PHENOTIPS®

SOFTWARE LICENSE AND SUPPORT AGREEMENT

This Master License and Services Agreement (the "**Agreement**") is made and entered into, effective as of January 24, 2026 (the "Effective Date") between **Gene42 Inc. o/a PhenoTips**, a Canadian company having its principal place of business at 1400 - 18 King Street East, Toronto, Ontario, M5C 1C4, Canada ("**Gene42**") and *INSERT CLIENT NAME* ("**CLIENT**"), having its principal place of business at *INSTER CLIENT ADDRESS* ("**Licensee**").

WHEREAS Gene42 has available certain computer programs and services which Licensee wishes to use for Licensee's data processing purposes; and Gene42 is willing to permit Licensee to make use of such programs upon the terms and conditions set forth in this Agreement.

NOW THEREFORE in consideration of the terms and conditions set forth in this Agreement, Gene42 and Licensee agree as follows:

1. **DEFINITIONS**

Except as otherwise defined herein, capitalized terms in this Agreement shall have the meanings set forth below:

"**Authorized User**" means an employee, contractor, registered student, physician or research assistant of Licensee authorized by Licensee in accordance with the terms of this Agreement to access and use the Software.

"**Base Software**" means the standard, unmodified computer programs licensed generally by Gene42 and listed in "Products and Services".

"**De-Identification"** means the process of removing any information that identifies the individual or for which it is reasonably foreseeable in the circumstances that it could be utilized, either alone or with other information, to identify the individual from the Data.

"**Documentation**" means Gene42's documentation describing the features and operation of the Software, and any updates thereto provided by Gene42, which is delivered or made available to Licensee.

"**Intellectual Property Rights**" means all world-wide intellectual and industrial property rights, including without limitation, all rights in each country to patents of any type, design rights, utility models or other similar invention rights, copyrights, mask work rights, trade secret rights, trademarks, trade names and service marks, including applications and registrations for any of the foregoing, in any country, arising under statutory or common law or by contract and whether or not perfected, now existing or hereafter filed, issued, or acquired.

"**Materials**" means (a) the Software and Documentation including without limitation the following information regarding the Software: (i) computer software (object and source codes), programming techniques and programming concepts, methods of processing, system designs embodied in the Software; (ii) benchmark results, manuals, program listings, data structures, flow charts, logic diagrams, functional specifications, file formats; and (iii) discoveries, inventions, concepts, designs, flow charts, documentation, product specifications, application program interface specifications, techniques and processes relating to the Software, (b) any software, programs, tools, systems, data or other materials made available by Gene42 to Licensee in the course of the performance under this Agreement, as well as (c) any information, materials or feedback provided by Licensee to Gene42 relating to the Materials.

"**Modification**" means any enhancements, modifications or additions to the Software or Documentation, including but not to: (a) a change to the delivered source code or metadata; (b) Updates and/or Upgrades; or (c) any development, other than a change to the delivered source code or metadata, that customizes, enhances, or changes existing functionality of the Software including, but not to, the creation of any new application program interfaces or alternative user interfaces, the extension of Gene42 data structures, or other change utilizing or incorporating any Materials.

"Products and Services Schedule" means a document, in a form provided by Gene42 and executed by both parties, that references this Agreement and specifies the Software licensed, Services to be provided, applicable fees, the Initial Term, and other transaction-specific details. This Agreement shall govern all Products and Services Schedules.

"**Software**" means (a) the Base Software; (b) any Upgrades or Updates to the Base Software made available pursuant to Appendix B; and (c) any complete or partial versions of any of the foregoing.

"**Update**" means a change to the current version of the Software or a component thereof, which may include bug fixes, enhancements to the capability of an already partially supported feature or changes in the number, type, and/or specification of the supported platform(s).

"**Upgrade**" means a release of the Software or component thereof that implements a fundamental change in the Software system philosophy and/or the software architecture.

2. **INSTALLATION AND INTEGRATION**
    - **2.1 Installation.** Upon the execution of a Products and Services Schedule containing a licensed product, Gene42 shall provision Licensee with access to the Software on Gene42's cloud-based software platform ("Cloud Platform"). Gene42 shall install the Software Programs on the Cloud Platform and deliver the Documentation to Licensee on the scheduled delivery date or dates, as the case may be. The date the Software Programs are initially available to Purchaser's Authorized Users shall be deemed the "Technical Go Live Date" and the data in which Testing begins. The "Operational Go Live Date" shall be defined as the day of completion of the acceptance testing period, as described in section 2.1 **Testing**.
    - **2.1 Testing**. As of the Technical Go Live Date, Purchaser may test the Software Programs for a period of 15 days, to check if it is free from defects in the programming code resulting in a failure of the Software Programs to conform in all material respects to the applicable Documentation, and which defect results in Purchaser's inability to use the Software Programs in the affected area because the function is disabled or severely impacted (each a "Critical Defect"). If Purchaser does not notify Supplier of such Critical Defects within such testing period, the Software Programs will be deemed to be accepted by Purchaser and that date will be considered the Operational Go Live Date. Supplier will promptly correct or provide a workaround solution for any Critical Defect of which the Purchaser notifies it in writing during such testing period, and provide Purchaser with an additional ten-day testing period. This procedure will continue until the Purchaser either accepts or rejects the Software Programs as permitted in this Section. All other defects found during the testing period that are not Critical Defects shall be addressed in accordance with the Software Support and Maintenance Schedule, Schedule B. If Purchaser rejects the Software Programs due to the existence of a Critical Defect, Supplier will provide a refund of the license fees paid by Purchaser for such rejected Software Programs. Upon receipt of Supplier's refund, the applicable license granted to Purchaser for such Software Programs will immediately terminate.
3. Statement of Work.

- General Where Licensee wishes to engage Gene42 for professional services—such as integrating the Software with Licensee's applications (e.g., standard electronic health records), developing Modifications, or performing an installation that requires materially more effort than standard—the parties shall execute a written Statement of Work ("SOW"). Each SOW will define: (i) the specific services, deliverables, and scope of work to be provided by Gene42 (the "Scope"); (ii) the fees payable by Licensee and the payment schedule; (iii) the projected timeline, milestones, and any dependencies on Licensee; and (iv) any other relevant terms. Each SOW shall be incorporated by reference into this Agreement. Neither party will have any obligation to provide or accept any deliverables or services until an SOW is fully executed in writing by both parties. This Agreement shall take precedence in any conflict with an SOW, unless the SOW expressly states its intent to amend a specific term of this Agreement for that SOW only.-executed SOW expressly amends a term of this Agreement for the purposes of that SOW only.
- **Scope and Change Orders.** The executed SOW represents the complete agreement between the parties for the work defined therein. **Gene42's obligation is strictly to performing the services and providing the deliverables as explicitly described in the Scope.** If Licensee requests any modification, addition, or deviation from the Scope, it must be submitted to Gene42 as a formal change request. If the parties agree to the change, they shall negotiate and execute a written **"Change Order"** detailing the new work, any adjustments to fees or expenses, and any impact on the delivery schedule or other terms. Gene42 is under no obligation to perform any work outside the agreed-upon Scope until a Change Order is fully executed by authorized representatives of both parties.

4. **LICENSE AND RESTRICTIONS**
   - License Grant. Subject to the terms and conditions of this Agreement, Gene42 grants to Licensee a non-exclusive, non-transferable license to (a) permit only Authorized Users to use the Software for its own internal purposes for the collection [and analysis] of patient data and (b) use, copy and modify the Documentation solely for Licensee's internal use in conjunction with the Software.
   - Restrictions. Licensee shall not, nor permit any person (including any Authorized User) to, modify, translate, create derivative works of, reverse engineer, disassemble or decompile the Software, or any portion thereof, which has been delivered to Licensee in binary/object code form. Licensee may not use or permit third parties to use the Software to conduct processing, time-sharing, outsourcing, application service provider or hosting services for any other person.
   - Authorized Users. Licensee is responsible for issuing and managing the passwords required for Authorized Users to access the Software, for maintaining the confidentiality of such passwords and accounts, and for all activities in respect of the Software that occur under Authorized Users' passwords or accounts. Licensee shall promptly notify Gene42 of any unauthorized use of any Authorized User's password or account or any other breach of security in connection with the Software.
5. **SERVICES AND SERVER PERFORMANCE MONITORING**
   - Services. The Software may send and/or receive data from one or more Gene42's Services ("Services") in order to provide workflow assistance, suggestions, to improve the user experience, and to evaluate and improve the functionality of the Services over time. Examples of Services are: extracting Human Phenotype Ontology (HPO) terms from free-text notes, suggesting gene matches based on selected HPO terms, and

suggesting genes based on phenotype information. In order to provide, evaluate, and improve the Services, anonymized and de-identified data (collectively "Data") will be collected and uploaded to the server on which the Services are hosted. The Data includes usage information such as the number of Authorized Users, number of patient records, de-identified patient data (including sex, age range, coded phenotypes, coded gene identifiers and classification, and variant classification) that has been stripped of any Protected Health Information as defined by the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule, aggregate anonymized free-text data (including non-standard phenotype terms and free-text notes from certain sections of the Software), and other relevant data (including the PhenoTips® server IP address, Web Browser User Agent, API Key, PhenoTips® Record Number, and responses to any suggestions made by the Services).

- Application and Server Performance Monitoring. In order to fulfill its support obligation, proactively address issues, monitor and maintain security through usage and audit logs, and to improve product experience, Gene42 may monitor server performance and use of the software through server and application monitoring utilities. These utilities collect application usage and server performance data for monitoring, analyzing, improvement and alerting purposes and rely upon a background program ("agent") that periodically transmits information about their system state and performance ("metrics") to said utilities. The metrics shall not include any identifiable personal health information (PHI) whatsoever, and shall include data such as the following, without limitation:
- Hard disk space consumption
- CPU utilization
- RAM usage
- Number of Authorized Users/Records
- Login activity
- Session activity

6. **SUPPORT AND MAINTENANCE**
   - Licensee Support. Licensee shall be responsible for providing front line support to, and handling all queries and correspondence from, the Authorized Users (and any third parties) in respect of the Software, including managing requests for support from Gene42.
   - Gene42 Support. Gene42 will provide Licensee with (a) any Updates and Upgrades; and (b) defect correction support, as further set out in Appendix B.
7. **FEES AND PAYMENT**
   - **Fees**. In consideration of (a) the rights to the Material granted herein; and (b) the provision of the support and maintenance services set out in Appendix A, Licensee shall pay Gene42 the annual license fees and annual support fees specified in the applicable Products and Services Schedule.
   - Payment; Interest. Licensee shall remit payments for all fees by cheque or by wire transfer to a bank account designated by Gene42. Except as otherwise set out herein, any and all payments made under this Agreement shall be non-refundable. If Licensee fails to make any payment under this Agreement when due and payable, interest shall accrue on such unpaid amount at the lesser of rate of one and a half percent (5%) per month or the highest rate permitted by law, calculated on a daily basis from the date such amount first becomes due and payable through the date actually received by Gene42.

