A part of: ThermoFisher SCIENTIFIC

CONNECTED CARE PORTAL

LIFE TECHNOLOGIES CORPORATION

THERMO FISHER CLOUD TERMS OF USE

Last Updated December 12, 2018

These Terms of Use ("**Terms**") govern your access to and use of Life's proprietary infrastructure, software, applications and services ("**Services**"). By accessing or using the Services, you accept these Terms and conclude a legally binding contract between you and Life Technologies Corporation, a Thermo Fisher Scientific business ("**Life**"). To access or use the Services, you must be 18 years or older and have the requisite power and authority to enter into these Terms, including on behalf of your organization if you use the Services for its benefit. If you do not accept these Terms, do not register for or use the Services.

If you are located within the People's Republic of China (including Hong Kong), a separate set of Terms of Use apply to you. Any claim, dispute or controversy of whatever nature between you and Life arising out of or relating to these Terms or the Services will be resolved by final and binding arbitration in accordance with Section 16 below. Please print these Terms for your records.

1. DEFINITIONS

A. Parties

"**You**" and "**your**" refer to you, the user of the Services. A "**user**" is someone who registers for, accesses, browses, crawls, scrapes, or in any way uses the Services. If your organization has authorized or otherwise permits you to access or use the Services for its benefit, "**you**" also includes your organization.

"**We**", "**us**" and "**our**" refer to Life.

B. Services

"**Services**" includes any component of, and any one of, Life's proprietary infrastructure, platform, software, applications and services.

C. Laws

"**HIPAA**" means the Health Insurance Portability and Accountability Act of 1996, as updated and amended by Subtitle D of the Health Information Technology for Economic and Clinical Health Act.

"**GDPR**" means the European Union General Data Protection Regulation (2016/679) ("**GDPR**").

D. Data

"**Personal Data**" means any information relating to an identified or identifiable individual.

"**Protected Health Information**" shall have the same meaning as under HIPAA.

"**Uploaded Data**" means information that you upload to the Services, other than User Data.

"**User Data**" means information relating to you, in your capacity as the individual user of the Services.

2. CHANGES TO THE TERMS OF USE

We may modify these Terms from time to time. The most current version of these Terms will be located here. You understand and agree that these Terms govern your access to or use of the Services effective as of your access to or use of the Services. If we make changes to these Terms, we will notify you, but you should revisit these terms on a regular basis as revised versions will be binding on you. Any such revisions will be effective upon our posting

of new Terms. You understand and agree that your continued access to or use of the Services after the effective date of revisions to the Terms indicates your acceptance of the revisions.

3. DATA AND PRIVACY

A. Privacy Policy

The following statement does not apply if you are located in the European Economic Area or Switzerland. By accessing or using the Services, you consent to our use of your User Data as described in our Privacy Policy (available at www.lifetechnologies.com/privacy-policy.html).

B. Do Not Upload Personal Data Except As Permitted

Life makes available via its proprietary platform two types of applications: (1) Research-Use Only Apps; and (2) Multipurpose Apps. Which applications are Research-Use Only Apps and which applications are Multipurpose Apps will be clearly indicated on the platform.

(1) Research-Use Only Apps

If you are a covered entity or business associate, as defined under HIPAA, you are prohibited from uploading any Protected Health Information to Research-Use Only Apps.

Whether or not you are a covered entity or business associate, as defined under HIPAA, you are prohibited from uploading Personal Data to Research-Use Only Apps. For the avoidance of doubt, you may upload genetic data and data relating to an individual's blood and tissue samples to Research-Use Only Apps provided that you comply with these Terms and do not also upload any identifiers that could be used to identify the individual to whom such data relates, including, but not limited to, name, address, contact information, social security number, government ID number, medical record number, full-face photograph or a similar image, any elements of dates (except year) for dates that are directly related to the individual, the age of any individual over 89, or any other unique identifying characteristic or code, unless: (i) the characteristic or code is not derived in any way from an identifier of the individual; (ii) you do not disclose such characteristic or code to any other party, including Life; and (iii) you do not use the characteristic or code for any purpose other than to re-identify the individual.

(2) Multipurpose Apps

You are permitted to upload Personal Data to Multipurpose Apps, subject to these Terms.

C. Your Warranties regarding Uploaded Data and User Data

You represent and warrant to us that: (i) you have all necessary rights and permissions to upload any and all Uploaded Data to the Services; (ii) you only provide us with accurate and truthful User Data; and (iii) your and our use of Uploaded Data as contemplated in these Terms will not violate any applicable law or any contract or obligation to which you are bound, and will not infringe or misappropriate the intellectual property rights, privacy rights, or any other right of any person.

D. Our Use of Uploaded Data

We and our service providers will only use Uploaded Data on your behalf to provide the Services or else as permitted or required by applicable law. In accordance with applicable laws, we and our service providers may monitor the Services and collect data regarding your use of the Services and the performance and operation of the Services, and use such data to provide support to users, detect and address threats to the functionality, security, integrity and availability of the Services, detect and address violations of these Terms, and improve the Services and other Life services.

You hereby grant to us and our service providers a worldwide, royalty-free, fully-paid, non-exclusive, transferable, sublicensable license to copy, modify, publicly display and distribute Uploaded Data in furtherance of the purposes stated in these Terms. This license ends when Uploaded Data is no longer stored within our Services.

E. Other Users

Our Services allow you to transmit Uploaded Data to other registered users of the Services ("**Other Users**"). When you transfer Uploaded Data to an Other User, you acknowledge that you will no longer have control over that data. For example, an Other User may copy, download, modify, store, use and further transfer that information, even if you have changed that information, changed your sharing settings, or later remove that information. If you permit an Other User to transmit such user's data to you through the Services ("**Other User Data**"), you are responsible and liable for your use of Other User Data, and you must use the Other User Data in accordance with these Terms and in accordance with all applicable laws. We will have no obligation or responsibility for your use of Other User Data. Your interactions with Other Users are solely between you and them, and we will not be responsible or liable for any loss or claim relating to such dealings or with respect to any other person's or entity's use or disclosure of Uploaded Data. If there is a dispute between you and an Other User, you will manage any such dispute or disagreement directly, and you agree not to bring any proceedings against us with respect to these dealings.

