Archer Analysis Unlimited (AAU) Demonstration Site - SOFTWARE TERMS OF SERVICE

(for Archer Analysis Unlimited v 7.0 and later)

Terms last updated January 26, 2024.

These AAU Demonstration Site- Software Terms of Service ("**Terms**") are entered into between you ("**Client**") and Integrated DNA Technologies Inc., together with its subsidiaries ("**Company**" or "**IDT**") (Client and Company together, the "**Parties**," and each separately a "**Party**"), as of the date Client first uses the Application as defined below.

PLEASE READ THE FOLLOWING LEGALLY BINDING TERMS CAREFULLY BEFORE USING OR ACCESSING THE SERVICE (AS DEFINED BELOW). THIS AGREEMENT SHALL APPLY TO ANY QUOTE, ORDER, ORDER ACKNOWLEDGEMENT, AND INVOICE REFERENCING THE SERVICE, AND ANY LICENSE OR DELIVERY OF THE SERVICE BY IDT OR ITS AFFILIATE. BY SELECTING THE ACCEPT OPTION, OR OTHERWISE ACCESSING OR USING THE SERVICE (AS DEFINED HEREIN), YOU ACKNOWLEDGE THAT YOU HAVE READ THESE TERMS, UNDERSTAND THEM, AND AGREE TO BE BOUND BY THEM. IDT IS WILLING TO PROVIDE ACCESS TO THE SERVICE ONLY ON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS AND CONDITIONS OF THIS AGREEMENT. IF YOU DO NOT AGREE TO THESE TERMS, IDT IS UNWILLING TO GRANT YOU ACCESS TO THE SERVICE AND YOU SHOULD NOT USE THE SERVICE. THE TERM "YOU" AND "YOUR" REFERS COLLECTIVELY TO YOU, THE USER ACCEPTING THIS AGREEMENT AND THE ENTITY THAT YOU REPRESENT. IF YOU ARE ACCEPTING THIS AGREEMENT ON BEHALF OF AN ENTITY, YOU REPRESENT AND WARRANT THAT: (i) YOU HAVE FULL LEGAL AUTHORITY TO BIND SUCH ENTITY TO THESE TERMS; (ii) YOU HAVE READ AND UNDERSTAND THESE TERMS; AND (iii) YOU AGREE, ON BEHALF OF SUCH ENTITY, TO THESE.

Section 1.
PRODUCTS & SERVICES

1.1 Products. Subject to these Terms, IDT will provide Client its multi-tenant Archer Analysis Unlimited demonstration site ("**Application**").

1.2 Access & Use. Access to and use of said Application is achieved via a web-based access option ("Web-Based Access Option") The Web-Based Access Option means, in accordance with these Terms, that Client shall obtain web-based access to the Application via the internet location provided by IDT. The method of accessing and/or utilizing the Application shall be referred to as "**SaaS Services**."

1.5 Client's Use. IDT shall provide a non-exclusive, non-transferable right to access and use the Application in the Territory in accordance with the documentation and these Terms.

1.6 Authorized Users; Patients/Specimens. Client shall provide IDT with the identities of Client's employees and agents that will be provided password protected access to the SaaS Services (the "**Authorized Users**"). Client is responsible for compliance by its affiliates and each Authorized User with the Terms. Client acknowledges and understands that all Authorized Users will have access to all information and data in Client's account and Client is solely responsible for their access and use of information. Client is responsible to notify IDT when Authorized Users are no longer authorized to have access to Client's Account and request that IDT revoke each such Authorized User's account privileges. Client shall notify IDT immediately of any unauthorized use of any password or account or any other known or suspected breach of security or misuse of the Services. Client is responsible for the use of the Application and the SaaS Services by any and all employees, contractors, or other users that access the Application or the SaaS Services utilizing Client's System, SaaS Service, or account and/or access credentials. Client shall implement appropriate safeguards to ensure that Authorized Users do not share passwords or access information with each other or anyone else.

1.7 Territory. The "Territory" shall mean the European Union. The Services are only available in the Territory and Client therefore acknowledges and agrees that Client will access the Application and use

the SaaS Services only in the Territory and only in connection with services Client performs in the Territory.

1.8 Use Restrictions. Client shall neither directly or indirectly, nor permit any party to do any of the following: (i) copy, modify, create derivative works of, publish, license, sublicense, sell, market, distribute or otherwise commercially exploit the Application or SaaS Services; (ii) reverse engineer, decompile, disassemble or otherwise attempt to gain access to the source code form of the Application or SaaS Services; (iii) use the Application, SaaS Services or associated documentation in violation of export control Laws and regulations; (iv) remove any proprietary or legal notices from the Application, SaaS Services, documentation or any other IDT materials furnished or made available hereunder; (v) access the Application or SaaS Services in order to build a competitive product or service; or (vi) copy any features, functions, content or graphics of the Application or SaaS Services; (vii) make the Application or SaaS Services available to anyone other than Authorized Users; (viii) sell, resell, rent or lease the Application or SaaS Services, including, without limitation, use the Application or SaaS Services on a service bureau or time sharing basis or otherwise for the benefit of a third party; (iv) use the Application or SaaS Services to store or transmit infringing, libelous, or otherwise unlawful or tortious material, or to store or transmit material in violation of third-party privacy rights; (x) use the Application or SaaS Services to store or transmit malicious code; (xi) interfere with or disrupt the integrity or performance of the Application or SaaS Services or any data contained therein; (xii) attempt to gain unauthorized access to the Application or SaaS Services or their related data, systems or networks; (xiii) publish or disclose to third parties any evaluation of the Application or SaaS Services without IDT's prior written consent; (ix) publish or disclose to third parties any data or information related to Client's results from or Client's experience with using the Application or SaaS Services, without IDT's prior written consent; (xx) perform vulnerability, load, or any other test of the Application or SaaS Services without IDT's prior written consent; or (xxi) use the Application or SaaS Services in any manner or for any purpose that infringes or misappropriates any intellectual property right or other right of any person, or that violates any Laws. Client: (a) is solely responsible for the accuracy, quality, integrity and legality of all electronic data or information submitted by Client to the Application or SaaS Services ("**Client's Data**") and of the means by which Client acquired Client's Data; (b) shall prevent unauthorized access to or use of the Application or SaaS Services, and notify IDT promptly of any such unauthorized access or use; and (c) shall use the Application or SaaS Services only in accordance with any user guides, acceptable use policies for the Application or SaaS Services, and all applicable Laws. "**Laws**" means all applicable national, state and local or foreign laws, ordinances, regulations, guidance documents, policies and codes as may be amended from time to time.

Section 2.

DATA

2.1 Ownership; Rights.

3.1.2 As between the Parties, subject to the BAA, Client shall own all data and information that Client provides and stores using the Application or SaaS Services or has provided and stored on its behalf ("**Client Data**").

3.1.3 IDT may access Client's account and Client Data from time to time as IDT deems necessary or appropriate for purposes of performing the Services, including, without limitation, providing support, performing account administration and generating invoices with respect to Client's use of the Application and receipt of the Services. Except as permitted in these Terms or in the Business Associate Agreement attached hereto as Exhibit A ("BAA") (if applicable with respect to specific Applications and SaaS Services), IDT shall not during the Term edit, delete or disclose the contents of Client Data unless authorized by Client or IDT is required to do so by law or in the good faith belief that such action is necessary to: (1) conform with Laws or comply with legal process served on IDT; (2) protect and defend the rights or property of IDT and its licensors; or (3) enforce these Terms or establish any rights hereunder. Notwithstanding any provision herein to the contrary, IDT may use de-identified Client Data provided by the Client, and use such de-identified data, including data regarding Client's usage of the Application and Services ("**Usage Data**"), to analyze, develop, modify and improve IDT's product and service offerings, including, without limitation, databases with

aggregated data, algorithms, machine learning models and analysis services. Likewise, Client shall permit IDT to have reasonable access to the Client System to obtain de-identified Client Data and Usage Data for the purposes described in this subsection. Furthermore, IDT may use de-identified Client Data, and Usage Data to generate, utilize and publish aggregated data, statistics, analytical results and trend information related to the usage of the Application or SaaS Services (such as usage patterns), but only if such information is not attributed to Client and personally identifying information of Client's users is not provided.

2.2 Client is responsible for its Client Data, including its accuracy and content ensuring that no data is de-identified prior to being uploaded , and agrees to comply with Laws and the Section 1.6 (Use Restrictions) in using the Service. Client represents and warrants that it has made all disclosures and has all rights, consents and permissions necessary to use its Client Data with the Services and grant IDT the rights in Section 3.1, all without violating or infringing Laws, third-party rights (including intellectual property, publicity or privacy rights) or any terms or privacy policies that apply to the Client Data.