- Taxes. Except for income taxes payable by Gene42, Licensee shall pay (and Gene42 shall have no liability for) any taxes, tariffs, duties and other charges or assessments imposed or levied by any government or governmental agency in connection with this Agreement, including without limitation, any sales, use, goods and services and value-added taxes on any payments due Gene42 in connection with this Agreement and the Software and services provided to Licensee hereunder. If Licensee determines it is obligated by law to withhold from payments made to Gene42 any amounts equal to applicable withholding taxes, Licensee agrees that it shall notify Gene42 in writing prior to withholding any such amounts and shall co-operate with Gene42 in good faith to minimize any withholding taxes, all in accordance with applicable law.

8. **INTELLECTUAL PROPERTY RIGHTS; PUBLICLY AVAILABLE SOFTWARE**
   - Ownership. All right, title and interest in and to the Materials, including all Intellectual Property Rights in each of the foregoing, are vested in and shall at all times remain the sole and exclusive property of Gene42. All ideas, concepts, methods, know-how and techniques of Gene42 or related to the Materials shall remain the sole property of Gene42. Licensee agrees that nothing herein transfers or conveys to Licensee any ownership right, title or interest in or to the Materials, or any Intellectual Property Rights therein.
   - Licensee Modifications. Licensee shall not make any Modifications utilizing any code from the Software without Gene42's prior written consent. Gene42 shall own any Modifications (such as, for example, application program interfaces) made by Licensee. Gene42 shall have sole discretion to determine, if, and when, such Modifications may be added to the base version of the next or subsequent Base Software as part of an Update or Upgrade.
   - Gene42 Modifications. Gene42 shall own each Modification made by or on behalf of Gene42 or its agents, consultants and representatives, with or without Licensee's involvement. Gene42 shall have sole discretion to determine if, and when, such Modification may be added to the base version of the next or a subsequent Base Software as part of an Update or Upgrade. Only upon inclusion of a Modification in the Base Software shall Gene42 Software support services be available for such Modification in accordance with Appendix B.
9. **INDEMNIFICATION**
   - Infringement and Defense of Licensee. Gene42 shall defend Licensee against claims brought against Licensee by any third party alleging that Licensee's use of the Software, in accordance with the terms and conditions of this Agreement, constitutes a direct infringement or misappropriation of a copyright or trade secret rights, and Gene42 will pay damages finally awarded against Licensee (or the amount of any settlement Gene42 enters into) with respect to such claims. This obligation of Gene42 shall not apply if the alleged infringement or misappropriation results from use of the Software in conjunction with any other software, failure to use an Update if such infringement or misappropriation could have been avoided by use of the Update, or unlicensed activities. To the extent Gene42 is prejudiced as a result, this Section shall not apply if Licensee fails to timely notify Gene42 in writing of any such claim. Gene42 is permitted to control fully the defense and any settlement of any such claim as long as such settlement shall not include a financial obligation on Licensee. If Licensee declines Gene42's proffered defense, or otherwise fails to give full control of the defense to Gene42's designated counsel, then Licensee waives Gene42's obligations under this Section. Licensee shall cooperate fully in the defense of such claim and

may appear, at its own expense, through counsel reasonably acceptable to Gene42. Gene42 expressly reserves the right to cease such defense of any claim(s) in the event the Software is no longer alleged to infringe or misappropriate, or is held not to infringe or misappropriate, the third party's rights. Gene42 may settle any claim on a basis requiring Gene42 to substitute for the Software alternative substantially equivalent non-infringing programs and supporting documentation. Licensee shall not undertake any action in response to any infringement or misappropriation, or alleged infringement or misappropriation of the Software that is prejudicial to Gene42's rights.

- THE PROVISIONS OF THIS SECTION 9 STATE THE SOLE, EXCLUSIVE, AND ENTIRE LIABILITY OF GENE42 TO LICENSEE, AND IS LICENSEE'S SOLE REMEDY, WITH RESPECT TO THE INFRINGEMENT OR MISAPPROPRIATION OF THIRD-PARTY INTELLECTUAL PROPERTY RIGHTS.

10. **DISCLAIMER AND LIMITATION OF LIABILITY**
    - Disclaimer. Except as may otherwise be provided herein, the Software is provided "as is" without warranty or condition of any kind, including without limitation, any warranty or condition of its merchantability, merchantable quality, non-infringement or fitness for a particular purpose. Further, Gene42 does not warrant, guarantee, or make any representations that the Software will be free from bugs and minor defects or that use of the Software will be uninterrupted or regarding the use, the results of the use, of the Software or Documentation in terms of correctness, accuracy, reliability or otherwise. Gene42 will not be responsible under this Agreement (a) if the Software is not used in accordance with the Documentation; or (b) if the defect or liability is caused by Licensee, a Modification developed by Licensee, or third-party software. GENE42 DISCLAIM ALL OTHER WARRANTIES EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, MERCHANTABLE QUALITY OR FITNESS FOR A PARTICULAR PURPOSE EXCEPT TO THE EXTENT THAT ANY WARRANTIES IMPLIED BY LAW CANNOT BE VALIDLY WAIVED.
    - Limitation of Liability. EXCEPT FOR BREACHES OF CONFIDENTIALITY OR DAMAGES/HARM TO INDIVIDUALS OR TANGIBLE PERSONAL PROPERTY (I) IN NO EVENT WILL EITHER PARTY BE LIABLE FOR ANY INDIRECT, INCIDENTAL, CONSEQUENTIAL, SPECIAL, EXEMPLARY OR PUNITIVE DAMAGES ARISING FROM ANY BREACH OF THIS AGREEMENT, INCLUDING BUT NOT TO LOSS OF PROFITS OR LOSS OF BUSINESS OPPORTUNITY, EVEN IF SUCH DAMAGES ARE FORESEEABLE AND WHETHER OR NOT SUCH PARTY HAS BEEN ADVISED OF THE POSSIBLITY THEREOF, AND (II) EXCEPT FOR PAYMENT AND INDEMNIFICATION OBLIGATIONS, THE MAXIMUM AGGREGATE LIABILITY OF A PARTY ARISING OUT OF OR IN CONNECTION WITH THIS AGREEMENT SHALL NOT EXCEED ANY AMOUNTS PAID TO GENE42 IN THE TWELVE MONTHS PRECEDING THE EVENTS THAT GAVE RISE TO THE CAUSE OF ACTION. The provisions of this Agreement allocate the risks between Gene42 and Licensee. The license and support fees reflect this allocation of risk and the limitations of liability herein.

11. **CONFIDENTIALITY AND PERSONAL INFORMATION**
    - Definition. In this Agreement, "**Confidential Information**" means the confidential, secret or proprietary information, information that is considered to be personal information or personal health information under any applicable privacy and data protection laws (collectively, "**Personal Information**"), know-how, documents and

other materials of one party (the "**Disclosing Party**") that are marked confidential, restricted or proprietary or that may reasonably be considered as confidential from its nature or from the circumstances surrounding its disclosure, including without limitation, technical, financial and business information, which has been or may hereafter be disclosed or delivered, directly or indirectly, to the other party (the "**Recipient**"), either orally, in writing or in any other form. Confidential Information shall not include information, know-how, documents and other materials which the Recipient can demonstrate by competent and sufficient evidence: (i) were already in the possession of the Recipient at the time of disclosure; or (ii) are received by the Recipient in good faith and on a non-confidential basis and without a use restriction from a third party who lawfully obtained and disclosed such information; or (iii) are approved for disclosure by the Disclosing Party in writing; or (iv) are independently developed by the Recipient without reference to or using any Confidential Information of the Disclosing Party. Notwithstanding the foregoing, Confidential Information shall be deemed to include the Materials, without further requirement to label or designate such as confidential.

- Use of Confidential Information. Confidential Information shall not be reproduced in any form except as required to accomplish the intent of this Agreement. Any reproduction of any Confidential Information of the other shall remain the property of the Disclosing Party and shall contain any and all confidential or proprietary notices or legends which appear on the original. With respect to the Confidential Information of the Disclosing Party, each Recipient: (a) shall take all steps the Recipient takes to protect its own similar proprietary and confidential information, which shall not be less than a reasonable standard of care, to keep all Confidential Information strictly confidential; and (b) shall not disclose any Confidential Information of the Disclosing Party to any person other than Recipient's employees or contractors whose access is necessary to enable Recipient to exercise its rights hereunder. Licensee shall ensure that any employee or contractor to whom Gene42 Confidential Information is disclosed is under a written agreement with Licensee to maintain the confidentiality of such Confidential Information in accordance with the terms of this Agreement, and shall issue instructions to such employees and contractors to receive, use and maintain the confidentiality of such Confidential Information in accordance with the provisions of this Agreement. Licensee shall be liable for any breach of the confidentiality obligations set forth in this Agreement by its employees, auditors and consultants. Confidential Information of a Disclosing Party disclosed to the Recipient prior to execution of this Agreement shall be subject to the protections afforded hereunder.
- Personal Information. Each party agrees to comply with their respective obligations under applicable privacy and data protection laws and regulations. For greater certainty, the parties intend that the only Personal Information to which Gene42 might have access would occur in the course of Gene42 providing defect correction services to Licensee in accordance with Appendix B, where Gene42 may require access to such Personal Information to recreate and correct defects to the Software reported by Licensee. With respect to Personal Information provided or made available to Gene42 by Licensee:
    - Gene42 agrees not to use the Personal Information for any purposes other than as required to perform its obligations under this Agreement, and to maintain appropriate security measures to protect the security and confidentiality of the

Personal Information, including physical, technological and administrative measures; and

- Licensee agrees that it has the authority and/or has obtained all necessary consents from the subject individuals as required under applicable laws and regulations to enable the Personal Information to be transferred, disclosed or otherwise made available to Gene42 for use by Gene42, provided such use is in accordance with this Agreement.

- Legal Disclosure. Notwithstanding anything to the contrary in this Agreement, the Recipient may disclose the Confidential Information of the Disclosing Party if such disclosure is in response to, and only to the extent required by, a valid court order or other valid legal process; provided however that prior to any such disclosure the Recipient must first give written notice to the Disclosing Party.

12. . TERM AND TERMINATION

12.1. Term of Agreement (MLSA). This Agreement shall commence on the Effective Date and shall continue in full force and effect as long as any Products and Services Schedule entered into hereunder remains active and has not expired or been terminated, or until this Agreement is terminated earlier in accordance with Section 12.4 (Termination for Cause) (the "Agreement Term").

12.2. Term of Products and Services Schedules. The initial license and/or service term (the "Initial Term") for any Software or Services shall be as specified in the applicable Products and Services Schedule. Following the Initial Term, such Products and Services Schedule shall automatically renew for successive periods (each a "Renewal Term") as specified in that Schedule (or if not specified, for successive one-year terms), unless either party gives the other written notice of its intention **not to renew** at least sixty (60) days prior to the end of the then-current term. The Initial Term and all Renewal Terms of a Products and Services Schedule are collectively referred to as its "Schedule Term."