F. Business Associate Agreement

The Business Associate Agreement attached at **Appendix A** shall form part of these Terms and govern your disclosure and our use of any Protected Health Information that you upload to the Services if and to the extent that: (i) you are a covered entity and we are a business associate, as these terms are defined under HIPAA; and (ii) you and we are required to enter into a business associate agreement pursuant to HIPAA.

G. European Data Processing Terms

The data processing terms attached at **Appendix B** shall form part of these Terms and govern your disclosure and our use of Personal Data (other than User Data) that you upload to the Services if and to the extent that: (i) the Personal Data relates to individuals in the European Economic Area; and (ii) the GDPR applies to your disclosure of such Personal Data to us.

4. GRANT OF RIGHTS; ACCOUNTS

A. Limited License

Subject to these Terms, we grant you a limited, nonexclusive, non-sublicensable, non-transferable right to access and use our Services, and any associated or supporting content or data, hardware, user manuals or other documentation related to the Services (including without limitation associated sample files or programs, media, printed materials, patches, upgrades, utilities, tools, and/or "online" or electronic documentation) ("**Associated Materials**"). You may use the Services and Associated Materials solely for your private or business purposes and, if you are an organization or entity, only your authorized employees and agents may use the Services and Associated Materials. If certain Services use registration codes, access to the number of licensed copies of such Services is controlled by the relevant registration codes. For example, if you have a registration code that enables you to use three copies of an application on the Services simultaneously, you may not install more than three separate instances of such application.

B. Account and Login

If you registered for the Services as an individual, you must establish a unique user ID and associated password ("**Login Credentials**") to gain access to and use the Services. If you have registered an account for the Services on behalf of an organization, each member of your organization who wishes to use the Services must register separately for the Services and establish Login Credentials unique to him or her. You are fully responsible for maintaining the confidentiality of your User Data and Login Credentials, and fully responsible and liable for any and all activity that occurs under your account as a result of your failing to keep this information confidential. If your User Data changes, you must update it promptly. You are prohibited from using the Login Credentials or account of another user of the Services unless we have provided our express written consent in advance. Multiple accounts

held by the same individual are subject to termination by us. If we have reason to believe that the User Data you provide to us is untrue, inaccurate, out-of-date or incomplete, we may suspend or terminate your account.

5. RESTRICTIONS ON YOUR USE OF THE SERVICES AND ASSOCIATED MATERIALS

You shall not use or allow the use of the Services or Associated Materials:

(i) for any illegal, unlawful or malicious purpose or activity;

(ii) for activities that we deem improper for any reason whatsoever in our sole discretion;

(iii) for rental or in the operation of a service bureau, including without limitation, providing third party hosting, or third party application integration or application provider services;

(iv) by persons who are not employees or contractors of yours or the organization on whose behalf you have accepted these Terms;

(v) as essential equipment in the operation of any nuclear facility, aircraft navigation or communication systems or air traffic control machines;

(vi) for any use in which failure of the Services could lead to death, personal injury or severe physical or environmental damage;

(vii) as, or in substitution of, medical advice;

(viii) for the purpose, in whole or in part, of building a solution that would compete with the Services or to assist another person in building such a solution;

(ix) to defame, abuse, harass, stalk, intimidate, bully, threaten or otherwise violate the rights of others, including without limitation others' privacy rights or rights of publicity;

(x) to send or otherwise post unauthorized commercial communications (such as spam); or

(xi) upload content that is hateful, threatening, or pornographic, incites violence, or contains nudity or graphic or gratuitous violence.

You shall not:

(i) download any open source software to the Services;

(ii) modify, adapt, sublicense, translate, sell, reverse engineer, decompile or disassemble any portion of the Services;

(iii) remove any proprietary, copyright, trade secret or warning legend from the Services or Associated Materials;

(iv) impersonate any person or entity, falsely state or otherwise misrepresent your affiliation with any person or entity, or use or provide any fraudulent, misleading or inaccurate information, in connection with the Services;

(v) access or use (or attempt to access or use) another user's account without permission, or solicit another user's Login Credentials;

(vi) transmit to us or our service providers, or transmit via the Services, any software or materials that contain any viruses, worms, Trojan horses, defects, or other items of a destructive nature;

(vii) "frame" or "mirror" the Services;

(viii) use any robot, spider, site search/retrieval application or other manual or automatic device or process to retrieve, index, "data mine" or in any way reproduce or circumvent the navigational structure or presentation of the Services;

(ix) harvest or collect information about or from other users of the Services (except as otherwise permitted herein);

(x) probe, scan or test the vulnerability of the Service, or breach the security or authentication measures on the Service, monitor data or traffic on the Service, or take any action that imposes an unreasonable or disproportionately large load on the infrastructure of the Service, such as a denial of service attack; or

(xi) violate the Amazon Web Services Acceptable Use Policy found at http://aws.amazon.com/aup/.

If a component of the Services requires you to use such component, and data generated by such component, for the sole purpose of review and analysis of data generated by Life instruments, you agree to do so. The components subject to this requirement will be clearly identified on the platform.

We may review your use of the Services for the purposes of determining whether you have complied with these Terms. Any such review shall be conducted during regular business hours at your facilities or through a remote monitoring/connectivity application and shall not unreasonably interfere with your business activities.

We may take preventative or corrective actions relating to your use of the Services to protect Life, our affiliates, licensors, partners, suppliers and users.

6. TERM AND TERMINATION

A. Subscription Term

We offer subscription terms of varying lengths, and the term during which you may use the Services will either: (i) depend on the length of subscription that you have purchased or (ii) be at our sole discretion if we provide the Services free of charge. At the expiration of your subscription term, these Terms will terminate. If your access to the Services is granted on a trial basis, you are hereby notified that license management software may be included to automatically cause the Services to cease functioning at the end of the trial period (and in any case you agree to discontinue usage at the end of the trial period or at our written request).

B. Termination

You may terminate these Terms by closing your account. We may terminate your access to the Services if you do not comply with these Terms. We reserve the right to discontinue the Services and/or close your account in our sole discretion upon at least ninety (90) days' notice to you, during which time we will make available Uploaded Data, as it exists at that time, to you for download.

C. Effect of Termination

Upon termination of your use of the Services or of these Terms, you must discontinue using the Services and Associated Materials. Upon discontinuation or termination of the Services, you will no longer have rights to access or use the Services or Uploaded Data, and except as may be required by law, we will delete Uploaded Data or otherwise render it inaccessible. Sections 2, 3, 5, 6(C), 8, 10, 11, 12, 13, 14, 15 and 16, the attached Business Associate Agreement and Data Processing Terms, if they apply to us, and any other provisions and terms that by their nature extend beyond termination, shall survive the termination or expiration of these Terms.