2.3 Security. While IDT will use reasonable and appropriate safeguards designed to protect Client Data, Client is solely responsible for the accuracy, quality, integrity, legality, reliability and appropriateness of all Client Data. Notwithstanding any other agreement between the parties, IDT will have no liability to Client or any third party for the deletion, correction, destruction, loss, infringement or failure of the Application or SaaS Services to process or store any Client Data. IDT reserves the right to establish a maximum amount of storage and a maximum amount of Client Data that Client may store, process, post or transmit on or through any Application or SaaS Services

2.4 Business Associate Agreement. "**Business Associate Services**" means Services provided by IDT where IDT acts as a "business associate" as defined by 45 C.F.R. 160.103, and "**Covered Entity Services**" means Services provided by IDT where IDT acts as a "covered entity" as defined by 45 C.F.R. 160.103. If Client provides IDT with any "Protected Health Information" as defined under HIPAA, then the terms of the Business Associate Agreement attached as Exhibit A to these Terms shall apply. The BAA will not govern the use, disclosure and security of PHI with respect to Covered Entity Services.

3.5 Data Processing Addendum. If Client provides IDT with any "personal data" as defined under the General Data Protection Regulation (or other applicable privacy regulations that requires the Parties to enter into similar terms), then the terms of the Data Processing Addendum ("**DPA**") attached as Exhibit B to these Terms shall apply with regard to that data.

Section 3.
WARRANTIES; COMPLIANCE WITH LAW

3.1 Mutual Warranties. Each party represents and warrants to the other that: (i) it is organized and validly existing under the Laws of the state of its formation and has full authority to enter into these Terms and to carry out its obligations hereunder; (ii) these Terms are a legal and valid obligation binding upon such party and enforceable against such party, except to the extent such enforceability may be limited by bankruptcy, reorganization, insolvency or similar Laws of general applicability governing the enforcement of the rights of creditors or by the general principles of equity (regardless of whether considered in a proceeding at law or in equity); and (iii) the delivery and performance of Services under these Terms does not conflict with any agreement, instrument or contract, oral or written, to which such party is bound.

3.2 Disclaimers.

4.3.1 EXCEPT AS EXPRESSLY PROVIDED HEREIN, NEITHER PARTY MAKES ANY WARRANTIES OF ANY KIND, WHETHER EXPRESS, IMPLIED, STATUTORY OR OTHERWISE, AND EACH PARTY SPECIFICALLY DISCLAIMS AND EXCLUDES ALL OTHER WARRANTIES, WHETHER STATUTORY, EXPRESS OR IMPLIED, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OF THIRD PARTY RIGHTS. FOR THE AVOIDANCE OF DOUBT, IDT DOES NOT WARRANT THAT THE APPLICATIONS OR SERVICES WILL MEET CLIENT'S NEEDS OR REQUIREMENTS, THAT THE

APPLICATIONS OR THE PROVISION OF THE SERVICES WILL BE UNINTERRUPTED OR THAT THE APPLICATIONS OR SERVICES WILL BE AVAILABLE AT ANY PARTICULAR TIME OR ERROR-FREE, OR THAT THE APPLICATION OR SERVICES WILL RESULT IN ANY PARTICULAR HEALTH OUTCOMES. FURTHER, IDT DOES NOT WARRANT THAT ALL ERRORS IN THE APPLICATIONS OR SERVICES ARE CORRECTABLE OR WILL BE CORRECTED. Client acknowledges that, notwithstanding the taking by IDT of security precautions, use of, or connection to, the Internet provides the opportunity for unauthorized third parties to circumvent such precautions and illegally gain access to the Services and Client Data. Accordingly, IDT cannot and does not guarantee the privacy, security, integrity or authenticity of any information so transmitted over or stored in any system connected to the Internet or that any security precautions taken will be adequate or sufficient.

4.3.2 Client Review. Without limiting the generality of the disclaimers in Section 4.3.1, Client acknowledges and agrees that: The Application and Services are research use only products. The Client agrees to take full responsibility for knowing and adhering to the use limitations associated with the Research Use Only designation applied to the products and services. The Client further acknowledges that Research Use Only Application and/or Services have not been approved for use in any clinical, diagnostic, or therapeutic applications or procedures or for any other use requiring compliance with any law or regulation regulating clinical, diagnostic, or therapeutic products or any similar products. Client acknowledges that the Application has not been tested or validated for any particular use or purpose or for safety or effectiveness. It is Client's responsibility to take any actions necessary for any specific use or applications and to ensure the Application and/or Services and data/materials that may be generated by or through the use of the Application and/or Services meet applicable requirements for such use. Furthermore, the Client agrees to ensure that the Application and/or Services are utilized by end-users for research use and are not used for the purpose of providing patient-specific information for the diagnosis, prevention, or treatment of any disease or impairment of, or the assessment of the health of, individual patients. The Client accepts fully responsibility for using and allowing others to use the Research Use Only Application and/or Services outside of a research context, and agrees to bear full and exclusive responsibility for providing the required documentation to any regulatory reviewing entity and obtaining any license(s) or other approvals necessary to use the Application and/or Services in proprietary applications or in any non-research (e.g., clinical) applications or contexts. IDT will not be responsible or liable for any losses, costs, expenses, or any other forms of liability arising out of the unauthorized or unlicensed use of the Application.

4.3.3 Updates. IDT does not guarantee that information will be updated on a regular basis or that the Application will continue to be updated for an unlimited period of time. There is also no guarantee that any adverse or important outcomes will be reported in the literature or incorporated in the Application or SaaS Service. CLIENT AND ITS AUTHORIZED USERS MUST EXERCISE THEIR INDEPENDENT PROFESSIONAL JUDGMENT AT ALL TIMES.

4.3.4. No FDA Approval. The Applications and SaaS Services have not been reviewed, cleared, authorized, or approved by the United States Food and Drug Administration and cannot be used to prevent, diagnose or treat any disease or other health condition. 4.4 Compliance with Law. Client and its affiliates shall use the Product and Services in compliance with the requirements of all Laws.

Section 4.
INTELLECTUAL PROPERTY AND CONFIDENTIALITY

4.1 Intellectual Property. As between the Parties and except for the limited express rights granted to Client under Section 1.2 of these Terms, IDT owns all right, title and interest, including all related intellectual property rights, in and to the Application, SaaS Services and all Deliverables, along with any improvements or modifications thereto. Client acknowledges that the limited rights granted under these Terms do not provide Client with title to or ownership of the Application or the Services, the Deliverables, any customizations thereto, or any intellectual property therein. For clarity, no right or license to the intellectual property of either party is granted pursuant to these Terms. In the event that Client provides comments or feedback relating to IDT, the Application or SaaS Services, Deliverables, or any of its products or services

("**Feedback**"), any such Feedback shall be owned exclusively by IDT.

4.2 Confidential Information. "**Confidential Information"** means any software, data, business, financial, operational, client, vendor or other information disclosed by one party to the other and not generally known by or disclosed to the public. Notwithstanding anything herein to the contrary, Confidential Information does not include information that is: (a) already known to or otherwise in the possession of a Party at the time of receipt from the other Party, provided such knowledge or possession was not the result of a violation of any obligation of confidentiality; (b) publicly available or otherwise in the public domain prior to disclosure by a Party; (c) rightfully obtained by a Party from any third party having a right to disclose such information without breach of any confidentiality obligation by such third party; (d) developed by a Party independent of any disclosure hereunder, as evidenced by a Party's records or (e) Protected Health Information (which is governed by the BAA rather than these confidentiality terms).

4.3 Confidentiality Obligations. Each party shall maintain all of the other Party's Confidential Information in confidence and will protect such information with the same degree of care that such Party exercises with its own Confidential Information. If a party suffers any unauthorized disclosure, loss of, or inability to account for the Confidential Information of the other Party, then the disclosing Party shall promptly notify and cooperate with the Party suffering the disclosure or loss and take such actions as may be necessary or reasonably requested by the Party suffering the disclosure or loss to minimize the damage that may result therefrom. Except as provided in these Terms, a Party shall not use or disclose (or allow the use or disclosure of) any Confidential Information of the other Party without the express prior written consent of such Party. If a Party is legally required to disclose the Confidential Information of the other Party, the Party required to disclose will, as soon as reasonably practicable, provide the other Party with written notice of the applicable order or subpoena creating the obligation to disclose so that such other Party may seek a protective order or other appropriate remedy. In any event, the Party subject to such disclosure obligation will only disclose that Confidential Information if the Party is advised by counsel that it is legally required to disclose the information. In addition, such Party will exercise reasonable efforts to obtain assurance that confidential treatment will be accorded to such Confidential Information. Access to and use of any Confidential Information shall be restricted to those employees and persons within a Party's organization who have a need to use the information to exercise rights under or perform these Terms or, in the case of Client, to make use of the Services and Deliverables, and are subject to a contractual, professional or other obligation to keep such information confidential. A Party's consultants and subcontractors may be included within the meaning of "persons within a party's organization," provided that such consultants and subcontractors have executed confidentiality agreement with provisions similar to those contained in this section. A Party may only disclose information concerning these Terms and the transactions contemplated hereby, including providing a copy of these Terms, to the following: (a) potential acquirers, merger partners, investors, lenders, financing sources, and their personnel, attorneys, auditors and investment bankers, solely in connection with the due diligence review of such Party by persons and provided that such disclosures are made in confidence, (b) the Party's outside accounting firm, or (c) the Party's outside legal counsel. A party may also disclose these Terms in connection with any litigation or legal action concerning these Terms.