12.3. No Termination for Convenience; Non-Cancelable. Except as expressly provided in Section 12.4 (Termination for Cause), no Products and Services Schedule may be terminated by Licensee prior to the end of its then-current Schedule Term. All payment obligations for Software or Services licensed for a given Schedule Term are non-cancelable and all fees paid are non-refundable.

12.4. Termination for Cause. This Agreement and any Products and Services Schedules hereunder may be terminated by a non-breaching party upon the earliest to occur of the following: (a) thirty (30) days after that party gives the other party written notice of a material breach of this Agreement (which includes, without limitation, more than thirty days delinquency in Licensee's payment of any money due hereunder), unless the breaching party has cured such breach during such thirty (30) day period; (b) immediately upon written notice for a material breach of this Agreement or any Schedule that is incapable of being cured; or (c) immediately upon written notice if the other party files for bankruptcy, becomes insolvent, or makes an assignment for the benefit of creditors.

12.5. Effect of Termination or Expiration. (a) **For Cause.** Upon any termination of this Agreement for cause, all of Licensee's rights hereunder, including any rights granted under all active Products and Services Schedules, shall immediately terminate. Licensee shall immediately cease all use of the Materials and PhenoTips Confidential Information. (b) **Expiration (Non-Renewal) of a Schedule.** Upon the expiration (i.e., non-renewal) of the final active Schedule Term, the procedures in Section 12.5(c) shall apply. This Agreement shall automatically terminate once all active Schedule Terms have expired and the provisions of Section 12.5(c) have been completed. (c) **Data Export and Wind-Down.** When Licensee provides notice of **non-renewal** as described in Section 12.2, or upon expiration of the final Schedule Term, PhenoTips shall render the PhenoTips instance and all data "read-only" for the final thirty (30) days of the final Schedule Term. Within such final thirty (30) day period, PhenoTips shall provide Licensee with all patient and family record data stored in the Software. The data will be provided to the Licensee via a secure download link in three (3)

formats: SQL dump of the entire database, a ZIP file of all attachments on the file system, and a PDF export of each patient and family record. (d) **Return of Materials.** Within thirty (30) days following any termination or expiration, Licensee shall irretrievably destroy or, upon PhenoTips's request, deliver to PhenoTips all copies of the Materials and PhenoTips Confidential Information in every form, except to the extent it is legally required to keep it for a longer period (in which case such return or destruction shall occur at the end of such period). Licensee must certify to PhenoTips in writing that it has satisfied its obligations under this Section.

12.6. Survival. All terms of this Agreement that by their nature extend beyond its expiration or termination (including, without limitation, provisions governing confidentiality, intellectual property ownership, payment obligations, disclaimers of warranties, limitations of liability, and indemnification) shall survive the expiration or termination of this Agreement for any reason.

13. **GENERAL PROVISIONS**
    - Publicity. Neither party shall use the name of the other party in publicity, advertising, or similar activity, without the prior written consent of the other (with such consent not to be unreasonably withheld), except that, (a) provided (i) Gene42 does not disclose any Licensee Confidential Information or specific project details, and (ii) Licensee is not asked or required to endorse Gene42 or the Software without Licensee's prior consent, Licensee hereby permits Gene42 to acknowledge that Licensee is a licensee of the Software and Licensee of Gene42 in any format or media, including without limitation, Licensee lists, conference attendee lists, in general discussions with licensees or prospective licensees, and in Gene42's marketing and advertising materials (including on the Gene42 website); and (b) upon Gene42's request, Licensee agrees to act as a reference customer for the Software, including via reference calls and stories, press testimonials, and site visits. Gene42 will make reasonable efforts to avoid having the reference activities unreasonably interfere with Licensee's business.
    - Assignment; No Third Party Beneficiaries. Licensee may not assign any of its rights and obligations under this Agreement without Gene42's prior written consent, which shall not be unreasonably withheld, provided that Licensee may assign this Agreement in whole or in part without consent to an affiliate or a purchaser of all or substantially all of Licensee's assets. Subject to the foregoing, this Agreement will inure to the benefit of and be binding upon the parties and each of their respective successors and assigns. Nothing in this Agreement expressed or implied is intended to confer upon any third party any rights or remedies.
    - Severability. It is the intent of the parties that in case any one or more of the provisions contained in this Agreement shall be held to be invalid or unenforceable in any respect, such invalidity or unenforceability shall not affect the other provisions of this Agreement, and this Agreement shall be construed as if such invalid or unenforceable provision had never been contained herein.
    - No Waiver. If either party should waive any breach of any provision of this Agreement, it shall not thereby be deemed to have waived any preceding or succeeding breach of the same or any other provision hereof.
    - Counterparts. This Agreement may be signed in two counterparts, each of which shall be deemed an original and which shall together constitute one Agreement. Signatures sent by electronic means (facsimile or scanned and sent via e-mail) shall be deemed original signatures.
    - Regulatory Matters. Licensee shall be responsible for complying with all applicable governmental regulations of the country where Licensee is registered, and any foreign

countries with respect to the use of the Materials by Licensee. Licensee will not export or re-export the Software, or any copies thereof, either directly or indirectly, outside of the country in which such materials are delivered to Licensee by Gene42, except in compliance with all applicable laws, ordinances and regulations. Licensee shall have the exclusive obligation to ensure that any export of the Software is in compliance with all applicable export laws and the import laws of the foreign country.

- Governing Law and Jurisdiction. This Agreement and any claims arising out of or relating to this Agreement and its subject matter shall be governed by and construed under the laws of the Province of Ontario and the laws of Canada applicable therein. Licensee hereby submits to the exclusive jurisdiction of the courts located in the Province of Ontario for any legal action or proceeding arising out of or related to this Agreement.
- Notices. All notices or reports which are required or may be given pursuant to this Agreement shall be in writing and shall be deemed duly given when delivered to the respective executive offices of Gene42 and Licensee at the addresses first set forth in this Agreement. Where in this Section or elsewhere in this Agreement written form is required, that requirement can be met by facsimile transmission, exchange of letters or other written form.
- Force Majeure. Any delay or non-performance of any provision of this Agreement (other than for the payment of amounts due hereunder) caused by conditions beyond the reasonable control of the performing party shall not constitute a breach of this Agreement, and the time for performance of such provision, if any, shall be deemed to be extended for a period equal to the duration of the conditions preventing performance.
- Entire Agreement. This Agreement (including its Appendices and any SOWs executed between the parties) constitutes the complete and exclusive statement of the agreement between Gene42 and Licensee with respect to its subject matter, and all previous representations, discussions, and writings are merged in, and superseded by this Agreement and the parties disclaim any reliance on any such representations, discussions and writings. This Agreement may be modified only by a writing signed by both parties. This Agreement shall prevail over any additional, conflicting, or inconsistent terms and conditions which may appear on any purchase order or other document furnished by Licensee to Gene42.

14. **COPYRIGHT NOTICE AND DISCLAIMER**

IN NO EVENT SHALL UT OR HSC BE LIABLE TO ANY PARTY FOR DIRECT, INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES, INCLUDING LOST PROFITS, ARISING OUT OF THE USE OF THE SOFTWARE, EVEN IF THE UNIVERSITY OF TORONTO OR HSC HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

UT AND HSC SPECIFICALLY DISCLAIM ANY WARRANTIES, INCLUDING, BUT NOT TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE SOFTWARE PROVIDED HEREUNDER IS PROVIDED “AS IS”. NEITHER UT NOR HSC HAS ANY OBLIGATION TO PROVIDE MAINTENANCE, SUPPORT, UPDATES, ENHANCEMENTS OR MODIFICATIONS

APPENDIX A

SOFTWARE SUPPORT AND MAINTENANCE SCHEDULE

1. **Overview**

Gene42's support service is comprised of the following:

- **Upgrades:** Gene42 will provide Licensee with a new release of the Base Software when a new release is generally made available to Gene42 customers as part of software support services;
- **Updates:** Gene42 will provide Licensee with interim Base Software fixes, updates and enhancements when such are generally made available to Gene42 customers as part of software support services;
- **Basic Helpdesk Support:** Licensee may contact Gene42 to report suspected defects and to obtain answers to basic questions regarding the features and functions of the Base Software and clarification of the Documentation. Gene42 may be contacted via:

- Web conference (e.g. Webex, Zoom)
- Email (support@phenotips.com)
- Phone (+1-888-682-5252)
- Zendesk (https://phenotips.zendesk.com/hc/en-us/requests/new)

2. **Calculation of Support Hours**

Support Hours counted towards the support package shall be calculated as follows:

1. For each support activity in the support period, the time spent per Gene42 staff member will be tracked to the minute and second
2. For each task, round up the time spent to the next 10th minute interval.
3. Sum up the time spent per task (as calculated in the previous step) for all tasks, to arrive at the grand total for support hours consumed by the licensee.

Support Hours include any time spent by Gene42 staff responding to any query relating to the Licensee's PhenoTips instance, account creation requests and any action performed by Gene42 staff, including but not to communication, clarification, investigation, diagnosis, patching, testing and deployment related to any issues reported by the Licensee to Gene42.

3. **Defect Correction Services**

A "defect" means a problem within the Base Software that is caused by an error in the programming code resulting in a failure of the Base Software to conform in all material respects to the design specifications in the applicable Documentation. Defect correction services are provided with respect to the then-current commercially available release of the Base Software. Defects reported by Licensee will be corrected in accordance with this Appendix B. Gene42 will analyze and diagnose defects in the Base Software brought to the attention of Gene42 and submitted by Licensee containing detailed problem descriptions, and supporting documentation as described below. All defects will be classified by Gene42 on a severity scale as set out in Table 2.

Gene42 agrees to use reasonable efforts to investigate and solve all reported defects in conformance with the timeframes set out in Table 1.

4. **Defect Reporting**

Licensee agrees to provide Gene42 with all information requested by Gene42 in order to replicate and diagnose the issue submitted. Licensee will provide at the minimum the following information when reporting an issue:

- a reasonably detailed description of the issue, including steps to recreate the issue
- a screenshot of the user interface showing the issue when applicable

Licensee acknowledges that Gene42's ability to provide support and maintenance is dependent on information provided by the Licensee being timely and accurate, and Gene42 will not be responsible for Licensee failures to provide such information.

5. **Severity Levels**

Table 1

Issue Type (see Table 2)	Initial Response Time
Critical Issue	Within 1 business day
Major Issue	Within 3 business days
Minor Issue	Within 10 business days

Note: A business day is any day that is not a Saturday or Sunday, or statutory and civic holiday observed in Ontario, Canada.