7. THIRD PARTY APPLICATIONS

The Services may, from time to time, make Life or third-party software applications available to you through use of the Services ("**App(s)**"). If you elect to download an App, then you may need to agree to separate terms and conditions governing your use of the App. Apps are provided solely as a convenience to you. Third-party Apps are not under our control, and we are not responsible for and do not endorse the content or functions of third party Apps, and you must exercise independent judgment regarding your interaction with all Apps. You should review all terms and policies governing Apps, including privacy and data gathering practices, and should make whatever investigation you feel necessary or appropriate before downloading or using any Apps.

8. CONFIDENTIAL INFORMATION

You agree to protect our Confidential Information with the same degree of care used to protect your own confidential information (but in no event less than a reasonable standard of care), and not to use or disclose any portion of such Confidential Information to third parties, except as expressly authorized in these Terms. You acknowledge that the Services and Associated Materials, including their content, structure, organization and design constitute proprietary and valuable trade secrets (and other intellectual property rights) of Life and/or our licensors. The term "**Confidential Information**" means, collectively, non-public information that we (and our licensors) provide and

reasonably consider to be of a confidential, proprietary or trade secret nature, including but not limited to confidential elements of the Services and Associated Materials, and our or our licensors' technology and know-how, whether in tangible or intangible form, whether designated as confidential or not, and whether or not stored, compiled or memorialized physically, electronically, graphically, photographically, or in writing. Confidential Information does not include any information which you can demonstrate by credible evidence: (a) is, as of the time of its disclosure, or thereafter becomes part of the public domain through no fault of yours; (b) was rightfully known to you prior to the time of its disclosure, or to have been independently developed by you without use of Confidential Information; and/or (c) is subsequently learned from a third party not under a confidentiality obligation with respect to such Confidential Information. Confidential Information that is required to be disclosed by you pursuant to a duly authorized subpoena, court order, or government authority shall continue to be Confidential Information for all other purposes and you agree, prior to disclosing pursuant to a subpoena, court order, or government authority, to provide prompt written notice and assistance to us prior to such disclosure, so that we may seek a protective order or other appropriate remedy to protect against disclosure.

9. FEES

If you have registered to use the Services in exchange for the payment of fees, then you must pay those fees in accordance with the terms of your registration. All fees are nonrefundable, and if you do not pay fees when due then we may, without limiting our other available remedies, suspend your access to the Services until all overdue payments are received, or terminate these Terms and close your account.

10. OWNERSHIP; INTELLECTUAL PROPERTY

A. Ownership

You acknowledge that the Associated Materials and the Services (including their structure, sequence, organization, text, graphics, user interfaces, visual interfaces, photographs, trademarks, logos, sounds, artwork and computer code, including but not limited to the design, structure, "look and feel" and arrangement of the content of the Services), are owned, controlled or licensed by or to us, is and remains the proprietary information of Life and our affiliates, suppliers and licensors, and are protected by intellectual property laws. You acknowledge that all intellectual property rights relating to the Services (other than Uploaded Data and User Data) and the Associated Materials are, as between you and Life, solely and exclusively owned by Life. All modifications, enhancements or changes to the Services and the Associated Materials are and shall remain the property of Life and our licensors and suppliers, without regard to the origin of such modifications, enhancements or changes. No ownership rights in the Services or Associated Materials are granted, and we reserve all right, title and interest therein and thereto. Use of the Services does not grant you a license to intellectual property or other rights of Life or its affiliates or licensors or any third parties, whether express, implied, by estoppel or otherwise, or grant you the right to make or have made any products, or to use the Services or Associated Materials beyond the scope of these Terms. You will not challenge the ownership or rights in and to the Services and the Associated Materials, including without limitation all copyrights and other proprietary rights. Nothing in these Terms limits our ability to enforce our intellectual property rights.

B. Feedback

If you have comments regarding the Services or ideas on how to improve them ("**Feedback**"), please note that by doing so, you also assign, and hereby assign, all right, title, and interest worldwide in Feedback to Life and agree to assist Life, at Life's expense, in perfecting and enforcing Life's rights thereto and ownership thereof. You acknowledge and agree that Life may use and incorporate Feedback into the Services or for other business purposes without compensation and without restriction.

11. DISCLAIMERS

TO THE MAXIMUM EXTENT PERMITTED UNDER APPLICABLE LAW, THE SERVICES, ASSOCIATED MATERIALS AND ANY SUPPORT AND INFORMATION PROVIDED BY US IN CONNECTION WITH THE

SERVICES, ARE PROVIDED “AS IS” AND ON AN “AS AVAILABLE BASIS” “WITH ALL FAULTS” AND WITHOUT WARRANTY OF ANY KIND.

TO THE FULLEST EXTENT PERMITTED BY LAW, LIFE, ITS AFFILIATES, SERVICE PROVIDERS, AGENTS, PARTNERS AND LICENSORS DISCLAIM ALL WARRANTIES AND REPRESENTATIONS OF ANY KIND, WHETHER EXPRESS, IMPLIED, OR STATUTORY, INCLUDING BUT NOT LIMITED TO ANY IMPLIED OR OTHER WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE, NON-INFRINGEMENT OR NON-MISAPPROPRIATION OF INTELLECTUAL PROPERTY OR PROPRIETARY RIGHTS OF A THIRD PARTY, CUSTOM, TRADE, QUIET ENJOYMENT, ACCURACY OF INFORMATIONAL CONTENT, OR SYSTEM INTEGRATION. NO WARRANTY IS MADE THAT THE SERVICES WILL BE OPERABLE OR ACCESSIBLE, OPERATE IN AN ERROR FREE, BUG FREE, UNINTERRUPTED OR SECURE MANNER, IN COMBINATION WITH THIRD PARTY HARDWARE OR SOFTWARE PRODUCTS, OR THAT OUR SECURITY PROCEDURES AND MECHANISMS WILL PREVENT LOSS OR ALTERATION OF OR IMPROPER ACCESS TO YOUR INFORMATION OR DATA.