4.4 Return of Confidential Information. All of a Party's Confidential Information disclosed to the other Party, and all copies thereof, are and shall remain the property of the disclosing Party. All such Confidential Information and any and all copies and reproductions thereof shall, upon request of the disclosing party or the expiration or termination of these Terms, be promptly returned to the disclosing Party or destroyed (and removed from the Party's computer systems and electronic media) at the disclosing Party's direction, except as prohibited by applicable law, and except that to the extent any Confidential Information is contained in a party's backup media, databases and e-mail systems, then such Party shall continue to maintain the confidentiality of such information and shall destroy it as soon as practicable and, in any event, no later than required by such Party's record retention policy. In the event of any destruction hereunder, the Party who destroyed such Confidential Information shall, if requested, provide to the other Party written certification of compliance therewith within fifteen days after destruction.

4.5 Equitable Relief. The receiving Party acknowledges that unauthorized disclosure of Confidential Information could cause substantial harm to the disclosing Party for which damages alone might not be a sufficient remedy and, therefore, that upon any such disclosure by the receiving Party the disclosing Party will be entitled to appropriate equitable relief in addition to whatever other remedies it might have at law or equity.

Section 5.
TERM AND TERMINATION

5.1 Term. Unless earlier terminated in accordance with this Section 6, these Terms are in effect as of the Effective Date and will expire sixty (60) days thereafter("Term") .

5.2 Termination for convenience. IDT may terminate these Terms immediately upon notice to Client for any reason or no reason at all. Effect of Termination. The termination or expiration these Terms for any reason shall not affect Client's or IDT's rights or obligations that expressly or by their nature continue and survive (including without limitation, the provisions concerning ownership, confidentiality, limitation on liability, indemnity and the warranty disclaimers). Client acknowledges that, due to the limited nature of these Terms, no Application or SaaS Services should be used in order to maintain any records, and that the Client Data may be destroyed at any time after sixty (60) days following expiration or termination of these Terms.

5.3 Remedies. Where a breach of certain provisions of these Terms may cause either Party irreparable injury or may be inadequately compensable in monetary damages, either Party may seek equitable relief in addition to any other remedies which may be available. The rights and remedies of the Parties under these Terms are not exclusive and are in addition to any other rights and remedies available at law or in equity.

Section 6.
INDEMNITY AND LIMITATION ON LIABILITY

6.1 Client Obligations. Client shall defend IDT against any cause of action, suit or proceeding (each a "Claim") made or brought against IDT by a third party arising out of or attributable to Client's use of the Application or Services and shall indemnify IDT for any damages finally awarded against, and for reasonable attorney's fees incurred by, IDT in connection with the Claim, on condition that IDT (a) promptly gives Client written notice of the Claim (provided, however, that the failure to give such notice shall not relieve Client of its indemnification obligations hereunder except to the extent that Client is materially prejudiced by such failure); (b) gives Client sole control of the defense and settlement of the Claim (provided that Client may not settle any Claim unless the settlement unconditionally release IDT of all liability); and (c) provides reasonable assistance in connection with the defense (at Client's reasonable expense).

6.2

6.3 Exclusion of Consequential and Related Damages. IN NO EVENT SHALL IDT HAVE ANY LIABILITY TO CLIENT FOR ANY LOST PROFITS OR REVENUES OR FOR ANY INDIRECT, SPECIAL, INCIDENTAL, CONSEQUENTIAL, COVER OR PUNITIVE DAMAGES HOWEVER CAUSED, WHETHER IN CONTRACT, TORT (INCLUDING NEGLIGENCE) OR UNDER ANY OTHER THEORY OF LIABILITY, AND WHETHER OR NOT IDT HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES AND NOTWITHSTANDING ANY FAILURE OF THE ESSENTIAL PURPOSE OF THESE TERMS OR ANY LIMITED REMEDY HEREUNDER.

Section 7.
OTHER PROVISIONS

7.1 Marketing. IDT will not refer to Client or its logo as a user of the Application and Services and will not describe Client's business in IDT's advertising, marketing, promotional, website, and investor materials.

7.2 Notices. Any notice under these Terms must be given in writing. IDT may provide notice to you via email. You agree that any such electronic communication will satisfy any applicable legal communication requirements, including that such communications be in writing.. **All notices to IDT must be sent to the attention of the Legal Department** 1710 Commercial Park, Coralville, IA 52241 cc legal@idtdna.com.

7.3 Assignment. Neither party may transfer

these Terms without the other party's prior written consent, except that IDT may, without Client's consent, assign these Terms to an affiliate, or another entity pursuant to a corporate reorganization, merger, acquisition or sale of all or substantially all of its assets to which these Terms relate. Any attempted assignment or delegation in violation of the foregoing is void. These Terms are binding upon the Parties and their successors and permitted assigns.

7.4 Updates. IDT may, in its discretion from time to time, make updates to these Terms, and such updates shall automatically apply. When updates are made, IDT will make a new copy of these Terms available on its website. All changes are effective immediately upon posting and apply to all access to and use of the Services thereafter. The date these Terms were last revised is identified at the top of the page. Client's continued use of the Services following the posting of revised Terms means that Client accepts and agrees to the changes. Client agrees to check this page from time to time so that Client is aware of any changes, as such changes are binding on Client.

7.5 Relationship Defined. Nothing contained herein shall constitute an employee employer relationship, joint venture, partnership or agency for the other for any purpose or in any sense whatsoever. As such, neither Party shall have the right to make any warranty or representation that such a relationship exists.

7.6 Headings and Captions. Section headings are used for convenience only and shall in no way affect the construction or interpretation of these Terms.

7.7 Waiver and Severability. An individual waiver of a breach of any provision of these Terms requires the consent of the Party whose rights are being waived and such waiver will not constitute a subsequent waiver of any other breach. Any provision of these Terms held to be unenforceable shall not affect the enforceability of any other provisions of these Terms, and the unenforceable provision shall be construed to reflect the economic effect of the unenforceable provision.

7.8 Governing Law. The laws of the State of Delaware govern all matters arising out of these Terms, without regard to any conflict of law principles applied therein. The UN Convention on Contracts for the International Sale of Goods and Uniform Computer Information Transactions Act (UCITA) will not apply to these Terms. The Parties may bring any disputes arising out of or related to these Terms or any Order Form non-exclusively in a court located in New Castle County, Delaware and submit to the personal jurisdiction of such courts. Each party expressly waives its rights to a trial by jury in connection with any dispute arising out of or related to these Terms.

7.9 Entire Agreement. These Terms and all exhibits and addenda thereto are incorporated herein and constitute the entire agreement of the Parties with respect to the subject matter hereof and thereof. These Terms supersede all prior or contemporaneous negotiations, representations, promises, and agreements concerning the subject matter herein whether written or oral.

7.10 Force Majeure. Neither party will be liable for any default or delay in the performance of obligation under these Terms if and to the extent such default, delay, or failure to perform hereunder is caused by an event (including, strikes, lockouts, labor troubles, fire, flood, terrorism, pestilence, earthquake, pandemic-- including that arising in connection with COVID-19 and its variants--epidemics, embargo, accident, explosion, shortages of power or material or natural resources of any kind, governmental laws, orders, regulations, elements of nature or acts of God, riots, insurrection, or civil disorders) beyond the reasonable control of such Party. However, the foregoing force majeure clause shall never excuse a Party's obligation to adhere to all Applicable Laws. Before taking shelter in this provision, the Client must promptly notify IDT in writing of the occurrence of the event beyond its reasonable control that affects the fulfillment of its obligations under this Agreement.