Table 2

Minor Issue

Issue Severity Level	Issue Definition	Answer to the issue
Critical Issue	System unavailable for use or significant functionality failure affecting all users.	*We take the issue into account considering the time frame defined by the Licensee's Software Support and Maintenance Schedule. We provide a workaround, a bug fix or a solution the Licensee agrees on within a reasonable time on a reasonable-effort basis.*
Major Issue	System unavailable for use by some users or some significant functionality failure affecting some or most users.	*We take the issue into account considering the time frame defined by the Licensee's Software Support and Maintenance Schedule. We provide the workaround patch to our customer.*

Other faults: typically, a trivial action that is not part of the core feature set of the application (for instance, the autosuggest for tags is not displayed in the Safari browser) does not work as expected.	*We take the issue into account considering the time frame defined by the Licensee's Software Support and Maintenance Schedule. We help the Licensee find a way to achieve his/her initial purpose without performing the given action. We provide the Licensee with the date when the issue encountered is likely to get fixed.*

APPENDIX B

INTERNATIONAL DATA TRANSFER AGREEMENT

Part 1: Tables

Table 1: Parties and signatures

Start date	July 1, 2024	
The Parties	**Exporter (who sends the Restricted Transfer)**	**Importer (who receives the Restricted Transfer)**
Parties' details	Full legal name: Main address (if a company registered address):	Full legal name: Gene42 Inc. Trading name (if different): PhenoTips Main address (if a company registered address): 18 King Street East, Suite 1400, Toronto, Ontario, M5C 1C4, Canada Official registration number (if any) (company number or similar identifier):
Key Contact	Full Name (optional): Job Title:	Full Name (optional): Job Title: CEO
Importer Data Subject Contact	Contact details including email:	Contact details including email: pawel@phenotips.com
Signatures confirming each Party agrees to be bound by this IDTA	Signed for and on behalf of the **Exporter** set out above Signed:	Signed for and on behalf of the Importer set out above Signed:

Table 2: Transfer Details

UK country's law that governs the IDTA:	✔️ England and Wales Northern Ireland Scotland
Primary place for legal claims to be made by the Parties	✔️ England and Wales Northern Ireland Scotland
The status of the Exporter	In relation to the Processing of the Transferred Data: ✔️ Exporter is a Controller Exporter is a Processor or Sub-Processor
The status of the Importer	In relation to the Processing of the Transferred Data: Importer is a Controller ✔️ Importer is the Exporter's Processor or Sub-Processor Importer is **not** the Exporter's Processor or Sub-Processor (and the Importer has been instructed by a Third Party Controller)
Whether UK GDPR applies to the Importer	✔️ UK GDPR applies to the Importer's Processing of the Transferred Data UK GDPR does not apply to the Importer's Processing of the Transferred Data
Linked Agreement	**If the Importer is the Exporter's Processor or Sub-Processor** – the agreement(s) between the Parties which sets out the Processor's or Sub-Processor's instructions for Processing the Transferred Data: Name of agreement: Software License and Support Agreement Date of agreement: July 1, 2024 Parties to the agreement: CLIENT and Gene42 Inc. (o/a PhenoTips) Reference (if any): n/a **Other agreements** – any agreement(s) between the Parties which set out additional obligations in relation to the Transferred Data, such as a data sharing agreement or service agreement: Name of agreement: n/a Date of agreement: n/a

	Parties to the agreement: n/a Reference (if any): n/a **If the Exporter is a Processor or Sub-Processor** – the agreement(s) between the Exporter and the Party(s) which sets out the Exporter's instructions for Processing the Transferred Data: Name of agreement: n/a Date of agreement: n/a Parties to the agreement: n/a Reference (if any): n/a
Term	The Importer may Process the Transferred Data for the following time period: ✔ the period for which the Linked Agreement is in force time period: (only if the Importer is a Controller or not the Exporter's Processor or Sub-Processor) no longer than is necessary for the Purpose.
Ending the IDTA before the end of the Term	✔ the Parties cannot end the IDTA before the end of the Term unless there is a breach of the IDTA or the Parties agree in writing. the Parties can end the IDTA before the end of the Term by serving: months' written notice, as set out in Section 29 (How to end this IDTA without there being a breach).
Ending the IDTA when the Approved IDTA changes	Which Parties may end the IDTA as set out in Section 29.2: ✔ Importer ✔ Exporter neither Party
Can the Importer make further transfers of the Transferred Data?	✔ The Importer MAY transfer on the Transferred Data to another organisation or person (who is a different legal entity) in accordance with Section 16.1 (Transferring on the Transferred Data). The Importer MAY NOT transfer on the Transferred Data to another organisation or person (who is a different legal entity) in accordance with Section 16.1 (Transferring on the Transferred Data).
Specific restrictions when the Importer may transfer on the Transferred Data	The Importer MAY ONLY forward the Transferred Data in accordance with Section 16.1: ✔ if the Exporter tells it in writing that it may do so. to:

	to the authorised receivers (or the categories of authorised receivers) set out in: there are no specific restrictions.
Review Dates	No review is needed as this is a one-off transfer and the Importer does not retain any Transferred Data First review date: The Parties must review the Security Requirements at least once: each month(s) each quarter each 6 months ✔ each year each year(s) ✔ each time there is a change to the Transferred Data, Purposes, Importer Information, TRA or risk assessment

Table 3: Transferred Data

Transferred Data	The personal data to be sent to the Importer under this IDTA consists of: ✔ The categories of Transferred Data will update automatically if the information is updated in the Linked Agreement referred to. The categories of Transferred Data will NOT update automatically if the information is updated in the Linked Agreement referred to. The Parties must agree a change under Section 5.3.
Special Categories of Personal Data and criminal convictions and offences	The Transferred Data includes data relating to: ✔ racial or ethnic origin political opinions religious or philosophical beliefs trade union membership ✔ genetic data biometric data for the purpose of uniquely identifying a natural person ✔ physical or mental health sex life or sexual orientation criminal convictions and offences none of the above ✔ set out in: Section 4 of the Software License and Support Agreement And:

	✔️ The categories of special category and criminal records data will update automatically if the information is updated in the Linked Agreement referred to. The categories of special category and criminal records data will NOT update automatically if the information is updated in the Linked Agreement referred to. The Parties must agree a change under Section 5.3.
Relevant Data Subjects	The Data Subjects of the Transferred Data are: ✔️ The categories of Data Subjects will update automatically if the information is updated in the Linked Agreement referred to. The categories of Data Subjects will not update automatically if the information is updated in the Linked Agreement referred to. The Parties must agree a change under Section 5.3.
Purpose	The Importer may Process the Transferred Data for the following purposes: ✔️ The Importer may Process the Transferred Data for the purposes set out in: Section 4 of the Software License and Support Agreement. In both cases, any other purposes which are compatible with the purposes set out above. ✔️ The purposes will update automatically if the information is updated in the Linked Agreement referred to. The purposes will NOT update automatically if the information is updated in the Linked Agreement referred to. The Parties must agree a change under Section 5.3.

Table 4: Security Requirements

Security of Transmission	**We use firewalls to protect our self-managed cloud services.** Gene42's self-managed cloud services (Amazon Web Services) have firewalls in place that allow application ports and one SSH port allowing access to our DevOps team. **All data in transit is encrypted.** Gene42 configures messages sent from PhenoTips software to other systems to be encrypted in transit.
Security of Storage	**All data at rest is encrypted.** Gene42 always encrypts confidential data at rest. Gene42 aligns the validity of cryptographic keys and certificates with the application's critical content at least once a year.
Security of Processing	**We regularly backup our data.** Data is hosted on Microsoft Azure with high availability and redundancy built into the architecture. Gene42 client images are backed up at all of the following frequencies: • Hourly (expires after one day) • Daily (expires after one week) • Weekly (expires after 4 weeks) • Monthly (never expires) • After a backup expires or is no longer required it is permanently deleted.

Gene42 employees do not have direct access to the backup files. Gene42 submits requests to our cloud-service provider MedStack to restore backups from available backup images.

We regularly test and assess risks. Gene42 has processes in place for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures related to ensuring business continuity/disaster recovery, and our security of data processing.

Organisational security measures

We choose the most appropriate secure setting for our software. All of our publicly accessible services which require authentication and authorization are secure using the Auth0 solution. Auth0 provides brute-force protection and suspicious IP throttling. Our systems are set to lockout after ten or fewer unsuccessful login attempts, or limit the number of login attempts to no more than ten within five minutes.

Gene42 aligns the validity of cryptographic keys and certificates with the application's critical content at least once a year.

Authentication of Gene42 administrators is based on cryptographic techniques, hardware tokens or challenge/response protocols (strong authentication) is mandatory in the following situations:

· when Single Sign-On is applied;

· for any type of access from an untrusted network;

· when managing critical security features (such as firewalls, routers and intrusion detection and prevention systems).

We control who has access to your data. Gene42 has established and documented an access security policy, which requires at least that:

· Gene42 administrators have a unique login ID and password combination;

· Gene42 has a password management system for secrets management

· shared login ID and password combinations are not permitted;

· administrator access is limited to the network and the network services they have been specifically authorized for.

Gene42 establishes a formal process to manage the access rights of Gene42 administrators. The access administration process includes at least:

· the allocation of no more rights than those necessary to perform the tasks; and

· the modification or withdrawal of those rights when the employment changes or ends.

User accounts are created on an as-needed basis. New employees are granted reduced privileges on new accounts and are then upgraded as needed by business requirements. Only senior administrators approve and create new accounts. All new staff members are given the least number of privileges to perform their job and those privileges may change if needed to perform their duties. All services used by PhenoTips have built-in role-privilege systems that are leveraged each to suit our needs. We use SSO whenever possible to limit the number of accounts we have to manage. PhenoTips ensures that no devices can be accessed without entering a username and password. Users do not share accounts.

When an individual leaves the organisation their accounts are removed/disabled from all critical systems. For internal communication services, their accounts are documented for archival purposes.

Gene42 establishes a formal process to manage the access rights of PhenoTips users. The access administration process includes at least:

• the registration of PhenoTips Users and their assigned rights;

• the allocation of no more rights than those necessary to perform the tasks; and

• the modification or withdrawal of those rights when the contract changes or ends.

PhenoTips Users are informed of the access security policy and confirm they shall not disclose any personal confidential authentication information and they shall take action immediately in the event of a breach in order to limit the consequences.

PhenoTips Users are authenticated securely via OIDC/OAuth2: Two-Factor Authentication. Clients may choose to either (i) provide a specific set of users or (ii) integrate their Active Directory to enable SSO.

PhenoTips supports multiple standard protocols and mechanisms for SSO, including:

1. LDAP

2. OAuth2/OIDC/SMART

Technical security minimum requirements

We choose the most appropriate secure setting for our software. Gene42 authenticates client users using the client's authentication management system via OIDC identity authentication protocol. Gene42 relies on the security practices and policies of the client to ensure that access to the application is protected.

We protect ourselves from viruses and other malware. Our computers and laptops are protected from malware by having anti-malware software installed and limiting installation of applications to an approved set (i.e. using an App Store and a list of approved applications). Where we have anti-malware software installed, it is set to scan web pages and send warnings about accessing malicious websites.

We keep PhenoTips software up-to-date. Gene42 provides security, OS and application updates for major application updates and regular updates at the client's request and desired frequency. We work with several third-party service providers to ensure our software and services are working smoothly.