YOU ACKNOWLEDGE THAT WE HAVE NO CONTROL OVER THE SPECIFIC CONDITIONS UNDER WHICH YOU USE THE SERVICES. LIFE CANNOT AND DOES NOT WARRANT THE PERFORMANCE OF THE SERVICES OR RESULTS THAT MAY BE OBTAINED BY THE USE OF THE SERVICES. THE SERVICES AND ANY SUPPORT OFFERED BY US DOES NOT REPLACE YOUR OBLIGATION TO EXERCISE YOUR INDEPENDENT JUDGMENT IN USING THE SERVICES.

Certain states and/or jurisdictions do not allow certain warranty disclaimers, in which case certain disclaimers in this Section 11 may not apply to you.

12. LIMITATIONS OF LIABILITY

A. Limitation of Liability

TO THE FULLEST EXTENT ALLOWED BY LAW, IN NO EVENT SHALL LIFE OR ITS AFFILIATES, SUPPLIERS OR LICENSORS BE LIABLE, WHETHER IN CONTRACT, TORT, WARRANTY, OR UNDER ANY STATUTE (INCLUDING WITHOUT LIMITATION ANY TRADE PRACTICE, UNFAIR COMPETITION OR OTHER STATUTE OR REGULATION OF SIMILAR IMPORT) OR ON ANY OTHER BASIS FOR SPECIAL, INCIDENTAL, INDIRECT, PUNITIVE, MULTIPLE OR CONSEQUENTIAL DAMAGES SUSTAINED BY YOU OR ANY OTHER PERSON OR ENTITY, WHETHER OR NOT FORESEEABLE AND WHETHER OR NOT LIFE IS ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, INCLUDING WITHOUT LIMITATION DAMAGES ARISING FROM OR RELATED TO THE SERVICES, ASSOCIATED MATERIALS, LOSS OF USE, LOSS OF DATA, DOWNTIME, OR FOR LOSS OF REVENUE, PROFITS, GOODWILL, OR BUSINESS OR OTHER FINANCIAL LOSS.

B. Damage Cap

IN ANY CASE, THE ENTIRE LIABILITY OF LIFE AND ITS AFFILIATES, SUPPLIERS AND LICENSORS UNDER THESE TERMS, OR ARISING OUT OF THE SERVICES, SHALL NOT EXCEED THE AMOUNTS ACTUALLY PAID BY YOU FOR THE SERVICE DURING THE THREE (3) MONTHS IMMEDIATELY PRECEDING THE CAUSE OF ACTION.

C. Acknowledgement

You agree that the limitations of liability set forth in this Section 12 shall be effective despite any failure of consideration or of an exclusive remedy. You acknowledge that the Services fees (if any) have been set and these Terms are accepted by Life in reliance upon these limitations of liability and that these limitations form an essential basis of the bargain between the parties. Certain states and/or jurisdictions do not allow the limitation of liability for incidental, consequential or certain other types of damages, so certain exclusions and limitations set forth in this Section 12 may not apply to you.

13. INDEMNITY

If a third party makes a claim against Life or its directors, officers, shareholders, proprietors, partners, employees, agents, representatives, servants, attorneys, predecessors, successors or assigns, or those of its affiliates ("**Life Parties**") related to your use of the Service, your contravention of these Terms, your use of Other User Data, or your provision to us of any Uploaded Data or User Data, then you will indemnify and hold Life Parties harmless from and against any and all claims, losses, damages, liabilities, costs and expenses (including reasonable attorneys' fees and other costs of defending and/or settling any proceeding) that such Life Parties may suffer or incur as a result of the claim. You will defend such claim, at your expense, if instructed by us.

14. U.S. GOVERNMENT END USERS

The Services and Associated Materials are copyright protected Commercial Computer Software and Computer Software Documentation as those terms are defined in 48 C.F.R. 2.101. The Government shall obtain only those rights to the Services and Associated Materials as are authorized by 48 C.F.R. 12.212 or 48 C.F.R. 227.7202-3, as applicable. Any use, modification, reproduction, release, performance, display or disclosure of the Services and Associated Materials by the U.S. Government shall be governed solely by these Terms.

15. EXPORT RESTRICTIONS

You agree to adhere to all applicable export control laws and regulations with respect to your use of the Service, and you will not export or re-export or permit access to the Services or Associated Materials, in whole or in part, directly or indirectly, to any country to which such export or re-export is restricted by any laws or regulations of the U.S. or the country in which you obtained the Services or Associated Materials, or unless properly authorized by the U.S. Government or other applicable regulatory authority as provided by law or regulation. You represent that you are not named on any U.S. or other applicable government denied-party list.

16. ARBITRATION

A. Arbitration

Any claim or cause of action arising out of, related to or connected with these Terms or the Services that cannot be resolved through negotiation and settlement (a "**Dispute**") may only be heard by an arbitrator pursuant to binding arbitration as described in this Section 16. Arbitration shall be conducted by and submitted to a single arbitrator ("**Arbitrator**") selected from and administered by the San Diego office of JAMS in accordance with its then-existing Comprehensive Arbitration Rules & Procedures, and you consent to this as the sole and exclusive venue and jurisdiction for resolving Disputes. The Arbitrator may award compensatory damages, but may not award non-economic damages, such as for emotional distress, or pain and suffering or punitive or indirect, incidental or consequential damages. Each party shall bear its own attorneys' fees, cost and disbursements arising out of the arbitration, and shall pay an equal share of the fees and costs of the Arbitrator and JAMS; however, the Arbitrator may award to the prevailing party reimbursement of its reasonable attorneys' fees and costs (including, for example, expert witness fees and travel expenses), and/or the fees and costs of the Arbitrator. Within fifteen (15) calendar days after conclusion of the arbitration, the Arbitrator shall issue a written award and a written statement of decision describing the material factual findings and conclusions on which the award is based, including the calculation of any damages awarded. Judgment on the award may be entered by any court of competent jurisdiction.

B. Restrictions

To the fullest extent permitted by applicable law, no arbitration under these Terms shall be joined to an arbitration involving any other party, whether through class action proceedings or otherwise. Also, regardless of any statute or law to the contrary, any Dispute must be filed within one (1) year after such claim or cause of action arose or be forever banned.