7.11 Compliance. By agreeing to these Terms, Client specifically intend to comply with all Applicable Laws, including but not limited to: (i) the Federal Food, Drug, and Cosmetic Act, 21 U.S.C. §§ 301 et. seq. and all United States Food and Drug Administration ("FDA") regulations; (ii) the federal anti-kickback statute (42 U.S.C. 1320a-7(b) and its implementing regulations); and (iii) the federal physician self-referral law, also referred to as the "Stark Law" (42 U.S.C. 1395nn and its implementing regulations); (iv) the federal Health

Insurance Portability and Accountability Act of 1996, as amended by the Health Information Technology for Economic and Clinical Health Act of 2009, and their implementing regulations, including the Privacy Standards adopted by the U.S. Department of Health and Human Services, as well as but not limited to the obligations set forth in the BAA attached as Exhibit A; and (v) and any other federal, state, local or foreign law, regulation, guidance document or policy that is concerned with the design, manufacturing, marketing, promotion, sale, use, safety, efficacy, or reliability of, or the postmarket surveillance over, medical devices, or components thereof, which are subject to change from time to time. Accordingly, the Parties agree that IDT has not conditioned Client's access to the Services upon any agreement by Client to purchase, use or recommend or influence another person's decision to purchase or use any product or service offered by IDT or any affiliate of IDT.

The following terms apply depending on the Application(s) subscribed to in the Order Form:

PRODUCT TERMS

1. Archer Analysis Unlimited (AAU) Application Terms

1.1. **SUPPORT SERVICES.**

1.1.1. IDT will provide to Client the support services described in this Section 1 for the support and maintenance of the Application and SaaS Services provided in the applicable Order Form ("AAU Support Services").

1.1.2. Support Channel. Client may make a request for AAU Support Services by emailing IDT at archercustomersuccess@idtdna.com or through other such other method as may be designated by IDT. IDT will use commercially reasonable efforts to respond to emails received during Business Hours within two hours and assign the request a Severity Level. IDT will use commercially reasonable efforts to respond to emails received outside of Business Hours within two hours on the next Business Day after the email is received and assign the request a Severity Level. "Business Days" means Monday through Friday, except for generally recognized U.S. holidays, and "Business Hours" means 8:00 am to 5:00 pm Pacific Time Zone adjusted for daylight saving time during Business Days.

1.1.3. Updates. Updates (if any) are included at no additional charge during the term of the applicable Order Form. If applicable, Client agrees to install any Updates provided by IDT in a timely manner. IDT is under no obligation to offer any Updates or Upgrades. "Updates**"** means, collectively, any modifications, alterations, enhancements and updates to the SaaS Services offered in the applicable Order Form.

1.1.4. Limitations. IDT shall not be obligated to provide AAU Support Services with respect to: (a) any modifications, customizations, alterations or additions to the SaaS Services made by Client; or (b) any computer program incorporating all or any part of the SaaS Services; (c) use of the SaaS Services in a manner not in accordance with these Terms or in conjunctions with any unauthorized other software, equipment or operating environments; or (d) gross negligence or intentional misconduct by any user of the SaaS Services. AAU Support Services does not include any services to be performed at Client's location or any other location outside of IDT's premises.

1.1.5. Additional Services. Any additional support services rendered by IDT and not specified in this Section 5, will be charged to Client on an hourly basis at IDT's then-current service fee.

1.1.6. Sole Remedy. Provision of AAU Support Services as described in this Section 1 is IDT's sole obligations and Client's sole remedy with respect to maintenance and support of the SaaS Services described in the applicable Order Form IDT shall not have other liability or obligation with respect

to any errors or other problems with the SaaS Services described in the applicable Order Form.

Exhibit A

Integrated DNA Technologies, Inc. (ACTING AS BUSINESS ASSOCIATE)
BUSINESS ASSOCIATE AGREEMENT

Last Updated: January 12, 2024

This Business Associate Agreement ("BAA") is by and between the Integrated DNA Technologies, Inc., a Delaware corporation having its principal place of business at 1710 Commercial Park, Coralville, IA 52241 ("Business Associate" or "IDT") and customer purchasing services from IDT pursuant to a written agreement ("Covered Entity" or "Customer") on behalf of itself and on behalf of all or its affiliates and/or controlled healthcare organizations (each a "Party" and collectively the "Parties").

WHEREAS, the Parties have entered into, or are entering into, or may subsequently enter into, one or more agreements whereby Business Associate performs certain functions, activities, or services (collectively "**Underlying Agreements**") for or on behalf of Covered Entity that may involve the use or disclosure of Protected Health Information (as defined herein) and Electronic Protected Health Information (as defined herein); and

WHEREAS, this Agreement is intended to comply with the requirement for written assurances between the Parties as contemplated by the Standards for Privacy of Individually Identifiable Health Information at 45 C.F.R. Parts 160 and 164, Subparts A and E, as may be amended from time to time (the "Privacy Rule") and the Security Standards for Health Insurance Reform at 45 C.F.R. Parts 160, 162 and 164, as may be amended from time to time (the "Security Rule"); and

WHEREAS, the "Health Information Technology for Economic and Clinical Health" ("HITECH") Act, contained within the American Recovery and Reinvestment Act of 2009 (Pub. L. No. 111-5, 123 Stat. 226), modifies the Privacy Rule and the Security Rule (hereinafter, all references to the Privacy Rule and the Security Rule shall include all amendments to such rules as may be published from time to time in connection with the HITECH Act, and all references to the HITECH Act shall include any accompanying regulations whether in effect as of the effective date of this Agreement or subsequently promulgated); and

NOW, THEREFOR, in consideration of the Parties' continuing obligations under the Underlying Agreements and the agreements herein and other good and valuable consideration, the receipt and sufficiency of which is hereby acknowledged, and only if and to the extent the Underlying Agreements involve the use or disclosure of Protected Health Information (as defined herein) and Electronic Protected Health Information (as defined herein), the Parties agree as follows:

1. **Definitions**
   Except as otherwise defined herein, any and all capitalized terms in this Agreement shall have the definitions set forth in the Privacy Rule or the Security Rule.

   "Business Associate" has the meaning set forth above.

   "Breach" has the meaning given to such term in 45 C.F.R. § 164.402.

   "Covered Entity" has the meaning set forth above.

   "Data Use Agreement" has the meaning has the same meaning as the term "data use agreement" in 45 C.F.R. § 164.514(e)(4) of the Privacy Rule. Section 4 of this Agreement constitutes a Data Use Agreement.

   "Designated Record Set" has the same meaning as the term "designated record set" in 45 C.F.R. § 164.501 of the Privacy Rule.

"Electronic Protected Health Information" ("ePHI") has the same meaning as the term "electronic protected health information" in 45 C.F.R. § 160.103 of the Security Rule, limited to the information created or received by Business Associate from or on behalf of Covered Entity.

"HITECH" Act has the meaning set forth above.

"HIPAA" means the Health Insurance Portability and Accountability Act of 1996 (Pub. L. No. 104-191), as amended, together with its implementing regulations.

"Individual" has the same meaning as the term "individual" in 45 C.F.R. § 160.103 of the Privacy Rule.

"Limited Data Set" has the same meaning as the term "limited data set" as defined at 45 C.F.R. § 164.514(e)(1).

"Privacy Rule" has the meaning set forth above.

"Protected Health Information ("PHI")" has the same meaning as the term "protected health information" in 45 C.F.R. § 160.103 of the Privacy Rule (including, without limitation, Electronic Protected Health Information), limited to the information created or received by Business Associate from or on behalf of Covered Entity.

"Required by Law" has the same meaning as the term "required by law" in 45 C.F.R. § 164.103 of the Privacy Rule.

"Secretary" means the Secretary of the Department of Health and Human Services or his or her designee.

"Security Incident" has the same meaning as the term "security incident" in 45 C.F.R. § 164.304 of the Security Rule.

"Security Rule" has the meaning set forth above.

"Unsecured PHI" has the meaning given to such phrase in the Breach Notification Rule at 45 C.F.R. § 164.402.

2. Obligations and Activities of Business Associate

(A) Business Associate acknowledges and agrees that all PHI that is created or received by Covered Entity and used by or disclosed to Business Associate or created or received by Business Associate on Covered Entity's behalf shall be subject to this Agreement.

(B) Business Associate agrees to not use or disclose PHI other than as permitted or required by this Agreement or as Required by Law.

(C) Business Associate agrees to use appropriate safeguards to prevent use or disclosure of PHI other than as provided for by this Agreement.

(D) Business Associate agrees to mitigate, to the extent practicable, any harmful effect that is known to Business Associate of a use or disclosure of PHI by Business Associate in violation of the requirements of this Agreement, the Privacy Rule or the Security Rule.

(E) Business Associate agrees to notify Covered Entity promptly following discovery of any Breach of Unsecured PHI. Any notice pursuant to this Section 2(E) will include, to the extent possible, the identification of each Individual whose Unsecured PHI has been, or is reasonably believed by Business Associate, to have been accessed, acquired or disclosed during such Breach. Business Associate will also

provide Covered Entity other available information that Covered Entity is required to include in its notification to the Individual.

(F) Business Associate agrees to report to Covered Entity any use or disclosure of PHI not provided for by this Agreement or any Security Incident of which it becomes aware.

