data stored on a laptop must be securely erased prior to disposal, reuse, resale or return to a vendor at end of a lease;
3. Laptops must be physically secured when unattended;
4. Vendor must use a standard configuration on all laptops that requires the screensaver to activate after not more than ten (10) minute of inactivity and requires entry of the users password to access the data on the laptop;
5. Laptops must use log-in passwords that are complex, at least seven (7) characters in length, must be changed at least every ninety (90) days and cannot be reused for at least ten (10) iterations;
6. Laptops must lock out after five (5) invalid attempts at entering the log-in password;
7. Users must not share passwords required to log in to laptops with unauthorized users of the laptops.

(iii) Safeguards That Apply to smartphones or PDA's Containing Life Time Data
1. A password or PIN to gain access to the data stored on it;
2. Device must erase all data stored on them after not more than ten (10) invalid log-in attempts;
3. Device must lock after a period of inactivity of not more than twenty (20) minutes, requiring that the log-in password or PIN be entered;
4. All Life Time Data stored on a device must be securely erased prior to disposal, reuse, resale or return to a vendor at end of a lease;
5. Users must not share passwords or PINs required to access the data on a device with unauthorized users.

(iv) Safeguards That Apply to Other Portable Media Containing Life Time Data
1. USB drives must erase all data stored on them after not more than ten (10) invalid log-in attempts;
2. Portable Media must require the use of a complex password or PIN to gain access to stored data;
3. All Life Time Data stored on portable media must be securely erased prior to disposal, reuse, or resale of the portable media;
4. Users must not share passwords required to access the data on portable media with unauthorized users of the portable media.

4. **Disclosure of Life Time Data.** Vendor will limit access to Life Time Data solely to its permitted subcontractors and those personnel of Vendor who need access in connection with the performance of Services under the Agreement. Vendor will not sell, disclose, release or otherwise make available Life Time Data to any other party. The disclosure of Life Time Data will be limited to the specific information necessary for such subcontractors and personnel to perform the services under the Agreement. Vendor will inform its personnel with access to Life Time Data of the requirements set forth in this Amendment and will ensure that such personnel are bound by and comply with such requirements. Vendor will ensure that each subcontractor that has access to Life Time Data is bound by and complies with the same obligations as Vendor under this Amendment.

Vendor will not be in violation of its obligations under the immediately preceding paragraph when Life Time Data is disclosed by Vendor to the extent legally required by a valid order of a court of competent jurisdiction or administrative agency, or a validly enforceable subpoena; provided that (i) Vendor provides prompt written notice to Life Time and the applicable of any such request or requirement with reasonably sufficient details regarding the request or requirement and the Life Time Data that Vendor is contemplating disclosing

so that Life Time and related entities may seek a protective order or other appropriate remedy and (ii) Vendor reasonably cooperates with Life Time or related entities in their efforts to seek such order or remedy.

5. **Audit**. If Vendor is processing credit card data on behalf of Life Time, Vendor must provide Life Time with current PCI-DSS Attestation of Compliance. These attestations, ISO 27001 certification, the SOC reports, and the PCE-DSS AOC – must be provided to Life Time on an annual basis. Any reported exceptions may be considered a violation of the Agreement. Vendor must promptly implement a corrective plan to Life Time.

6. **Security Breach**. Vendor must promptly notify Life Time if any known or suspected breach, act, or omission compromises the security, confidentiality, or integrity of Life Time's Data,within three (3) days. Vendor must appoint an employee to serve as the primary security contact for Life Time. This employee must be able to assist Life Time at all times as a contact in resolving problems associated with a security breach. Vendor will promptly investigate each potential, actual or suspected breach and assist Life Time in connection with any investigation that Life Time may conduct. Vendor will take all steps requested by Life Time to limit, stop, or otherwise remedy any potential, actual, or suspected breach.

7. **Termination**. Without limiting any other right to terminate the Agreement or any other remedy available to Life Time, upon the occurrence of any security breach of Vendor's obligations under this Amendment, Life Time may immediately terminate the Agreement.

8. **Disposal or Return of Life Time Data.** Promptly upon the completion of the Agreement or the written request of Life Time, all Life Time Data in any form, in Vendor's possession or under its control must be (i) destroyed in a manner that prevents its recovery or restoration or, (ii) if so directed by returned to Life Time in a secure manner without Vendor retaining any actual or recoverable copies, in both instances without charge. Notwithstanding the immediately preceding sentence, Vendor may retain copies of Life Time Data to the extent required by applicable law or regulation; provided that Vendor notifies Life Time of the retained Life Time Data.

9. **Request to Access and Correct Personal Data**. In the event Vendor receives a request from a third party to access any Personal Data in Vendor's possession, Vendor will promptly forward a copy of such request to Life Time. Except as expressly permitted in section d this Amendment, Vendor will not disclose any Personal Data to a third party, whether in response to a request or otherwise.

   Upon request, Vendor will make Personal Data in its possession available to Life Time or any third party designated in writing by Life Time, and will correct Personal Data in Vendor's possession in accordance with the instructions in such request.

10. **Cooperation and Audit**. Vendor will provide Life Time with information as may be reasonably requested by Life Time from time to time with regard to Vendor's compliance with its obligations under this Amendment, including, if available and not subject to the attorney-client, work product or any similar privilege, the results of any audits or tests performed on Vendor's information security program or on any components thereof. Vendor will permit Life Time, a third party chosen by Life Time and reasonably acceptable to Vendor, to audit Vendor's records, procedures, and privacy, confidentiality and security controls upon reasonable notice and during regular business hours, at Vendor's offices, for purposes of verifying Vendor's compliance with this Amendment.

11. **No Limitations of Liability; Indemnification**. Notwithstanding anything in the Agreement to the contrary, the limitations or exclusions of liability set forth in the Agreement, if any, will not apply to this Amendment and will not limit Vendor's liability for failing to satisfy any of its obligations under this Amendment. Vendor agrees to indemnify, defend, and hold harmless Life Time, its officers, directors, agents, and employees from any and all claims, liability, loss, damage, expense, or costs (including reasonable attorneys' fees) incurred from: (a) claims of privacy right violations or data security breaches, (b) any of Life Time's actions taken on behalf of or for the benefit of Vendor in connection with the Agreement, whether caused in whole or in part by the sole, joint, or concurrent negligence of Life Time, and (c) any act or omission of Vendor under the Agreement.

12. **Survival**. This Amendment shall survive the expiration or termination of the Agreement and thereafter remain in full force and effect for as long as Vendor or any of its subcontractors retains any Life Time Data;

provided, however, Sections Security Breach (6), Cooperation and Audit (10), No Limitations on Liability; Indemnification (11), and Survival (12) of this Amendment shall survive indefinitely.

13. **Severability**. If any provision of the Agreement is found to be invalid, illegal or unenforceable, the remaining provisions remain in full force if the essential provisions of these terms for each Party remain valid, legal and enforceable.

14. **Updates**. Life Time may update or modify these Data Privacy Terms and Conditions at any time. If changed, Life Time will post the revised Terms to http://www.lifetime.life/media.html with a "Last Updated" at the top of the Terms and Conditions. All changes are effective immediately. Any continued use of the Services following the effectiveness of any changes constitutes acceptance of such changes.