C. Acknowledgement

By agreeing to this binding arbitration provision, you understand that you are waiving certain rights and protections which may otherwise be available if a claim or dispute were determined by litigation in court, including, without limitation, the right to seek or obtain certain types of damages precluded by this

arbitration provision, the right to a jury trial, certain rights of appeal, the right to bring a claim as a class member in any purported class or representative proceeding, and the right to invoke formal rules of procedure and evidence.

D. Injunctive Relief

Notwithstanding Section 16(A), if you infringe or threaten to infringe our intellectual property rights, we may seek injunctive or other appropriate relief in any court having jurisdiction, and you hereby consent to, and waive all defenses of lack of personal jurisdiction and forum non conveniens with respect to venue and jurisdiction in such courts.

17. MISCELLANEOUS

A. Governing Law

These Terms shall be governed by the internal substantive laws of the State of California, without respect to any conflict of laws principles that would dictate a different body of law. The United Nations Convention on the International Sale of Goods is excluded from these Terms.

B. Severability

If any provision of these Terms shall be deemed unlawful, void, or for any reason unenforceable, then that provision shall be deemed severable from these Terms and shall not affect the validity and enforceability of any remaining provisions.

C. Waiver

No waiver of any term or condition of these Terms shall be deemed a further or continuing waiver of such term or any other term, and our failure to assert any right or provision under these Terms shall not constitute a waiver of such right or provision.

D. Entire Agreement

These Terms contain the entire agreement between you and Life with respect to the subject matter hereof and supersede all prior or other agreements between you and Life concerning this subject matter.

E. Order of Precedence

These Terms and the attached Business Associate Agreement and Data Processing Terms, if they apply to us, shall prevail notwithstanding any different, conflicting, or additional terms or conditions which may appear in any purchase order or other document submitted by you, and such additional or inconsistent terms are deemed rejected by us.

F. Binding Effect; Assignment

You may not sublicense, assign or transfer your rights to use the Service, in whole or in part, without our prior consent. Any attempted assignment or sublicense without such consent shall be void. We may assign these Terms (including your user registration), without your consent in connection with a merger, acquisition, corporate reorganization, or sale of all or substantially all of our assets, or to an affiliate or partner, or in connection with a change in control. These Terms are binding upon the parties' successors and permitted assigns.

G. European Union End Users

If the Services are used within a Member State of the European Union, nothing in this Agreement shall be construed as restricting any rights available under Directive 2009/24/EC of the European Parliament and of the Council of 23 April 2009 on the legal protection of computer programs.

H. Language; Headings

The controlling language of these Terms, and any proceedings relating to these Terms, shall be English. You agree to bear any and all costs of translation, if necessary. The headings to the sections of these Terms are used for convenience only and shall have no substantive meaning.

I. Notices

All notices and consents made hereunder shall be in writing and shall be deemed to have been given upon: (i) personal delivery, (ii) the second business day after sending by confirmed facsimile, or (iii) the first business day after sending by email. Notices to Life must be sent in writing to the following address: Life Technologies Corporation, 5791 Van Allen Way, Carlsbad, CA 92008, Attention: Legal Department, and notices to you will be sent to the latest email address you provide to us.

[Appendix A begins on the next page]

APPENDIX A - BUSINESS ASSOCIATE AGREEMENT

You are prohibited from uploading any Protected Health Information to Research Use Only Apps.

This Business Associate Agreement ("**BAA**") constitutes a binding agreement between you and us only if and to the extent that: (i) you upload any Protected Health Information to the Services (*i.e.*, Multipurpose Apps); (ii) you are a covered entity and we are a business associate, as these terms are defined in HIPAA; and (iii) you and we are required to enter into a business associate agreement pursuant to HIPAA.

WHEREAS, pursuant to HIPAA, you are a covered entity under HIPAA and we may from time to time act as a business associate under HIPAA in the performance of Services for you;

WHEREAS, it may be necessary for you to disclose certain information ("**Information**") to us for our performance of Services for you, some of which may constitute Protected Health Information under HIPAA; and

WHEREAS, the parties wish to enter into this BAA to address the requirements of HIPAA; and

WHEREAS, this BAA applies with respect to any and all Protected Health Information that may be collected, accessed, used, processed or disclosed pursuant to our performance of Services for you;

WHEREAS, pursuant to this BAA, the parties agree to access, use, process and disclose any such Protected Health Information in compliance with the requirements of HIPAA;

NOW THEREFORE, in consideration of the mutual promises contained herein and the exchange of information pursuant to the Terms, the parties agree as follows:

1. Definitions

Capitalized terms not defined in this BAA shall be defined as provided in the Terms or HIPAA.

2. Uses and Disclosures of Protected Health Information

2.1. You may from time to time disclose Protected Health Information to us in order for us to perform the Services. For purposes of this BAA, "Protected Health Information" is limited to Protected Health Information that is accessed, used, processed or disclosed pursuant to your use and our provision of the Services.

2.2. Notwithstanding Section 2.1 of this BAA, you will disclose to us only the minimum amount of Protected Health Information reasonably necessary to accomplish the intended purpose of your use of the Services. If practicable, you will use commercially reasonable efforts (i) to de-identify any and all Protected Health Information before providing such information to us, or (ii) to provide a Limited Data Set of such information. For the avoidance of doubt, information which has been de-identified according to the standards set forth in Section 164.514 of Title 45 of the U.S. Code of Federal Regulations does not constitute Protected Health Information and is not subject to the terms of this BAA.

2.3. We may only use the Protected Health Information we receive from you to provide the Services to you, for the proper management and administration of our organization, and to otherwise carry out our legal responsibilities; provided, however, that in all cases such use is permitted under applicable law.

2.4. We may disclose Protected Health Information if the disclosure is required by law. We may also disclose Protected Health Information for the proper management and administration of our business, provided we obtain reasonable assurances from the person to whom the information is disclosed that (i) such Protected Health Information will be held confidentially and used or further disclosed only as required by law and for the purpose for which such Protected Health Information was disclosed, and (ii) such person will notify us of any instances in which such person becomes aware of any breaches to the confidentiality of such Protected Health Information.

2.5. Neither party shall use or disclose such Protected Health Information for any purpose other than as permitted or required under this BAA or as required by law.

3. Safeguards and Subcontracting

3.1. We shall maintain appropriate safeguards including, but not limited to, administrative, physical and technical safeguards that reasonably and appropriately protect the confidentiality, integrity and availability of the Protected Health Information in accordance with Subpart C (Security Standards for the Protection

of Electronic Protected Health Information) of 45 C.F.R. § 164 to prevent use or disclosure of such Protected Health Information other than as provided in this BAA.