(G) Business Associate agrees to ensure that any agent, including a subcontractor, to whom it provides PHI received from, or created or received by Business Associate for, or on behalf of, Covered Entity agrees in writing to substantially similar restrictions and conditions that apply through this Agreement to Business Associate with respect to such information.

(H) Within fifteen (15) days of receiving a written request from Covered Entity, Business Associate agrees to provide to Covered Entity such information as is requested by Covered Entity to permit Covered Entity to respond to a request by an Individual to inspect and obtain a copy of PHI about the Individual that is maintained in a Designated Record Set, for as long as the PHI is maintained in the Designated Record Set, in accordance with 45 C.F.R. § 164.524; to amend PHI or a record about the Individual in a Designated Record Set, for as long as PHI is maintained in the Designated Record Set, in accordance with 45 C.F.R. § 164.526; and for an accounting of the disclosures of the Individual's PHI in accordance with 45 C.F.R. § 164.528.

(I) Business Associate agrees to make internal practices, books, and records, including policies and procedures and PHI, relating to the use and disclosure of PHI received from, or created or received by Business Associate on behalf of, Covered Entity, available to the Secretary, in a time and manner designated by the Secretary, for purposes of the Secretary determining Covered Entity's compliance with the Privacy Rule.

3. <u>Permitted Uses and Disclosures by Business Associate</u>

(A) Except as otherwise limited by this Agreement, Business Associate may use or disclose PHI to perform functions, activities or services for or on behalf of Covered Entity as contemplated by the Underlying Agreements provided that such use or disclosure does not violate the Privacy Rule or the HITECH Act if done by Covered Entity.

(B) Except as otherwise limited by this Agreement, Business Associate may use PHI for the proper management and administration of the Business Associate or to carry out the present and/or future legal responsibilities of the Business Associate.

(C) Except as otherwise limited by this Agreement, Business Associate may disclose PHI (i) to carry out the present/or future legal responsibilities of the Business Associate or otherwise permitted or required by applicable law, and (ii) when Business Associate is acquired or merged with a third party, in which case, Business Associate reserves the right to transfer the PHI to a successor in interest that assumes Business Associate's obligations under this Agreement.

(D) Except as otherwise limited by this Agreement, Business Associate may disclose PHI for the proper management and administration of the Business Associate, provided that disclosures are Required by Law, or Business Associate obtains reasonable assurances from the person to whom the PHI is disclosed that it will remain confidential and be used or further disclosed only as Required by Law or for the purpose for which it was disclosed to the person, and the person notifies Business Associate of any breaches in the confidentiality of the PHI.

(E) Business Associate may use PHI to report violations of law to appropriate federal and state authorities, consistent with 45 C.F.R. § 164.502(j)(1).

(F) Except as otherwise limited by this Agreement, Business Associate may use PHI to aggregate data as permitted by 45 C.F.R. § 164.504(e)(2)(i)(B), including, without limitation, to create graphic or visual representations of such aggregate data, and use and disclose such aggregated data to others.

(G) Except as otherwise limited by this Agreement, Business Associate may use PHI to create de-identified information sets provided that the de-identification conforms to the requirements of 45 C.F.R. §164.514(b). Once de-identified, data is no longer subject to this Agreement.

(H) Except as otherwise limited by this Agreement, Business Associate may use PHI to create a Limited Data Set, and may, pursuant to a Data Use Agreement as set forth in Section 4.1 between the Parties, use such Limited Data Set for its own research purposes or public health activities.

4. Data Use Agreement

4.1 Pursuant to Section 3(H) hereof, Business Associate may receive from Covered Entity or create Limited Data Sets for Business Associate. With respect to any such Limited Data Set, Business Associate agrees that it will:

(A) Use or disclose such Limited Data Set only for research, public health activities, or as required by law.

(A) Use reasonable and appropriate physical, technical and administrative safeguards to prevent use or disclosure of the Limited Data Set other than as provided for by this Section 4.1.

(B) Report to Covered Entity any use or disclosure of a Limited Data Set not provided for in this Section 4.1 of which Business Associate becomes aware.

(C) Ensure that any agent, including any subcontractor, to whom Business Associate provides the Limited Data Set agrees in writing to the same restrictions and conditions that apply to Business Associate under this Section 4.1 with respect to the Limited Data Set.

(D) Not attempt to identify or contact any of the individuals whose PHI is included in the Limited Data Set.

4.2. Pursuant to Section 3(I) hereof, Covered Entity may receive Limited Data Sets from Business Associate. With respect to any such Limited Data Set, Covered Entity agrees that it will:

(A) Use or disclose such Limited Data Set only for research, public health activities, health care operations, or as required by law.

(B) Use reasonable and appropriate physical, technical and administrative safeguards to prevent use or disclosure of the Limited Data Set other than as provided for by this Section 4.2.

(C) Report to Business Associate any use or disclosure of a Limited Data Set not provided for in this Section 4.2 of which Covered Entity becomes aware.

(D) Ensure that any agent, including any subcontractor, to whom Covered Entity provides the Limited Data Set agrees in writing to the same restrictions and conditions that apply to Covered Entity under this Section 4.2 with respect to the Limited Data Set.

(E) Not attempt to identify or contact any of the individuals whose PHI is included in the Limited Data Set.

5. **Obligations of Covered Entity on Behalf of Business Associate**

(A) Covered Entity shall notify Business Associate of any limitation(s) in its notice of privacy practices in accordance with 45 C.F.R. § 164.520, to the extent that such limitation(s) may affect Business Associate's use or disclosure of PHI.

(B) Covered Entity shall notify Business Associate of any changes in, or revocation of, permission by an Individual to use or disclose PHI, to the extent that such changes may affect Business Associate's use or disclosure of PHI.

(C) Covered Entity shall notify Business Associate of any restriction to the use or disclosure of PHI that it has agreed to in accordance with 45 C.F.R. § 164.522, to the extent that such restriction may affect Business Associate's use or disclosure of PHI.

6. **Security Rule and HITECH Act Responsibilities of the Business Associate.**

With regard to its use and/or disclosure of ePHI, Business Associate hereby agrees to do the following:

(A) Comply with 45 C.F.R. §§ 164.308, 164.310, 164.312 and 164.316, with respect to ePHI, to prevent use or disclosure of ePHI other than as provided for by this Agreement.

(B) Require all of its subcontractors and agents that create, receive, maintain, or transmit ePHI on behalf of the Business Associate to agree, in writing, to adhere to substantially similar restrictions and conditions (in all material respects) concerning ePHI that apply to Business Associate pursuant to Section 5 of this Agreement.

(C) Report to Covered Entity any Security Incident of which it becomes aware that involves the Confidentiality, Integrity or Availability of the ePHI that it creates, receives, maintains or transmits for or on behalf of Covered Entity. The parties agree that this Section satisfies any reporting required by Business Associate of attempted but Unsuccessful Security Incidents (as defined below) for which the parties agree no additional report shall be required. For purposes of this Agreement, "Unsuccessful Security Incidents" include but are not limited to activity such as "pings" and other broadcast attacks on Business Associate's firewall, port scans, unsuccessful log-on attempts, denials of service and any other attempts to penetrate such computer networks or systems that do not result in unauthorized access, use or disclosure of ePHI.

(D) Authorize termination of this Agreement by Covered Entity if Covered Entity determines that Business Associate has violated a material term of this Agreement, in accordance with Section 6.

7. **Term and Termination**

(A) *Term.* The Term of this Agreement shall be effective as of the date set forth above, and shall terminate when all the PHI provided by Covered Entity to Business Associate, or created or received by Business Associate for or on behalf of Covered Entity, is destroyed or returned to Covered Entity or, if it is infeasible to return or destroy the PHI, protections are extended to such information, in accordance with the termination provisions in this Section 7.

(B) *Termination for Cause.* Upon Covered Entity's or Business Associate's knowledge of a material breach or violation by Business Associate of any provision of this Agreement, Covered Entity shall either:

(i) Provide an opportunity for Business Associate to cure the breach or end the violation and terminate the Underlying Agreements does not cure the breach or end the violation within a reasonable time as specified by Covered Entity;

(ii) Immediately terminate the Underlying Agreements if Business Associate has breached or violated a material term of this Agreement and cure is not possible; or

(iii) If neither termination nor cure is feasible, Covered Entity shall report the violation to the Secretary.

(C) *Effect of Termination.*

(i) Except as provided in paragraph (ii) of this Section, upon termination of the Underlying Agreements, for any reason, Business Associate shall return or destroy all PHI received from Covered Entity, or created or received by Business Associate for or on behalf of Covered Entity. This provision shall apply to PHI that is in the possession of subcontractors or agents of Business Associate. Business Associate shall retain no copies of the PHI. This Agreement shall terminate when all such PHI is either destroyed or returned to Covered Entity.