Gene42 hosts its application of the MedStack platform (using AWS and Azure). MedStack is a HITRUST, SOC2 compliant healthcare cloud platform. Gene42 uses Auth0 for authentication and authorization solutions. Gene42 uses Lyniate's services for HL7v2 message integration with its clients. Gene42 uses Sentry, a SOC2, HIPAA and GDPR compliant error monitoring system that automatically reports defects that users encounter while using the software. This assists with debugging, defect resolution, and proactive support. Event data is sent securely to Sentry servers and is scrubbed of any personally identifiable information (PII). Event data is 256-bit AES encrypted, both in transit and at rest, and is retained for 90 days. Event data is used solely for the purpose of identifying and correcting defects in the software.

Updates to the Security Requirements

The Security Requirements will update automatically if the information is updated in the Linked Agreement referred to.

✔️ The Security Requirements will NOT update automatically if the information is updated in the Linked Agreement referred to. The Parties must agree a change under Section 5.3.

Part 2: Extra Protection Clauses

Extra Protection Clauses:

(i) Extra technical security protections

(ii) Extra organisational protections

(iii) Extra contractual protections

Part 3: Commercial Clauses

Commercial Clauses See Software License and Support Agreement

Part 4: Mandatory Clauses

Information that helps you to understand this IDTA

1. This IDTA and Linked Agreements
    - Each Party agrees to be bound by the terms and conditions set out in the IDTA, in exchange for the other Party also agreeing to be bound by the IDTA.
    - This IDTA is made up of:

Part one: Tables;

Part two: Extra Protection Clauses;

Part three: Commercial Clauses; and

Part four: Mandatory Clauses.

- The IDTA starts on the Start Date and ends as set out in Sections 29 or 30.
- If the Importer is a Processor or Sub-Processor instructed by the Exporter: the Exporter must ensure that, on or before the Start Date and during the Term, there is a Linked Agreement which is enforceable between the Parties and which complies with Article 28 UK GDPR (and which they will ensure continues to comply with Article 28 UK GDPR).
- References to the Linked Agreement or to the Commercial Clauses are to that Linked Agreement or to those Commercial Clauses only in so far as they are consistent with the Mandatory Clauses.

2. Legal Meaning of Words
    - If a word starts with a capital letter it has the specific meaning set out in the Legal Glossary in Section 36.
    - To make it easier to read and understand, this IDTA contains headings and guidance notes. Those are not part of the binding contract which forms the IDTA.
3. You have provided all the information required
    - The Parties must ensure that the information contained in Part one: Tables is correct and complete at the Start Date and during the Term.
    - In Table 2: Transfer Details, if the selection that the Parties are Controllers, Processors or Sub-Processors is wrong (either as a matter of fact or as a result of applying the UK Data Protection Laws) then:

the terms and conditions of the Approved IDTA which apply to the correct option which was not selected will apply; and

the Parties and any Relevant Data Subjects are entitled to enforce the terms and conditions of the Approved IDTA which apply to that correct option.

- In Table 2: Transfer Details, if the selection that the UK GDPR applies is wrong (either as a matter of fact or as a result of applying the UK Data Protection Laws), then the terms and conditions of the IDTA will still apply to the greatest extent possible.

4. How to sign the IDTA
    - The Parties may choose to each sign (or execute):

the same copy of this IDTA;

two copies of the IDTA. In that case, each identical copy is still an original of this IDTA, and together all those copies form one agreement;

a separate, identical copy of the IDTA. In that case, each identical copy is still an original of this IDTA, and together all those copies form one agreement,

unless signing (or executing) in this way would mean that the IDTA would not be binding on the Parties under Local Laws.

5. Changing this IDTA
    - Each Party must not change the Mandatory Clauses as set out in the Approved IDTA, except only:

to ensure correct cross-referencing: cross-references to Part one: Tables (or any Table), Part two: Extra Protections, and/or Part three: Commercial Clauses can be changed where the Parties have set out the information in a different format, so that the cross-reference is to the correct location of the same information, or where clauses have been removed as they do not apply, as set out below;

to remove those Sections which are expressly stated not to apply to the selections made by the Parties in Table 2: Transfer Details, that the Parties are Controllers, Processors or Sub-Processors and/or that the Importer is subject to, or not subject to, the UK GDPR. The Exporter and Importer understand and acknowledge that any removed Sections may still apply and form a part of this IDTA if they have been removed incorrectly, including because the wrong selection is made in Table 2: Transfer Details;

so the IDTA operates as a multi-party agreement if there are more than two Parties to the IDTA. This may include nominating a lead Party or lead Parties which can make decisions on behalf of some or all of the other Parties which relate to this IDTA (including reviewing Table 4: Security Requirements and Part two: Extra Protection Clauses, and making updates to Part one: Tables (or any Table), Part two: Extra Protection Clauses, and/or Part three: Commercial Clauses); and/or

to update the IDTA to set out in writing any changes made to the Approved IDTA under Section 5.4, if the Parties want to. The changes will apply automatically without updating them as described in Section 5.4;

provided that the changes do not reduce the Appropriate Safeguards.

- If the Parties wish to change the format of the information included in Part one: Tables, Part two: Extra Protection Clauses or Part three: Commercial Clauses of the Approved IDTA, they may do so by agreeing to the change in writing, provided that the change does not reduce the Appropriate Safeguards.
- If the Parties wish to change the information included in Part one: Tables, Part two: Extra Protection Clauses or Part three: Commercial Clauses of this IDTA (or the equivalent information), they may do so by agreeing to the change in writing, provided that the change does not reduce the Appropriate Safeguards.

- From time to time, the ICO may publish a revised Approved IDTA which:

makes reasonable and proportionate changes to the Approved IDTA, including correcting errors in the Approved IDTA; and/or

reflects changes to UK Data Protection Laws.

The revised Approved IDTA will specify the start date from which the changes to the Approved IDTA are effective and whether an additional Review Date is required as a result of the changes. This IDTA is automatically amended as set out in the revised Approved IDTA from the start date specified.

6. Understanding this IDTA
    - This IDTA must always be interpreted in a manner that is consistent with UK Data Protection Laws and so that it fulfils the Parties' obligation to provide the Appropriate Safeguards.
    - If there is any inconsistency or conflict between UK Data Protection Laws and this IDTA, the UK Data Protection Laws apply.
    - If the meaning of the IDTA is unclear or there is more than one meaning, the meaning which most closely aligns with the UK Data Protection Laws applies.
    - Nothing in the IDTA (including the Commercial Clauses or the Linked Agreement) limits or excludes either Party's liability to Relevant Data Subjects or to the ICO under this IDTA or under UK Data Protection Laws.
    - If any wording in Parts one, two or three contradicts the Mandatory Clauses, and/or seeks to limit or exclude any liability to Relevant Data Subjects or to the ICO, then that wording will not apply.
    - The Parties may include provisions in the Linked Agreement which provide the Parties with enhanced rights otherwise covered by this IDTA. These enhanced rights may be subject to commercial terms, including payment, under the Linked Agreement, but this will not affect the rights granted under this IDTA.
    - If there is any inconsistency or conflict between this IDTA and a Linked Agreement or any other agreement, this IDTA overrides that Linked Agreement or any other agreements, even if those agreements have been negotiated by the Parties. The exceptions to this are where (and in so far as):

the inconsistent or conflicting terms of the Linked Agreement or other agreement provide greater protection for the Relevant Data Subject's rights, in which case those terms will override the IDTA; and

a Party acts as Processor and the inconsistent or conflicting terms of the Linked Agreement are obligations on that Party expressly required by Article 28 UK GDPR, in which case those terms will override the inconsistent or conflicting terms of the IDTA in relation to Processing by that Party as Processor.

- The words "include", "includes", "including", "in particular" are used to set out examples and not to set out a finite list.
- References to:

singular or plural words or people, also includes the plural or singular of those words or people;

legislation (or specific provisions of legislation) means that legislation (or specific provision) as it may change over time. This includes where that legislation (or specific provision) has been consolidated, re-enacted and/or replaced after this IDTA has been signed; and

any obligation not to do something, includes an obligation not to allow or cause that thing to be done by anyone else.

7. Which laws apply to this IDTA
    - This IDTA is governed by the laws of the UK country set out in Table 2: Transfer Details. If no selection has been made, it is the laws of England and Wales. This does not apply to Section 35 which is always governed by the laws of England and Wales.

How this IDTA provides Appropriate Safeguards

8. The Appropriate Safeguards
    - The purpose of this IDTA is to ensure that the Transferred Data has Appropriate Safeguards when Processed by the Importer during the Term. This standard is met when and for so long as:

both Parties comply with the IDTA, including the Security Requirements and any Extra Protection Clauses; and

the Security Requirements and any Extra Protection Clauses provide a level of security which is appropriate to the risk of a Personal Data Breach occurring and the impact on Relevant Data Subjects of such a Personal Data Breach, including considering any Special Category Data within the Transferred Data.

- The Exporter must:

ensure and demonstrate that this IDTA (including any Security Requirements and Extra Protection Clauses) provides Appropriate Safeguards; and

(if the Importer reasonably requests) provide it with a copy of any TRA.

- The Importer must:

before receiving any Transferred Data, provide the Exporter with all relevant information regarding Local Laws and practices and the protections and risks which apply to the Transferred Data when it is Processed by the Importer, including any information which may reasonably be required for the Exporter to carry out any TRA (the "Importer Information");

co-operate with the Exporter to ensure compliance with the Exporter's obligations under the UK Data Protection Laws;

review whether any Importer Information has changed, and whether any Local Laws contradict its obligations in this IDTA and take reasonable steps to verify this, on a regular basis. These reviews must be at least as frequent as the Review Dates; and

inform the Exporter as soon as it becomes aware of any Importer Information changing, and/or any Local Laws which may prevent or limit the Importer complying with its obligations in this IDTA. This information then forms part of the Importer Information.

- The Importer must ensure that at the Start Date and during the Term:

the Importer Information is accurate;

it has taken reasonable steps to verify whether there are any Local Laws which contradict its obligations in this IDTA or any additional information regarding Local Laws which may be relevant to this IDTA.

- Each Party must ensure that the Security Requirements and Extra Protection Clauses provide a level of security which is appropriate to the risk of a Personal Data Breach occurring and the impact on Relevant Data Subjects of such a Personal Data Breach.

9. Reviews to ensure the Appropriate Safeguards continue
    - Each Party must:

review this IDTA (including the Security Requirements and Extra Protection Clauses and the Importer Information) at regular intervals, to ensure that the IDTA remains accurate and up to

date and continues to provide the Appropriate Safeguards. Each Party will carry out these reviews as frequently as the relevant Review Dates or sooner; and

inform the other party in writing as soon as it becomes aware if any information contained in either this IDTA, any TRA or Importer Information is no longer accurate and up to date.