3.2. With respect to any Subcontractor or agent to whom we provide Protected Health Information, we shall first contractually obligate such Subcontractor or agent to agree to protect such Protected Health Information pursuant to terms and conditions at least as protective as the terms of this BAA.

4. Unauthorized Use or Disclosure

If we become aware of any unauthorized acquisition, access, use or disclosure of unsecured Protected Health Information in a manner not permitted under Subpart E (Privacy of Individually Identifiable Health Information) of 45 C.F.R. § 164 which compromises the security or privacy of the Protected Health Information as prescribed in HIPAA ("**Breach**"), we shall notify you in accordance with HIPAA. The parties agree to cooperate with respect to any required notifications that must be made to the individuals or the media with respect to any such Breach.

5. Designated Record Sets

5.1. Unless otherwise explicitly stated in the terms relating to the Services, the parties do not intend for us to maintain any Protected Health Information in a Designated Record Set for you. You agree to provide us only copies of Protected Health Information and to retain all original documents, and that we maintain no unique records in any Designated Record Set.

5.2. To the extent we maintain a Designated Record Set on your behalf and to the extent we maintain the only copy of Protected Health Information, we agree as follows:

5.2.1. We shall provide access, at your written request, Protected Health Information in a Designated Record Set, to your or, as directed by you, to an Individual to meet the requirements under 45 C.F.R. § 164.524.

5.2.2. Upon receipt of a written request by you, we shall make any amendment(s) to Protected Health Information in a Designated Record Set that you direct or agree to, pursuant to 45 C.F.R. § 164.526.

6. Obligations of Covered Entity

6.1. You shall notify us of any limitation(s) in your notice of privacy practices in accordance with 45 C.F.R. § 164.520, to the extent that such limitation may affect our use or disclosure of Protected Health Information in accordance with this BAA. We agree to comply with such limitations communicated by you.

6.2. You shall notify us of any changes in, or revocation of, permission by an Individual to use or disclose Protected Health Information, to the extent that such changes may affect our use or disclosure of Protected Health Information in accordance with this BAA. We agree to comply with such changes in, or revocation of, permission communicated by you.

6.3. You shall notify us of any restriction on the use or disclosure of Protected Health Information that you have agreed to in accordance with 45 C.F.R. § 164.522, to the extent that such restriction may affect our use or disclosure of Protected Health Information in accordance with this BAA. We shall comply with any such restrictions communicated by you.

7. Compliance with Law

7.1. Each party is responsible for its own compliance with any and all existing or subsequent laws, whether by statute, regulation, common law, or otherwise, related to its acquisition, access, use or disclosure of Protected Health Information. You agree that you shall have and maintain appropriate consents from data subjects, as may be necessary, for us to acquire, access, use or disclose Protected Health Information in accordance with its provision of Services and as otherwise permitted under this BAA.

7.2. Upon request by the Department of Health and Human Services ("HHS"), we shall make available to HHS our internal practices, books, and records relating to the use and disclosure of Protected Health Information for purposes of ensuring compliance with the provisions of HIPAA.

7.3. In the event that we receive an inquiry from an individual for access to or the right to amend Protected Health Information, we shall advise you of that communication and the request. The parties shall cooperate in making Protected Health Information available to the individual and in making the requested amendment of Protected Health Information. You shall retain and make available on request information required to provide an accounting of disclosures in accordance with the provisions of HIPAA.

8. Default, Termination

8.1. In the event that either party reasonably determines that the other has acquired, accessed, used or disclosed unsecured Protected Health Information in a manner inconsistent with a material term of this BAA, such party shall provide written notice of such breach to the other party and specify in reasonable detail any such breach. Upon receipt of such written notice, the receiving party shall have 30 days to

achieve compliance with this BAA or to establish a reasonable schedule for compliance with this BAA. In the event that a party fails or refuses to comply with this obligation, the other party may terminate the BAA upon written notice. If either party reasonably determines that the other party has acquired, accessed, used or disclosed Protected Health Information in a manner inconsistent with this BAA following written notice of a prior breach, the non-breaching party may immediately terminate this BAA.

8.2. Upon termination of this BAA for any reason, we, with respect to Protected Health Information received from you, or created, maintained, or received by us on your behalf in connection with your use and our provision of the Services, shall:

8.2.1. Retain only that Protected Health Information which is necessary for us to continue the proper management and administration of our organization or to carry out our legal responsibilities;

8.2.2. Destroy the remaining Protected Health Information that we still maintain in any form;

8.2.3. Continue to use appropriate safeguards and comply with Subpart C of 45 CFR Part 164 with respect to electronic Protected Health Information to prevent use or disclosure of the Protected Health Information, other than as provided for in this Section, for as long as we retain the Protected Health Information;

8.2.4. Not use or disclose the Protected Health Information retained by us other than for the purposes for which such Protected Health Information was retained and subject to the same conditions set out in this BAA which applied prior to termination; and

8.2.5. Destroy the Protected Health Information retained by us when it is no longer needed by us for the proper management and administration of our organization or to carry out our legal responsibilities.

9. Limitation of Liability/Indemnity

9.1. UNDER NO CIRCUMSTANCES WILL LIFE PARTIES (as defined in Section 13 of the Terms) BE LIABLE FOR ANY INDIRECT, INCIDENTAL, SPECIAL, PUNITIVE, EXEMPLARY OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, LOST PROFITS AND DAMAGES THAT RESULT FROM INCONVENIENCE, DELAY, OR LOSS OF USE) ARISING OUT OF ITS ACCESS TO OR USE, PROCESSING OR DISCLOSURE OF PROTECTED HEALTH INFORMATION, EVEN IF IT OR THEY HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. Some states do not allow the exclusion or limitation of liability for consequential or incidental damages; thus, certain parts of this limitation may not be applicable.

9.2. You will defend, indemnify, and hold Life Parties harmless from and against any and all claims, proceedings, damages, injuries, liabilities, losses, costs and expenses (including reasonable attorneys' fees and litigation expenses), relating to or arising from your: (i) unauthorized access to or use, processing or disclosure of Protected Health Information; (ii) breach of this BAA; or (iii) violation of applicable law.