(ii) In the event that Business Associate determines that returning or destroying the PHI is infeasible, Business Associate shall extend the protections of this Agreement to such PHI and limit further uses and disclosures of such PHI to those purposes that make the return or destruction infeasible, for so long as Business Associate maintains such PHI.

8. Notification

With respect to notice pursuant to paragraph 2(F) above, notice to the Covered Entity shall be made by telephone and followed promptly by a written notice to the contact provided by the Covered Entity to the Business Associate. Any other notice to the Covered Entity required or provided for under this Agreement shall be made in writing and shall be either personally delivered, mailed by first class mail or sent via facsimile to the appropriate individual as listed in this Section in this Agreement. Either Party may designate a different address in writing to the other.

For notice to the Business Associate:
Integrated DNA Technologies Inc.
1710 Commercial Park
Coralville, Iowa, 52241
Attn: HIPAA Security Officer
Email: jdupre1@idtdna.com
CC: dataprivacy@idtdna.com

9. Regulatory References

A reference in this Agreement to a section in the Privacy Rule, the Security Rule or the HITECH Act means the section as in effect or as amended.

10. Amendment

The Parties agree to take such action as is necessary to amend this Agreement from time to time as is necessary for Covered Entity to comply with the requirements of the Health Insurance Portability and Accountability Act of 1996, the Privacy Rule, the Security Rule and the HITECH Act, as amended.

11. Survival

The respective rights and obligations of the Business Associate under Section 7 of this Agreement shall survive the termination of this Agreement.

12. Interpretation

Any ambiguity in this Agreement shall be resolved to permit compliance with the Privacy Rule, the Security Rule and the HITECH Act, as amended. Any conflict between the terms of this Agreement and any other agreement relating to the same subject matter, which is the Business Associate requirements under the Privacy Rule, the

Security Rule and the HITECH Act, as amended, shall be resolved so that the terms of this Agreement supersede and replace the relevant terms of any such other agreement.

13. **Anti-Assignment**

Neither Party may assign either this Agreement or any of its rights, interests or obligations hereunder without the prior written approval of the other Party.

14. **Severability**

The provisions of this Agreement shall be severable, and if any provision of this Agreement shall be held or declared to be illegal, invalid or unenforceable, the remainder of this Agreement shall continue in full force and effect as though such illegal, invalid or unenforceable provision had not been contained herein.

15. **Governing Law**

Except to the extent that the Privacy Rule, the Security Rule, the HITECH Act, as amended, or other federal law applies, this Agreement and the obligations of the Parties hereunder will be governed by and interpreted in accordance with the laws of the State of Delaware. The Parties agree that each is aware of and is deemed to have been notified of any applicable state or local laws, rules or regulations and each party agrees to comply with such applicable state laws, rules and regulations. The Parties agree that this Agreement is hereby deemed to be modified to comply with such applicable state or local laws, rules or regulations.

Exhibit B

Integrated DNA Technologies, Inc.
Data Processing Addendum (Client Controller / IDT as Processor)

Last Update: January 12, 2024

This Data Protection Addendum ("Addendum") establishes minimum data protection and cybersecurity standards and related requirements in connection with the performance of services under a written agreement (the "Agreement").

Between Integrated DNA Technologies, Inc., a Delaware corporation ("Company") and Client ("Client"), each a "Party" and collectively the "Parties.

WHEREAS, the Parties to the Agreement seek to add certain data privacy and security terms to the Agreement.

NOW THEREFORE, for good and valuable consideration, the receipt and sufficiency of which is hereby acknowledged, the Parties agree to the following:

1. Definitions.

1.1 "Data Protection Law" Data Protection Law means all applicable data protection and privacy legislation in force from time which apply to a party relating to the use of Personal Data .

1.2 "Data Security Incident" means (i) the loss or misuse (by any means) of Personal Data; (ii) the inadvertent, unauthorized, and/or unlawful disclosure, access, alteration, corruption, transfer, sale, rental, destruction, or use of Personal Data; or (iii) any other act or omission that compromises or may compromise the security, confidentiality, or integrity of Personal Data or a System.

1.3 "Data Subject Request" means any request by a natural person to access, update, revise, correct, object to Processing or delete Personal Data or any similar request, whether or not made pursuant to the applicable Data Protection Law.

1.4 "Personal Data" means all data or information obtained by or on behalf of Client, in any form or format, that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, to an identified or identifiable natural person.

1.5 "Process" (including "Processing" or "Processed") means any operation or set of operations that is performed upon any Personal Data, whether or not by automatic means, including, but not limited to, collection, recording, organization, storage, access, adaptation, alteration, retrieval, consultation, use, disclosure, dissemination, making available, alignment, combination, blocking, deletion, erasure, or destruction.

1.6 "Services" means those services that Company performs pursuant to the Agreement.

1.7 "Special Data" means Personal Data that is considered special category data or sensitive data under applicable Data Protection Law, or that triggers notification requirements to individuals in the event of unauthorized disclosure, including without limitation government ID numbers, financial account numbers, biometric data, and health and health benefits information.

1.8 "System" means any system, network, platform, database, computer, or telecommunications or other information system owned, controlled or operated by or on behalf of either Party or their affiliates for the purpose of Processing Personal Data pursuant to the Agreement.

2. General Requirements.

2.1 Both parties will comply with all applicable requirements of Data Protection Law. This clause 2.1 is in addition to, and does not relieve, remove or replace, a party's obligations or rights under Data Protection Law.

2.2 The Parties acknowledge that for the purposes of Data Protection Law, the Client is the Controller and the Company is the Processor. Without prejudice to the generality of clause 2.1, the Client will ensure that it has all necessary appropriate consents and notices in place to enable lawful transfer of the Personal Data to the Company and/or lawful collection of the Personal Data by the Company on behalf of the Client for the duration and purposes of this Agreement.

2.3 Without prejudice to the generality of clause 2.1, the Company shall, in relation to any Personal Data processed in connection with the performance by the Company of its obligations under this agreement:

i. Process Personal Data as necessary to provide the Services to Client, in accordance with Applicable Data Protection Law and the written instructions of Client, which shall be to process the Client Personal Data for the purposes set out in Annex 1

ii. maintain the confidentiality of all Personal Data, and maintain adequate encryption, unless otherwise required under Applicable Laws;

iii. ensure that any personnel Processing Personal Data are obligated to maintain the confidentiality of that information;

iv. Where the Company is relying on Applicable Laws as the basis for processing Client Processor Data, the Company shall notify the Client of this before performing the processing required by the Applicable Laws unless those Applicable Laws prohibit the Company from so notifying the Client on important grounds of public interest. The Company shall inform the Client if, in the opinion of the Company, the instructions of the Client infringe Applicable Data Protection Laws.

2.4 The Client hereby provides its prior, general authorization for the Company to appoint sub-processors to process the Client Personal Data, provided that the Company:

i. shall ensure that the terms on which it appoints such sub-processors comply with applicable Data Protection Laws, and are consistent with the obligations imposed on the Client;

ii. shall remain responsible for the acts and omission of any such sub-processor as if they were the acts and omissions of the Company; and

iii. shall inform the Client of any intended changes concerning the addition or replacement of the sub-processors, thereby giving the Client the opportunity to engage with the Company on such changes. Company shall consider objections but will not be obliged to implement or make amends based on such objections, if the Client objects to the changes and cannot demonstrate, to the Company's reasonable satisfaction, that the objection is due to an actual or likely breach of applicable Data Protection Law.

2.5 The Company shall not sell Personal Data and shall not transfer the Personal Data to third parties, for a commercial purpose other than providing the Services, (including any related and ancillary activities performed by the Company related to or as a part of the Services), or in any manner transfer the Personal Data for commercial purposes, outside of the direct business relationship between Client and Company.

2.6 The Company shall not disclose Personal Data to third parties:

i. without the prior written approval of Client (which may be provided in an agreed list pursuant to Clause 9 of the Standard Contractual Clauses set forth in Annexure 2 of this Exhibit B), written and enforceable

agreement with such third party that includes terms that are no less restrictive than the obligations applicable to Company under this Addendum, and the Company remains fully liable for such third party; or

ii. unless required by applicable Data Protection Law, in which case Company shall wherever reasonably possible (a) notify Client in writing before complying with any disclosure requirement, (b) comply with reasonable directions of Client with respect to such disclosure, and (c) promptly inform Client of any Personal Data so disclosed.

2.7 Unless prohibited by Applicable Law on grounds including but not limited to public interest, the Company shall promptly notify Client of:

i. any request, inquiry, complaint, notice, or communication received from any third party, including a data subject or a supervisory authority, with respect to any Personal Data and comply with reasonable instructions of Client and applicable Data Protection Law in responding to such request, inquiry, complaint, notice or communication. Additionally, the Company shall at the written request and cost of the Client provide its reasonable assistance in responding to any such Data Subject Request received by Client.

ii. any provision of Personal Data to a government body or other authority or court, whether through legal means or otherwise, including specific details of the data provided.

iii. any instruction by Client that Company believes to be in violation of applicable Data Protection Law; and

iv. any substantial changes to the Company's notices, policies, or procedures that would impede Company's ability to fulfil the terms of this Addendum regarding protection of Personal Data.