- If, at any time, the IDTA no longer provides Appropriate Safeguards the Parties must Without Undue Delay:

pause transfers and Processing of Transferred Data whilst a change to the Tables is agreed. The Importer may retain a copy of the Transferred Data during this pause, in which case the Importer must carry out any Processing required to maintain, so far as possible, the measures it was taking to achieve the Appropriate Safeguards prior to the time the IDTA no longer provided Appropriate Safeguards, but no other Processing;

agree a change to Part one: Tables or Part two: Extra Protection Clauses which will maintain the Appropriate Safeguards (in accordance with Section 5); and

where a change to Part one: Tables or Part two: Extra Protection Clauses which maintains the Appropriate Safeguards cannot be agreed, the Exporter must end this IDTA by written notice on the Importer.

10. The ICO
    - Each Party agrees to comply with any reasonable requests made by the ICO in relation to this IDTA or its Processing of the Transferred Data.
    - The Exporter will provide a copy of any TRA, the Importer Information and this IDTA to the ICO, if the ICO requests.
    - The Importer will provide a copy of any Importer Information and this IDTA to the ICO, if the ICO requests.

The Exporter

11. Exporter's obligations
    - The Exporter agrees that UK Data Protection Laws apply to its Processing of the Transferred Data, including transferring it to the Importer.
    - The Exporter must:

comply with the UK Data Protection Laws in transferring the Transferred Data to the Importer;

comply with the Linked Agreement as it relates to its transferring the Transferred Data to the Importer; and

carry out reasonable checks on the Importer's ability to comply with this IDTA, and take appropriate action including under Section 9.2, Section 29 or Section 30, if at any time it no longer considers that the Importer is able to comply with this IDTA or to provide Appropriate Safeguards.

- The Exporter must comply with all its obligations in the IDTA, including any in the Security Requirements, and any Extra Protection Clauses and any Commercial Clauses.
- The Exporter must co-operate with reasonable requests of the Importer to pass on notices or other information to and from Relevant Data Subjects or any Third Party Controller where it is not reasonably practical for the Importer to do so. The Exporter may pass these on via a third party if it is reasonable to do so.
- The Exporter must co-operate with and provide reasonable assistance to the Importer, so that the Importer is able to comply with its obligations to the Relevant Data Subjects under Local Law and this IDTA.

The Importer

- General Importer obligations
    - The Importer must:

only Process the Transferred Data for the Purpose;

comply with all its obligations in the IDTA, including in the Security Requirements, any Extra Protection Clauses and any Commercial Clauses;

comply with all its obligations in the Linked Agreement which relate to its Processing of the Transferred Data;

keep a written record of its Processing of the Transferred Data, which demonstrate its compliance with this IDTA, and provide this written record if asked to do so by the Exporter;

if the Linked Agreement includes rights for the Exporter to obtain information or carry out an audit, provide the Exporter with the same rights in relation to this IDTA; and

if the ICO requests, provide the ICO with the information it would be required on request to provide to the Exporter under this Section 12.1 (including the written record of its Processing, and the results of audits and inspections).

- The Importer must co-operate with and provide reasonable assistance to the Exporter and any Third Party Controller, so that the Exporter and any Third Party Controller are able to comply with their obligations under UK Data Protection Laws and this IDTA.

13. Importer's obligations if it is subject to the UK Data Protection Laws
    - If the Importer's Processing of the Transferred Data is subject to UK Data Protection Laws, it agrees that:

UK Data Protection Laws apply to its Processing of the Transferred Data, and the ICO has jurisdiction over it in that respect; and

it has and will comply with the UK Data Protection Laws in relation to the Processing of the Transferred Data.

- If Section 1 applies and the Importer complies with Section 13.1, it does not need to comply with:
- Section 14 (Importer's obligations to comply with key data protection principles);
- Section 15 (What happens if there is an Importer Personal Data Breach);
- Section 15 (How Relevant Data Subjects can exercise their data subject rights); and
- Section 21 (How Relevant Data Subjects can exercise their data subject rights – if the Importer is the Exporter's Processor or Sub-Processor).

14. Importer's obligations to comply with key data protection principles
    - The Importer does not need to comply with this Section 14 if it is the Exporter's Processor or Sub-Processor.
    - The Importer must:

ensure that the Transferred Data it Processes is adequate, relevant and limited to what is necessary for the Purpose;

ensure that the Transferred Data it Processes is accurate and (where necessary) kept up to date, and (where appropriate considering the Purposes) correct or delete any inaccurate Transferred Data it becomes aware of Without Undue Delay; and

ensure that it Processes the Transferred Data for no longer than is reasonably necessary for the Purpose.

15. What happens if there is an Importer Personal Data Breach
    - If there is an Importer Personal Data Breach, the Importer must:

take reasonable steps to fix it, including to minimise the harmful effects on Relevant Data Subjects, stop it from continuing, and prevent it happening again. If the Importer is the Exporter's Processor or Sub-Processor: these steps must comply with the Exporter's instructions and the Linked Agreement and be in co-operation with the Exporter and any Third Party Controller; and

ensure that the Security Requirements continue to provide (or are changed in accordance with this IDTA so they do provide) a level of security which is appropriate to the risk of a Personal Data Breach occurring and the impact on Relevant Data Subjects of such a Personal Data Breach.

- If the Importer is a Processor or Sub-Processor: if there is an Importer Personal Data Breach, the Importer must:

notify the Exporter Without Undue Delay after becoming aware of the breach, providing the following information:

- a description of the nature of the Importer Personal Data Breach;
- (if and when possible) the categories and approximate number of Data Subjects and Transferred Data records concerned;
- likely consequences of the Importer Personal Data Breach;
- steps taken (or proposed to be taken) to fix the Importer Personal Data Breach (including to minimise the harmful effects on Relevant Data Subjects, stop it from continuing, and prevent it happening again) and to ensure that Appropriate Safeguards are in place;
- contact point for more information; and
- any other information reasonably requested by the Exporter,

if it is not possible for the Importer to provide all the above information at the same time, it may do so in phases, Without Undue Delay; and

assist the Exporter (and any Third Party Controller) so the Exporter (or any Third Party Controller) can inform Relevant Data Subjects or the ICO or any other relevant regulator or authority about the Importer Personal Data Breach Without Undue Delay.

- If the Importer is a Controller: if the Importer Personal Data Breach is likely to result in a risk to the rights or freedoms of any Relevant Data Subject the Importer must notify the Exporter Without Undue Delay after becoming aware of the breach, providing the following information:

a description of the nature of the Importer Personal Data Breach;

(if and when possible) the categories and approximate number of Data Subjects and Transferred Data records concerned;

likely consequences of the Importer Personal Data Breach;

steps taken (or proposed to be taken) to fix the Importer Personal Data Breach (including to minimise the harmful effects on Relevant Data Subjects, stop it from continuing, and prevent it happening again) and to ensure that Appropriate Safeguards are in place;

contact point for more information; and

any other information reasonably requested by the Exporter.

If it is not possible for the Importer to provide all the above information at the same time, it may do so in phases, Without Undue Delay.

- If the Importer is a Controller: if the Importer Personal Data Breach is likely to result in a high risk to the rights or freedoms of any Relevant Data Subject, the Importer must inform

those Relevant Data Subjects Without Undue Delay, except in so far as it requires disproportionate effort, and provided the Importer ensures that there is a public communication or similar measures whereby Relevant Data Subjects are informed in an equally effective manner.

- The Importer must keep a written record of all relevant facts relating to the Importer Personal Data Breach, which it will provide to the Exporter and the ICO on request.

This record must include the steps it takes to fix the Importer Personal Data Breach (including to minimise the harmful effects on Relevant Data Subjects, stop it from continuing, and prevent it happening again) and to ensure that Security Requirements continue to provide a level of security which is appropriate to the risk of a Personal Data Breach occurring and the impact on Relevant Data Subjects of such a Personal Data Breach.

16. Transferring on the Transferred Data
    - The Importer may only transfer on the Transferred Data to a third party if it is permitted to do so in Table 2: Transfer Details Table, the transfer is for the Purpose, the transfer does not breach the Linked Agreement, and one or more of the following apply:

the third party has entered into a written contract with the Importer containing the same level of protection for Data Subjects as contained in this IDTA (based on the role of the recipient as controller or processor), and the Importer has conducted a risk assessment to ensure that the Appropriate Safeguards will be protected by that contract; or

the third party has been added to this IDTA as a Party; or

if the Importer was in the UK, transferring on the Transferred Data would comply with Article 46 UK GDPR; or

if the Importer was in the UK transferring on the Transferred Data would comply with one of the exceptions in Article 49 UK GDPR; or

the transfer is to the UK or an Adequate Country.

- The Importer does not need to comply with Section 1 if it is transferring on Transferred Data and/or allowing access to the Transferred Data in accordance with Section 23 (Access Requests and Direct Access).

17. Importer's responsibility if it authorises others to perform its obligations
    - The Importer may sub-contract its obligations in this IDTA to a Processor or Sub-Processor (provided it complies with Section 16).
    - If the Importer is the Exporter's Processor or Sub-Processor: it must also comply with the Linked Agreement or be with the written consent of the Exporter.
    - The Importer must ensure that any person or third party acting under its authority, including a Processor or Sub-Processor, must only Process the Transferred Data on its instructions.
    - The Importer remains fully liable to the Exporter, the ICO and Relevant Data Subjects for its obligations under this IDTA where it has sub-contracted any obligations to its Processors and Sub-Processors, or authorised an employee or other person to perform them (and references to the Importer in this context will include references to its Processors, Sub-Processors or authorised persons).

What rights do individuals have?

18. The right to a copy of the IDTA

- If a Party receives a request from a Relevant Data Subject for a copy of this IDTA:

it will provide the IDTA to the Relevant Data Subject and inform the other Party, as soon as reasonably possible;

it does not need to provide copies of the Linked Agreement, but it must provide all the information from those Linked Agreements referenced in the Tables;

it may redact information in the Tables or the information provided from the Linked Agreement if it is reasonably necessary to protect business secrets or confidential information, so long as it provides the Relevant Data Subject with a summary of those redactions so that the Relevant Data Subject can understand the content of the Tables or the information provided from the Linked Agreement.

19. The right to Information about the Importer and its Processing
    - The Importer does not need to comply with this Section 19 if it is the Exporter's Processor or Sub-Processor.
    - The Importer must ensure that each Relevant Data Subject is provided with details of:

- the Importer (including contact details and the Importer Data Subject Contact);
- the Purposes; and
- any recipients (or categories of recipients) of the Transferred Data;

The Importer can demonstrate it has complied with this Section 19.2 if the information is given (or has already been given) to the Relevant Data Subjects by the Exporter or another party.

The Importer does not need to comply with this Section 19.2 in so far as to do so would be impossible or involve a disproportionate effort, in which case, the Importer must make the information publicly available.

- The Importer must keep the details of the Importer Data Subject Contact up to date and publicly available. This includes notifying the Exporter in writing of any such changes.
- The Importer must make sure those contact details are always easy to access for all Relevant Data Subjects and be able to easily communicate with Data Subjects in the English language Without Undue Delay.