10. Miscellaneous

10.1. **Governing Law and Venue Selection.** Regardless of the jurisdiction in which you reside, this BAA is made in the State of California, and will be construed and enforced in accordance with the law of the State of California (without regard to its provisions governing conflicts of law), as applied to agreements entered into and completely performed in the State of California. ANY ACTION ARISING OUT OF THIS BAA OR ANY ACTION TO ENFORCE THIS BAA WILL BE RESOLVED IN ACCORDANCE WITH THE THERMO FISHER CLOUD SOFTWARE TERMS OF USE.

10.2. **Amendments.** This BAA may not be modified, nor shall any provisions hereof be waived or amended, except in a writing duly signed by authorized representatives of the parties. The parties agree to take such action as is necessary to amend this BAA from time to time to comply with the requirements of HIPAA or other applicable laws relating to the privacy or security of Protected Health Information. Notwithstanding the foregoing, to the extent that any provision of this BAA is in conflict with any law, regulation, rule, or administrative policy of any governmental entity, this BAA will have been deemed to have been amended in order to bring it into conformity with these provisions.

10.3. **Interpretation.** This BAA shall be construed as broadly as necessary to implement and comply with HIPAA. The parties agree that any ambiguity in this BAA shall be resolved in favor of a meaning that complies and is consistent with HIPAA.

APPENDIX B - DATA PROCESSING TERMS

You are prohibited from uploading Personal Data to Research-Use Only Apps. For the avoidance of doubt, you may upload genetic data and data relating to an individual's blood and tissue samples to Research-Use Only Apps provided that you comply with these Terms and do not also upload any identifiers that could be used to identify the individual to whom such data relates, including, but not limited to, name, address, contact information, social security number, government ID number, medical record number, full-face photograph or a similar image, any elements of dates (except year) for dates that are directly related to the individual, the age of any individual over 89, or any other unique identifying characteristic or code, unless: (i) the characteristic or code is not derived in any way from an identifier of the individual; (ii) you do not disclose such characteristic or code to any other party, including Life; and (iii) you do not use the characteristic or code for any purpose other than to re-identify the individual.

These Data Processing Terms constitute a binding agreement between you and us only if and to the extent that: (i) you upload any Personal Data to the Services; and (ii) the GDPR requires that you and we enter into certain data processing terms that comply with Article 28 of the GDPR.

WHEREAS, Life provides Services to you and/or your affiliates and may receive custody or store, process or gain access to personal data related to your individual contacts or those of its affiliates, as further described in Appendix 1 hereto.

WHEREAS, you are required to conclude certain data processing terms with us to satisfy the requirements of the GDPR.

NOW THEREFORE, in consideration of the foregoing and other valuable consideration, receipt and adequacy of which is hereby acknowledged, You, as "**data exporter**", and Life Technologies Corporation as "**data importer**", each a "party"; together "the parties",

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

Clause 1
Definitions

For the purposes of the Clauses:

(a) *'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject'* and *'supervisory authority'* shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;

(b) '*the data exporter'* means the controller who transfers the personal data;

(c) *'the data importer'* means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

(d) *'the subprocessor'* means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

(e) '*the applicable data protection law'* means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

(f) *'technical and organisational security measures'* means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2

Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

Clause 3

Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.
2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.
3. The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.
4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b) that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

(g) to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

(j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5

Obligations of the data importer

The data importer agrees and warrants:

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;

(d) that it will promptly notify the data exporter about:

(i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,

(ii) any accidental or unauthorised access, and

(iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(h) that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing services by the subprocessor will be carried out in accordance with Clause 11;

(j) to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter.

Clause 6

Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or subprocessor is entitled to receive compensation from the data exporter for the damage suffered.

2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity.

3. The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.

4. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the subprocessor agrees that the data subject may issue a claim against the data subprocessor with regard to its own processing operations under the Clauses as if it were the data exporter or

the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the subprocessor shall be limited to its own processing operations under the Clauses.

Clause 7

Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:
   (a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;
   (b) to refer the dispute to the courts in the Member State in which the data exporter is established.
2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8

Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.
2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.
3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

Clause 9

Governing Law

The Clauses shall be governed by the law of the Member State in which the data exporter is established.

Clause 10

Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11

Subprocessing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses. Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.
2. The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.
3. The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.
4. The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12

Obligation after the termination of personal data processing services

1. The parties agree that on the termination of the provision of data processing services, the data importer and the subprocessor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.
2. The data importer and the subprocessor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

APPENDIX 1 - DETAILS OF PROCESSING

This Appendix forms part of the Clauses and must be completed and signed by the parties

Data exporter
The data exporter is your and/or your customers or affiliates.

Data importer
The data importer is us.

Data subjects
The personal data transferred concern data subjects residing in the European Economic Area and Switzerland.

Categories of data
The personal data transferred concern the following categories of data (please specify):

- See technical specifications of the Services.

Special categories of data (if appropriate)

- See technical specifications of the Services.

Processing operations
The personal data transferred will be subject to the following basic processing activities (please specify):

- We will process personal data to provide the Services, discharge our obligations in the Terms of Use relating to the Services and comply with applicable laws.

APPENDIX 2 - TECHNICAL AND ORGANIZATIONAL SECURITY MEASURES

This Appendix forms part of the Clauses and must be completed and signed by the parties.

Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached):
This Appendix 2 describes the technical and organizational security measures that we shall, as a minimum, maintain to protect the security of the personal data processed in connection with the Services and to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems.

Access Control to Processing Areas
We shall implement suitable measures in order to prevent unauthorized individuals from gaining access to the data processing equipment used for the data processing. Where appropriate, these measures include:

- establishing security areas;
- protection and restriction of access to processing areas;
- securing the data processing equipment;
- establishing access authorizations for staff and third parties;
- regulations on key cards;
- restrictions on key cards;
- all access to the data centre where the personal data is hosted is logged, monitored, and tracked; and
- the data center where the personal data is hosted is secured by a security alarm system.

Access Control to Data Processing Systems
We shall implement adequate measures to prevent our data processing systems from being used by unauthorized persons. Where appropriate, these measures include:

- identification of the terminal and/or the terminal user to our processing systems;
- automatic time-out of user terminal if left idle, identification and password required to reopen;
- automatic turn-off of the user ID when several erroneous passwords are entered, log file of events (monitoring of break-in-attempts);
- issuing and safeguarding of identification codes;

- dedication of individual terminals and/or terminal users, identification characteristics exclusive to specific functions;
- staff policies in respect of staff members' access rights to the personal data (if any), informing staff about their obligations and the consequences of any violations of such obligations;
- all access to data content is logged, monitored, and tracked; and
- use of industry-standard encryption and pseudonymization technologies.