2.8 The Company shall keep records that demonstrate its compliance with its obligations under this Exhibit B and allow for reasonable audits by the Client or the Client's designated auditor upon reasonable advanced written notice of at least 15 working days.

2.9 The Company shall reasonably assist and cooperate with Client (taking into account the nature of the processing and the information available to the Company), and at the Client's cost and written request, in responding to any request from a data subject and in ensuring the Client's compliance with its obligations under applicable Data Protection Law with respect to security, breach notifications, impact assessments and consultations with supervisory authorities or regulators.

2.10 The Company shall retain Personal Data only for as long as necessary to perform the Services, and at the end of the provision of the Services, at Client's choice, delete or return the Personal Data to Client unless expressly required otherwise by applicable Data Protection Law.

2.11 If Company becomes aware of a Data Security Incident it shall:

i. provide Client written notice without undue delay after becoming aware of such confirmed Data Security Incident;

ii. undertake an investigation of such Data Security Incident and reasonably cooperate with Client, its regulators and law enforcement agencies; and

iii. take such reasonable corrective action in a timely manner to remediate and prevent a recurrence of such Data Security Incident.

3. Client Representation and Warranty. Client represents and warrants that:

3.1 It has and shall maintain a lawful basis to provide or make Personal Data available to Company or has acquired the necessary consent in accordance with applicable Data Protection Law;

3.2 Client's instructions in respect of Processing of Personal Data shall, at all times, comply with applicable Data Protection Law; and

3.3 To the best of Clients knowledge, all personal data provided or made available to Company shall be accurate, complete, and not misleading.

4. Indemnification. Client shall indemnify Company, its affiliates, and their respective employees, agents, and officers from any and all allegations, claims, demands, costs (including, but not limited to, those associated with a regulatory inquiry), expenses (including, but not limited to, attorneys' fees and disbursements), losses, liabilities, penalties, fines, settlements, or damages arising out of or in connection with a breach of Client's Representation and Warranty in Clause 3, above.

5. Cyber and Information Security. Company represents and warrants that it shall establish, maintain, and comply with:

5.1 Administrative, technical, and physical safeguards designed to ensure the security, confidentiality, reliability, and integrity of Personal Data.

5.2 Safeguards should be commensurate with the type and amount of Personal Data Processed by Company), having regard to the state of the art and industry standards, and should, protect Personal Data and Systems against reasonably anticipated threats or hazards, including from unauthorized access, loss, theft, destruction, use, modification, collection, attack, or disclosure.

5.3 Safeguards should address the security controls set forth in the Center for Internet Security's Critical Security Controls, formerly known as the SANS Top 20, and comply with the Payment Card Industry Data Security Standards if Company Processes cardholder or other financial account data.

5.4 A written security program and policy that meets the requirements imposed under applicable Data Protection Law and aligns with established industry practices, and provides for: (i) defined organizational roles related to information security; (ii) appropriate internal controls with respect access given to Personal Data; (iii) a network security program which includes identification and authentication, maintenance and media disposal; (iv) audit and accountability; (v) system communication security, including incident response and planning; and (vi) physical and environmental protection.

6. International Transfers.

6.1 Company may transfer Client Personal Data outside of the jurisdiction it was collected as required for the Purpose, provided that the Company shall ensure that all such transfers are affected in accordance with applicable Data Protection Laws. For these purposes, the Client shall promptly comply with any reasonable request of the Company, including any request to enter into standard data protection clauses adopted by applicable regulatory authorities (including but not limited to the EU Commission, UK Information Commissioner), based on the applicable transfer of data.

6.2 The Parties agree that any international transfer of Personal Data will comply with applicable Data Protection Law.The terms of Annexure 1 of this Exhibit B will govern any international transfer of data that is:

(i) subject to the General Data Protection Regulation ("GDPR") of the European Union, and is to a jurisdiction that is not within the European Economic Area ("EU Transfer"); or

(ii) subject to the United Kingdom GDPR, and is to a jurisdiction outside the United Kingdom ("UK Transfer"); or

(iii) subject to the Swiss Federal Act on Data Protection ("FADP"), and is to a jurisdiction outside of Switzerland ("Swiss Transfer").

6.3 Any other international transfer of Personal Data requiring a data transfer agreement containing specific terms under applicable Data Protection Law will be governed by such terms.

7. Miscellaneous. In the event of a conflict or inconsistency between this Addendum and any other portion of the Agreement, this Addendum shall govern and control; provided that the terms of this Addendum are without limitation to, and are not intended to supersede or limit, any other terms that are more protective of Personal Data, privacy, or cybersecurity. If applicable, the Standard Contractual Clauses in Annexure 2 of this Addendum shall govern and control in the event of any conflict or inconsistency between the terms of the Agreement, this Addendum (including Annexure 1) and Annexure 2.

ANNEXURE 1

Supplemental requirements for the transfer of Personal Data out of the European Economic Area, UK, or Switzerland

1. Any EU Transfer, UK Transfer, or Swiss Transfer shall be subject to the following, unless another legal mechanism for the transfer applies: (i) with respect to EU Transfers, the provisions of Annexure 2 (Standard Contractual Clauses), (ii) with respect to UK Transfers, the provisions of Annexure 3 (International Data Transfer Addendum), and (iii) with respect to Swiss Transfers, the provisions in Clause 2 of this Annexure 1. In addition, the following supplemental requirements shall apply to any such transfer:

   (a) Company shall regularly make available to Client information regarding public authority requests for access to Personal Data and the manner of reply provided (if permitted by law);

   (b) Company warrants that it has not purposefully created technical back doors or internal processes to facilitate direct access by public authorities to Personal Data, and is not required under applicable law or practice to create or maintain back doors;

   (c) Company shall inquire of any public authority making an access request regarding Personal Data whether it is cooperating with any other state authorities in relation to the matter;

   (d) Company shall provide reasonable assistance to data subjects in exercising their rights to Personal Data in the receiving jurisdiction;

   (e) Company shall cooperate with Client in the event that a relevant supervisory authority or court determines that a transfer of Personal Data must be subject to specific additional safeguards;

   (f) Company shall implement encryption and/or other technical measures sufficient to reasonably protect against interception of Personal Data during transit, or other unauthorized access, by public authorities; and

   (g) Company shall have appropriate policies and procedures in place, including training, so that requests for access to Personal Data from public authorities are routed to the appropriate function and properly handled.

2. With respect to any Swiss Transfers, Annexure 2 (Standard Contractual Clauses) shall apply as amended in accordance with the statement of the Swiss Federal Data Protection and Information Commissioner ("FDPIC") of 27 August 2021 (originally available at https://www.edoeb.admin.ch/dam/edoeb/en/dokumente/2021/Paper%20SCC%20def.en%2024082021.pdf.download.pdf/Paper%20SCC%20def.en%2024082021.pdf). In particular:

   (a) the FDPIC shall be the competent supervisory authority insofar as the data transfer is governed by the FADP (Clause 13 of Standard Contractual Clauses);

   (b) the law of the EEA country specified in the Standard Contractual Clauses set out in Annexure 2 shall be the governing law (Clause 17 of Standard Contractual Clauses);

   (c) the courts of the EEA country as specified in the Standard Contractual Clauses set out in Annexure 2 shall be the choice of forum (Clause 18 of Standard Contractual Clauses), but this shall not exclude individuals in Switzerland from the possibility of bringing a claim in their place of habitual residence in Switzerland, in accordance with Clause 18(c) of Standard Contractual Clauses; and

   (d) the Standard Contractual Clauses set out in Annexure 2 shall protect the data of legal entities in Switzerland until the entry into force of the revised FADP.

ANNEXURE 2

Standard Contractual Clauses for the Transfer of Personal Data from the Community to Third Countries (2021 version – Module 2)

SECTION I

Clause 1

Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) for the transfer of personal data to a third country.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter "entity/ ies") transferring the personal data, as listed in Annex I.A. (hereinafter each "data exporter"), and

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A. (hereinafter each "data importer")

have agreed to these standard contractual clauses (hereinafter: "Clauses").

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2

Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3

Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii) Clause 8.1(b), 8.9(a), (c), (d) and (e);

(iii) Clause 9(a), (c), (d) and (e);

(iv) Clause 12(a), (d) and (f);

(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e);

(viii) Clause 18(a) and (b).

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4
Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5
Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6
Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Clause 7
Docking clause

(a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.

(b) Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.