20. How Relevant Data Subjects can exercise their data subject rights
    - The Importer does not need to comply with this Section 20 if it is the Exporter's Processor or Sub-Processor.
    - If an individual requests, the Importer must confirm whether it is Processing their Personal Data as part of the Transferred Data.
    - The following Sections of this Section 20, relate to a Relevant Data Subject's Personal Data which forms part of the Transferred Data the Importer is Processing.
    - If the Relevant Data Subject requests, the Importer must provide them with a copy of their Transferred Data:

Without Undue Delay (and in any event within one month);

at no greater cost to the Relevant Data Subject than it would be able to charge if it were subject to the UK Data Protection Laws;

in clear and plain English that is easy to understand; and

in an easily accessible form

together with

(if needed) a clear and plain English explanation of the Transferred Data so that it is understandable to the Relevant Data Subject; and

information that the Relevant Data Subject has the right to bring a claim for compensation under this IDTA.

- If a Relevant Data Subject requests, the Importer must:

rectify inaccurate or incomplete Transferred Data;

erase Transferred Data if it is being Processed in breach of this IDTA;

cease using it for direct marketing purposes; and

comply with any other reasonable request of the Relevant Data Subject, which the Importer would be required to comply with if it were subject to the UK Data Protection Laws.

- The Importer must not use the Transferred Data to make decisions about the Relevant Data Subject based solely on automated processing, including profiling (the "Decision-Making"), which produce legal effects concerning the Relevant Data Subject or similarly significantly affects them, except if it is permitted by Local Law and:

the Relevant Data Subject has given their explicit consent to such Decision-Making; or

Local Law has safeguards which provide sufficiently similar protection for the Relevant Data Subjects in relation to such Decision-Making, as to the relevant protection the Relevant Data Subject would have if such Decision-Making was in the UK; or

the Extra Protection Clauses provide safeguards for the Decision-Making which provide sufficiently similar protection for the Relevant Data Subjects in relation to such Decision-Making, as to the relevant protection the Relevant Data Subject would have if such Decision-Making was in the UK.

21. How Relevant Data Subjects can exercise their data subject rights– if the Importer is the Exporter's Processor or Sub-Processor
    - Where the Importer is the Exporter's Processor or Sub-Processor: If the Importer receives a request directly from an individual which relates to the Transferred Data it must pass that request on to the Exporter Without Undue Delay. The Importer must only respond to that individual as authorised by the Exporter or any Third Party Controller.
22. Rights of Relevant Data Subjects are subject to the exemptions in the UK Data Protection Laws
    - The Importer is not required to respond to requests or provide information or notifications under Sections 18, 19, 20, 21 and 23 if:

it is unable to reasonably verify the identity of an individual making the request; or

the requests are manifestly unfounded or excessive, including where requests are repetitive. In that case the Importer may refuse the request or may charge the Relevant Data Subject a reasonable fee; or

a relevant exemption would be available under UK Data Protection Laws, were the Importer subject to the UK Data Protection Laws.

If the Importer refuses an individual's request or charges a fee under Section 0 it will set out in writing the reasons for its refusal or charge, and inform the Relevant Data Subject that they are entitled to bring a claim for compensation under this IDTA in the case of any breach of this IDTA.

How to give third parties access to Transferred Data under Local Laws

23. Access requests and direct access
    - In this Section 23 an "Access Request" is a legally binding request (except for requests only binding by contract law) to access any Transferred Data and "Direct Access"

means direct access to any Transferred Data by public authorities of which the Importer is aware.
    - The Importer may disclose any requested Transferred Data in so far as it receives an Access Request, unless in the circumstances it is reasonable for it to challenge that Access Request on the basis there are significant grounds to believe that it is unlawful.
    - In so far as Local Laws allow and it is reasonable to do so, the Importer will Without Undue Delay provide the following with relevant information about any Access Request or Direct Access: the Exporter; any Third Party Controller; and where the Importer is a Controller, any Relevant Data Subjects.
    - In so far as Local Laws allow, the Importer must:

make and keep a written record of Access Requests and Direct Access, including (if known): the dates, the identity of the requestor/accessor, the purpose of the Access Request or Direct Access, the type of data requested or accessed, whether it was challenged or appealed, and the outcome; and the Transferred Data which was provided or accessed; and

provide a copy of this written record to the Exporter on each Review Date and any time the Exporter or the ICO reasonably requests.

24. Giving notice
    - If a Party is required to notify any other Party in this IDTA it will be marked for the attention of the relevant Key Contact and sent by e-mail to the e-mail address given for the Key Contact.
    - If the notice is sent in accordance with Section 1, it will be deemed to have been delivered at the time the e-mail was sent, or if that time is outside of the receiving Party's normal business hours, the receiving Party's next normal business day, and provided no notice of non-delivery or bounceback is received.
    - The Parties agree that any Party can update their Key Contact details by giving 14 days' (or more) notice in writing to the other Party.
25. General clauses
    - In relation to the transfer of the Transferred Data to the Importer and the Importer's Processing of the Transferred Data, this IDTA and any Linked Agreement:

contain all the terms and conditions agreed by the Parties; and

override all previous contacts and arrangements, whether oral or in writing.

- If one Party made any oral or written statements to the other before entering into this IDTA (which are not written in this IDTA) the other Party confirms that it has not relied on those statements and that it will not have a legal remedy if those statements are untrue or incorrect, unless the statement was made fraudulently.
- Neither Party may novate, assign or obtain a legal charge over this IDTA (in whole or in part) without the written consent of the other Party, which may be set out in the Linked Agreement.
- Except as set out in Section 1, neither Party may sub contract its obligations under this IDTA without the written consent of the other Party, which may be set out in the Linked Agreement.
- This IDTA does not make the Parties a partnership, nor appoint one Party to act as the agent of the other Party.
- If any Section (or part of a Section) of this IDTA is or becomes illegal, invalid or unenforceable, that will not affect the legality, validity and enforceability of any other Section (or the rest of that Section) of this IDTA.

- If a Party does not enforce, or delays enforcing, its rights or remedies under or in relation to this IDTA, this will not be a waiver of those rights or remedies. In addition, it will not restrict that Party's ability to enforce those or any other right or remedy in future.
- If a Party chooses to waive enforcing a right or remedy under or in relation to this IDTA, then this waiver will only be effective if it is made in writing. Where a Party provides such a written waiver:

it only applies in so far as it explicitly waives specific rights or remedies;

it shall not prevent that Party from exercising those rights or remedies in the future (unless it has explicitly waived its ability to do so); and

it will not prevent that Party from enforcing any other right or remedy in future.

What happens if there is a breach of this IDTA?

26. Breaches of this IDTA
    - Each Party must notify the other Party in writing (and with all relevant details) if it:

has breached this IDTA; or

it should reasonably anticipate that it may breach this IDTA, and provide any information about this which the other Party reasonably requests.

- In this IDTA "Significant Harmful Impact" means that there is more than a minimal risk of a breach of the IDTA causing (directly or indirectly) significant damage to any Relevant Data Subject or the other Party.

27. Breaches of this IDTA by the Importer
    - If the Importer has breached this IDTA, and this has a Significant Harmful Impact, the Importer must take steps Without Undue Delay to end the Significant Harmful Impact, and if that is not possible to reduce the Significant Harmful Impact as much as possible.
    - Until there is no ongoing Significant Harmful Impact on Relevant Data Subjects:

the Exporter must suspend sending Transferred Data to the Importer;

If the Importer is the Exporter's Processor or Sub-Processor: if the Exporter requests, the importer must securely delete all Transferred Data or securely return it to the Exporter (or a third party named by the Exporter); and

if the Importer has transferred on the Transferred Data to a third party receiver under Section 16, and the breach has a Significant Harmful Impact on Relevant Data Subject when it is Processed by or on behalf of that third party receiver, the Importer must:

- notify the third party receiver of the breach and suspend sending it Transferred Data; and
- if the third party receiver is the Importer's Processor or Sub-Processor: make the third party receiver securely delete all Transferred Data being Processed by it or on its behalf, or securely return it to the Importer (or a third party named by the Importer).

- If the breach cannot be corrected Without Undue Delay, so there is no ongoing Significant Harmful Impact on Relevant Data Subjects, the Exporter must end this IDTA under Section 1.

28. Breaches of this IDTA by the Exporter
    - If the Exporter has breached this IDTA, and this has a Significant Harmful Impact, the Exporter must take steps Without Undue Delay to end the Significant Harmful Impact

and if that is not possible to reduce the Significant Harmful Impact as much as possible.
    - Until there is no ongoing risk of a Significant Harmful Impact on Relevant Data Subjects, the Exporter must suspend sending Transferred Data to the Importer.
    - If the breach cannot be corrected Without Undue Delay, so there is no ongoing Significant Harmful Impact on Relevant Data Subjects, the Importer must end this IDTA under Section 1.

Ending the IDTA

29. How to end this IDTA without there being a breach
    - The IDTA will end:

at the end of the Term stated in Table 2: Transfer Details; or

if in Table 2: Transfer Details, the Parties can end this IDTA by providing written notice to the other: at the end of the notice period stated;

at any time that the Parties agree in writing that it will end; or

at the time set out in Section 29.2.

- If the ICO issues a revised Approved IDTA under Section 4, if any Party selected in Table 2 "Ending the IDTA when the Approved IDTA changes", will as a direct result of the changes in the Approved IDTA have a substantial, disproportionate and demonstrable increase in:

its direct costs of performing its obligations under the IDTA; and/or

its risk under the IDTA,

and in either case it has first taken reasonable steps to reduce that cost or risk so that it is not substantial and disproportionate, that Party may end the IDTA at the end of a reasonable notice period, by providing written notice for that period to the other Party before the start date of the revised Approved IDTA.

30. How to end this IDTA if there is a breach
    - A Party may end this IDTA immediately by giving the other Party written notice if:

the other Party has breached this IDTA and this has a Significant Harmful Impact. This includes repeated minor breaches which taken together have a Significant Harmful Impact, and

- the breach can be corrected so there is no Significant Harmful Impact, and the other Party has failed to do so Without Undue Delay (which cannot be more than 14 days of being required to do so in writing); or
- the breach and its Significant Harmful Impact cannot be corrected;

the Importer can no longer comply with Section 8.3, as there are Local Laws which mean it cannot comply with this IDTA and this has a Significant Harmful Impact.

31. What must the Parties do when the IDTA ends?
    - If the parties wish to bring this IDTA to an end or this IDTA ends in accordance with any provision in this IDTA, but the Importer must comply with a Local Law which requires it to continue to keep any Transferred Data then this IDTA will remain in force in respect of any retained Transferred Data for as long as the retained Transferred Data is retained, and the Importer must:

notify the Exporter Without Undue Delay, including details of the relevant Local Law and the required retention period;

retain only the minimum amount of Transferred Data it needs to comply with that Local Law, and the Parties must ensure they maintain the Appropriate Safeguards, and change the Tables and Extra Protection Clauses, together with any TRA to reflect this; and

stop Processing the Transferred Data as soon as permitted by that Local Law and the IDTA will then end and the rest of this Section 29 will apply.