Access Control to Use Specific Areas of Data Processing Systems

We shall ensure that the individuals entitled to use our data processing system are only able to access the personal data within the scope and extent covered by their respective authorization and that the personal data cannot be read, copied or modified or removed without authorization. Where appropriate, these measures include:

- staff policies in respect of each staff member's access rights and responsibilities with respect to the personal data;
- allocation of individual terminals and/or terminal user, and identification characteristics exclusive to specific functions;
- monitoring capability in respect of individuals who delete, add or modify the personal data and regular monitoring and updating of authorization profiles;
- effective and measurable disciplinary action against individuals who access the personal data without authorization;
- release of personal data limited to authorized individuals;
- control of files, including the controlled and documented destruction of personal data;
- policies controlling the retention of back-up copies; and
- use of industry-standard encryption pseudonymization technologies.

Transmission Control

We shall implement adequate measures to prevent the personal data from being read, copied, altered or deleted by unauthorized parties during the transmission thereof or during the transport of the data media. Where appropriate, these measures include:

- use of industry-standard firewall and encryption and pseudonymization technologies to protect the gateways and pipelines through which the personal data travels;
- as far as possible, all data transmissions are logged, monitored and tracked; and
- monitoring of the completeness and correctness of the transfer of personal data (end-to-end check).

Input Control

We shall implement adequate measures to ensure that it is possible to check and establish whether and by whom the personal data have been put into the data processing systems or removed from such systems. Where appropriate, these measures include:

- a policy for the authorization to put personal data into memory, as well as for the reading, alteration and deletion of stored personal data;
- authentication of the authorized personnel;
- individual authentication credentials such as user IDs that, once assigned, cannot be re-assigned to another individual;
- protective measures for the personal data input into memory, as well as for the reading, alteration and deletion of stored data;
- providing that entries to data processing facilities (the rooms housing the computer hardware and related equipment) are capable of being locked;
- automatic log-off of user IDs (requirement to re-enter password to use the relevant work station) that have not been used for a significant period of time;
- automatic deactivation of user authentication credentials (such as user IDs) in case the person is no longer authorized to access the personal data or in case of non-use for a substantial period of time, except for those individuals authorized solely for technical management;
- proof of the input restrictions and authorizations by the Processor; and

- electronic recording of entries.

Availability Control

We shall implement adequate measures to ensure that the personal data is protected from accidental destruction or loss, including measures to restore the availability and access to the personal data in a timely manner in the event of a physical or technical incident. Where appropriate, these measures include:

- infrastructure redundancy to ensure data access is regularly backed up and restored in a timely manner;
- tape backup is stored off-site and available for recovery in case of failure of SAN infrastructure for database server;
- only the controller may authorize the recovery of backups (if any) or the transfer of personal data outside of the location where the physical database is held, whereby in case of transfer the security measures shall be adjusted to avoid loss or unauthorized access to the personal data, when transferred;
- regular checks of all the implemented security measures described herein;
- removable media containing sensitive or judicial data shall be destroyed or made unusable when not used anymore; alternatively the data media may be re-used if data previously stored on that media cannot be re-constructed by any technical means; and
- any detected security incident is recorded, alongside the executed data recovery procedures, and the identification of the individuals who carried them out.

Separation of Data

We shall implement adequate measures to ensure that personal data collected for different purposes can be processed separately. Where appropriate, these measures include:

- access to data is separated through application security for the appropriate users (logical separation);
- modules within our database allow the separation of data regarding their purpose, *i.e.* by functionality and function;
- at the database level, the personal data is stored in different normalized tables, separated per module or function they support; interfaces, batch processes and reports are designed exclusively for specific purposes and functions, to ensure that the personal data collected for different purposes are processed separately; and
- measures of pseudonymization or encryption of personal data.

APPENDIX 3 - GDPR TERMS

This Appendix 3 applies to us solely to the extent that the GDPR applies to the processing of any personal data that you transfer to us under the Clauses.

For the purposes of this Appendix 3, "**controller**" means the relevant controller of the personal data.
Further to Article 28 of the GDPR, Life agrees that it:

a) processes the personal data only on documented instructions from the controller, including with regard to transfers of personal data to a third country or an international organisation, unless required to do so by Union or Member State law to which Life is subject; in such a case, Life shall inform the controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest; also, Life shall immediately inform the controller if, in its opinion, an instruction infringes the GDPR, national data protection laws in the EU or other applicable law; for the avoidance of doubt, the controller agrees that its instructions to Life for processing personal data include to process such data in accordance with any written agreement between Life and Purchaser or between Life and the controller;

b) ensures that persons authorised by Life to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;

c) takes all measures required pursuant to Article 32 of the GDPR (security of processing);

d) respects the conditions referred to in paragraphs 2 and 4 of Article 28 of the GDPR for engaging another processor; for the avoidance of doubt, the controller authorizes Life to engage another processor where the conditions referred to in paragraphs 2 and 4 of Article 28 of the GDPR have been met, and such authorization applies to Life's current processors, a list of which will be provided to the controller upon written request to Life;

e) taking into account the nature of the processing, assists the controller by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III of the GDPR, at the controller's cost, including, to the extent required to fulfill GDPR obligations, data subjects' right to access, rectification, erasure and portability of the data subject's personal data; (for the avoidance of doubt, processor shall only assist and enable controller to meet controllers obligations to satisfy data subjects' rights, but processor shall not respond directly to data subjects);

f) assists the controller, at the controller's cost, in ensuring compliance with the obligations pursuant to Articles 32 to 36 of the GDPR, including notifying the controller of any personal data breach without undue delay, taking into account the nature of processing and the information available to Life;

g) at the choice of the controller, deletes or returns all the personal data to the controller after the end of the provision of services relating to processing, and deletes existing copies unless required by law;

h) makes available to the controller all information necessary to demonstrate compliance with the obligations laid down in Article 28 of the GDPR and allow for and contribute to audits, up to once per year, and at the controller's cost, including inspections, conducted by the controller or another auditor mandated by the controller. Life can provide certificates or audit reports of its own auditors as evidence of compliance.