(c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8
Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

8.1 Instructions

(a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter "personal data breach"). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time,

the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter "sensitive data"), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union[1] (in the same country as the data importer or in another third country, hereinafter "onward transfer") if the third party is or agrees to be bound by these Clauses, under the appropriate Module, [2] or if:

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

[1] The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purpose of these Clauses.

[2] See the Standard Contractual Clauses available from the EU website for applicable Module terms (controller to controller, controller to processor, processor to subprocessor, or processor to controller).

(d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9
Use of sub-processors

(a) The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least 30 days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10
Data subject rights

(a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

Clause 11
Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12
Liability

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.

(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13
Supervision

(a) [Where the data exporter is established in an EU Member State:] The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679:] The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as

indicated in Annex I.C, shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679:] The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14

Local laws and practices affecting compliance with the Clauses

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards[3];

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

[3] As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative timeframe. This refers in particular to internal records or other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

Obligations of the data importer in case of access by public authorities

15.1 Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibittion, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16
Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17

Governing law

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of the jurisdiction of the Supervisory Authority for the data exporter, where applicable and where such law allows for third-party rights, and otherwise the law of Ireland.

Clause 18

Choice of forum and jurisdiction

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts of the member state whose law governs Clauses pursuant to Clause 17.

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

APPENDIX TO THE STANDARD CONTRACTUAL CLAUSES[4]

ANNEX I

A. LIST OF PARTIES

Data exporter(s):

Name and address: Entity Name and Address of "Client", as defined in the Agreement

Contact person's name, position and contact details: Primary Point of Contact of "Client", as defined in the Agreement

Activities relevant to the data transferred under these Clauses: See Addendum and Record of Processing Activity maintained by data exporter

Role (controller/processor): Processor of Customer Personal Data, Controller of Company Data

Data importer(s):

Name and address: Entity Name and Address of "Company", as defined in the Agreement

Contact person's name, position and contact details: Primary Point of Contact of "Company", as defined in the Agreement

Activities relevant to the data transferred under these Clauses: See Addendum and Record of Processing Activity maintained by data exporter

Role (controller/processor): Processor

[4] The Standard Contractual Clauses include this explanatory note: "It must be possible to clearly distinguish the information applicable to each transfer or category of transfers and, in this regard, to determine the respective role(s) of the Parties as data exporter(s) and/or data importer(s). This does not necessarily require completing and signing separate appendices for each transfer/category of transfers and/or contractual relationship, where this transparency can be achieved through one appendix. However, where necessary to ensure sufficient clarity, separate appendices should be used."

B. DESCRIPTION OF TRANSFER[5]

1. Subject Matter of the Processing

Personal Data is Processed for the following purposes:

(a) Business relationship

(b) Support of IDT systems, other products and services

(c) Improvement and enhancement of Archer and IDT products/services or develop new products/services

(d) Marketing

(e) Technical Support and troubleshooting.

2. Duration of the Processing

Personal Data will be Processed until:

(a) As long as necessary to fulfil the purposes and provide requested services pursuant to the Agreement, unless otherwise agreed upon in writing

(b) Technical Support, high level support, minimize downtime, responding to feedback from Client, metering, connectivity verification: until problem resolution.

3. Frequency of transfer

Personal Data will be Processed on a continuous basis.

C. Nature of the processing:

1. Processing **operations**

Personal Data will be subject to the following basic Processing activities:
Record, storage, consultation, use, disclosure by transmission, combination, restriction, erasure or destruction, anonymization.

2. Categories **of Data subjects**

The Personal Data to be Processed concerns the following categories of data subjects:
• Customer/Client and its employees and/or clients.

3. Categories **of personal data**

The Personal Data to be Processed concerns the following categories of data:
General contact information, Client's system information, Product or service complaints.

[5] Further details are included in the Agreement and the record of processing activity maintained by the data exporter.

4. **Competent Authority**

This will be the supervisory authority of the EU member State where the exporter is established, the Information Commission if the exporter is established in the United Kingdom ("UK") or the FDPIC if the exporter is established in Switzerland. Where the exporter is not established in an EU member State, the UK or Switzerland but it is subject to EU/UK/Swiss Data Protection Law, this will be the supervisory authority in the jurisdiction where IDT's representative is established (as required under EU/UK/Swiss Data Protection Law). Where the appointment of a representative is not required under EU/UK/Swiss Data Protection Law, the supervisory authority will be the CNIL in France if the individuals whose data is transferred are located in the EU, the Information Commissioner if the individuals are located in the UK or the FDPIC if the individuals are located in Switzerland. If the Personal Data originates from Canada, the supervisory authority will be one of the Commissioners who has jurisdiction over the matter as determined by the Applicable Data Protection Law.

ANNEX II

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANIZATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

This Annex 2 forms part of the DPA and describes the technical and organizational measures which IDT has implemented in accordance with Article 32(1) of the GDPR and other Applicable Data Protection Laws.

1- On site:

For instrument determination and performance optimization visits, IDT associates access only minimum necessary data, which does not contain any patient healthcare data. The data is transferred to the associate's notebook, is processed for customer report generation with recommendations, and is thereafter deleted per Standard Work and IDT data retention policies.

2- Remotely:

Access role: Only IDT Technical Support associates have secured access to Archer Analysis Unit and related features.

For remote support for complaints handling, IDT agents can use Remote Desktop Sharing (RDS) sessions, but only after the session is authorized by the Client at each instance.

Data transmission: Per IDT policy data is transmitted via secure encrypted method to internal IDT servers for associate to engage in customer support activities (TLS 1.2+ protocols are used for secured transactions).

3- Client sends data:

Sending by email, on web platform or per fax: data is sent by the Client via secure encrypted method to internal IDT associate within region. The Client, as Controller, is responsible for anonymizing Personal Data and uploading only the minimum data required before transferring to IDT. Further, IDT instrument software permits the Client to conceal or cloak specific Personal and Healthcare Data in its instrument report before exporting.

4- Data transfers within IDT Support functions:

If additional support is needed outside Client home region, only necessary information will be transmitted; unnecessary Personal and Healthcare Data will be deleted / completely anonymized and data will be sent via secure sharing method. Data at rest is encrypted and is destroyed per appropriate IDT customer care policy.

5- Policy and Practice:

IDT ensures the ongoing confidentiality, integrity, availability and resilience of processing systems and services. For this purpose, it has the ability to restore the availability and access to relevant services support and complaints case handling data in the IDT systems in a timely manner in the event of a physical or technical incident.

6- Processes:

IDT has a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.

* Procedure to de-identify/anonymize is instrument specific.

ANNEXURE 3

UK International Data Transfer Addendum
to the EU Commission Standard Contractual Clauses

This Addendum has been issued by the UK Information Commissioner for Parties making Restricted Transfers. The Information Commissioner considers that it provides Appropriate Safeguards for Restricted Transfers when it is entered into as a legally binding contract.

Part 1: Tables
Table 1: Parties

Start Date	The date of this Agreement.

The Parties		**Exporter (who sends the Restricted Transfer)**	**Importer (who receives the Restricted Transfer)**
Parties' details	Full legal name:	The full legal name for the entity identified as the "data exporter" in the Appendix Information (defined below).	The full legal name for the entity identified as the "data importer" in the Appendix Information (defined below).
	Trading name (if different):	Trading name of the Client if different from the legal name.	Integrated DNA Technologies UK Limited
	Main address (if a company registered address):	Asset out in the Appendix Information.	Asset out in the Appendix Information.
	Official registration number (if any) (company number or similar identifier):	UK Registration number of Client as provided by Client to Company.	ZB602963
Key Contact	Full name (optional):	As set out in the Appendix Information.	As set out in the Appendix Information.
	Job title:	As set out in the Appendix Information.	As set out in the Appendix Information.
	Contact details including email:	As set out in the Appendix Information.	As set out in the Appendix Information.

Table 2: Selected SCCs, Modules and Selected Clauses

Addendum EU SCCS	☒	The version of the Approved EU SCCs set out in Exhibit B, including the Appendix Information.

Table 3: Appendix Information
"**Appendix Information**" means the information which must be provided for the selected modules as set out in the Appendix of the Approved EU SCCs (other than the Parties), and which for this Addendum is set out in the Annexes to the Approved EU SCCs set out at Exhibit B, Annexure 2.

Table 4: Ending this Addendum when the Approved Addendum Changes

Ending this Addendum when the Approved Addendum changes	Which Parties may end this Addendum as set out in Section 19:	
	☐	Importer
	☒	Exporter
	☐	neither Party

Part 2: Mandatory Clauses
"Mandatory Clauses" means Part 2: Mandatory Clauses of the Approved Addendum, being the template Addendum B.1.0 issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18 of those Mandatory Clauses.
The Mandatory Clauses are hereby incorporated by reference into this Exhibit B, Annexure 3.