- When this IDTA ends (no matter what the reason is):

the Exporter must stop sending Transferred Data to the Importer; and

if the Importer is the Exporter's Processor or Sub-Processor: the Importer must delete all Transferred Data or securely return it to the Exporter (or a third party named by the Exporter), as instructed by the Exporter;

if the Importer is a Controller and/or not the Exporter's Processor or Sub-Processor: the Importer must securely delete all Transferred Data.

the following provisions will continue in force after this IDTA ends (no matter what the reason is):

- **Section 0** (This IDTA and Linked Agreements);
- **Section 2** (Legal Meaning of Words);
- **Section 6** (Understanding this IDTA);
- **Section 7** (Which laws apply to this IDTA);
- **Section 10** (The ICO);
- Sections 1 and 11.4 (Exporter's obligations);
- Sections 0, 0, 0, 0 and 0 (General Importer obligations);
- Section 1 (Importer's obligations if it is subject to UK Data Protection Laws);
- **Section 17** (Importer's responsibility if it authorised others to perform its obligations);
- **Section 24** (Giving notice);
- **Section 25** (General clauses);
- **Section 31** (What must the Parties do when the IDTA ends);
- **Section 32** (Your liability);
- **Section 33** (How Relevant Data Subjects and the ICO may bring legal claims);
- **Section 34** (Courts legal claims can be brought in);
- **Section 35** (Arbitration); and
- **Section 36** (Legal Glossary).

How to bring a legal claim under this IDTA

32. Your liability
    - The Parties remain fully liable to Relevant Data Subjects for fulfilling their obligations under this IDTA and (if they apply) under UK Data Protection Laws.
    - Each Party (in this Section, "Party One") agrees to be fully liable to Relevant Data Subjects for the entire damage suffered by the Relevant Data Subject, caused directly or indirectly by:

Party One's breach of this IDTA; and/or

where Party One is a Processor, Party One's breach of any provisions regarding its Processing of the Transferred Data in the Linked Agreement;

where Party One is a Controller, a breach of this IDTA by the other Party if it involves Party One's Processing of the Transferred Data (no matter how minimal)

in each case unless Party One can prove it is not in any way responsible for the event giving rise to the damage.

- If one Party has paid compensation to a Relevant Data Subject under Section 2, it is entitled to claim back from the other Party that part of the compensation corresponding to the other Party's responsibility for the damage, so that the compensation is fairly divided between the Parties.
- The Parties do not exclude or restrict their liability under this IDTA or UK Data Protection Laws, on the basis that they have authorised anyone who is not a Party (including a Processor) to perform any of their obligations, and they will remain responsible for performing those obligations.

33. How Relevant Data Subjects and the ICO may bring legal claims
    - The Relevant Data Subjects are entitled to bring claims against the Exporter and/or Importer for breach of the following (including where their Processing of the Transferred Data is involved in a breach of the following by either Party):

- **Section 0** (This IDTA and Linked Agreements);
- **Section 3** (You have provided all the information required by Part one: Tables and Part two: Extra Protection Clauses);
- **Section 8** (The Appropriate Safeguards);
- **Section 9** (Reviews to ensure the Appropriate Safeguards continue);
- **Section 0** (Exporter's obligations);
- **Section 12** (General Importer Obligations);
- **Section 13** (Importer's obligations if it is subject to UK Data Protection Laws);
- **Section 14** (Importer's obligations to comply with key data protection laws);
- **Section 15** (What happens if there is an Importer Personal Data Breach);
- **Section 16** (Transferring on the Transferred Data);
- **Section 17** (Importer's responsibility if it authorises others to perform its obligations);
- **Section 18** (The right to a copy of the IDTA);
- **Section 19** (The Importer's contact details for the Relevant Data Subjects);
- **Section 20** (How Relevant Data Subjects can exercise their data subject rights);
- **Section 21** (How Relevant Data Subjects can exercise their data subject rights– if the Importer is the Exporter's Processor or Sub-Processor);
- **Section 23** (Access Requests and Direct Access);
- **Section 26** (Breaches of this IDTA);
- **Section 27** (Breaches of this IDTA by the Importer);
- **Section 28** (Breaches of this IDTA by the Exporter);
- **Section 30** (How to end this IDTA if there is a breach);
- **Section 31** (What must the Parties do when the IDTA ends); and
- any other provision of the IDTA which expressly or by implication benefits the Relevant Data Subjects.
    - The ICO is entitled to bring claims against the Exporter and/or Importer for breach of the following Sections: Section 10 (The ICO), Sections 1 and 11.2 (Exporter's obligations), Section 0 (General Importer obligations) and Section 13 (Importer's obligations if it is subject to UK Data Protection Laws).
    - No one else (who is not a Party) can enforce any part of this IDTA (including under the Contracts (Rights of Third Parties) Act 1999).
    - The Parties do not need the consent of any Relevant Data Subject or the ICO to make changes to this IDTA, but any changes must be made in accordance with its terms.
    - In bringing a claim under this IDTA, a Relevant Data Subject may be represented by a not-for-profit body, organisation or association under the same conditions set out in

Article 80(1) UK GDPR and sections 187 to 190 of the Data Protection Act 2018.

34. Courts legal claims can be brought in
    - The courts of the UK country set out in Table 2: Transfer Details have non-exclusive jurisdictionover any claim in connection with this IDTA (including non-contractual claims).
    - The Exporter may bring a claim against the Importer in connection with this IDTA (including non-contractual claims) in any court in any country with jurisdiction to hear the claim.
    - The Importer may only bring a claim against the Exporter in connection with this IDTA (including non-contractual claims) in the courts of the UK country set out in the Table 2: Transfer Details
    - Relevant Data Subjects and the ICO may bring a claim against the Exporter and/or the Importer in connection with this IDTA (including non-contractual claims) in any court in any country with jurisdiction to hear the claim.
    - Each Party agrees to provide to the other Party reasonable updates about any claims or complaints brought against it by a Relevant Data Subject or the ICO in connection with the Transferred Data (including claims in arbitration).
35. Arbitration
    - Instead of bringing a claim in a court under Section 34, any Party, or a Relevant Data Subject may elect to refer any dispute arising out of or in connection with this IDTA (including non-contractual claims) to final resolution by arbitration under the Rules of the London Court of International Arbitration, and those Rules are deemed to be incorporated by reference into this Section 35.
    - The Parties agree to submit to any arbitration started by another Party or by a Relevant Data Subject in accordance with this Section 35.
    - There must be only one arbitrator. The arbitrator (1) must be a lawyer qualified to practice law in one or more of England and Wales, or Scotland, or Northern Ireland and (2) must have experience of acting or advising on disputes relating to UK Data Protection Laws.
    - London shall be the seat or legal place of arbitration. It does not matter if the Parties selected a different UK country as the 'primary place for legal claims to be made' in Table 2: Transfer Details.
    - The English language must be used in the arbitral proceedings.
    - English law governs this Section 35. This applies regardless of whether or not the parties selected a different UK country's law as the 'UK country's law that governs the IDTA' in Table 2: Transfer Details.
36. Legal Glossary

Word or Phrase	**Legal definition** **(this is how this word or phrase must be interpreted in the IDTA)**
Access Request	As defined in Section 23, as a legally binding request (except for requests only binding by contract law) to access any Transferred Data.
Adequate Country	A third country, or: · a territory; · one or more sectors or organisations within a third country;

	· an international organisation; which the Secretary of State has specified by regulations provides an adequate level of protection of Personal Data in accordance with Section 17A of the Data Protection Act 2018.
Appropriate Safeguards	The standard of protection over the Transferred Data and of the Relevant Data Subject's rights, which is required by UK Data Protection Laws when you are making a Restricted Transfer relying on standard data protection clauses under Article 46(2)(d) UK GDPR.
Approved IDTA	The template IDTA A1.0 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 5.4.
Commercial Clauses	The commercial clauses set out in Part three.
Controller	As defined in the UK GDPR.
Damage	All material and non-material loss and damage.
Data Subject	As defined in the UK GDPR.
Decision-Making	As defined in Section 20.6, as decisions about the Relevant Data Subjects based solely on automated processing, including profiling, using the Transferred Data.
Direct Access	As defined in Section 23 as direct access to any Transferred Data by public authorities of which the Importer is aware.
Exporter	The exporter identified in Table 1: Parties & Signature.
Extra Protection Clauses	The clauses set out in Part two: Extra Protection Clauses.
ICO	The Information Commissioner.
Importer	The importer identified in Table 1: Parties & Signature.
Importer Data Subject Contact	The Importer Data Subject Contact identified in Table 1: Parties & Signature, which may be updated in accordance with Section 19.
Importer Information	As defined in Section 0, as all relevant information regarding Local Laws and practices and the protections and risks which apply to the Transferred Data when it is Processed by the Importer, including for the Exporter to carry out any TRA.

Importer Personal Data Breach	A 'personal data breach' as defined in UK GDPR, in relation to the Transferred Data when Processed by the Importer.
Linked Agreement	The linked agreements set out in Table 2: Transfer Details (if any).
Local Laws	Laws which are not the laws of the UK and which bind the Importer.
Mandatory Clauses	Part four: Mandatory Clauses of this IDTA.
Notice Period	As set out in Table 2: Transfer Details.
Party/Parties	The parties to this IDTA as set out in Table 1: Parties & Signature.
Personal Data	As defined in the UK GDPR.
Personal Data Breach	As defined in the UK GDPR.
Processing	As defined in the UK GDPR. When the IDTA refers to Processing by the Importer, this includes where a third party Sub-Processor of the Importer is Processing on the Importer's behalf.
Processor	As defined in the UK GDPR.
Purpose	The 'Purpose' set out in Table 2: Transfer Details, including any purposes which are not incompatible with the purposes stated or referred to.
Relevant Data Subject	A Data Subject of the Transferred Data.
Restricted Transfer	A transfer which is covered by Chapter V of the UK GDPR
Review Dates	The review dates or period for the Security Requirements set out in Table 2: Transfer Details, and any review dates set out in any revised Approved IDTA.
Significant Harmful Impact	As defined in Section 26.2 as where there is more than a minimal risk of the breach causing (directly or indirectly) significant harm to any Relevant Data Subject or the other Party.
Special Category Data	As described in the UK GDPR, together with criminal conviction or criminal offence data.

Start Date	As set out in Table 1: Parties and signature.
Sub-Processor	A Processor appointed by another Processor to Process Personal Data on its behalf. This includes Sub-Processors of any level, for example a Sub-Sub-Processor.
Tables	The Tables set out in Part one of this IDTA.
Term	As set out in Table 2: Transfer Details.
Third Party Controller	The Controller of the Transferred Data where the Exporter is a Processor or Sub-Processor If there is not a Third Party Controller this can be disregarded.
Transfer Risk Assessment or TRA	A risk assessment in so far as it is required by UK Data Protection Laws to demonstrate that the IDTA provides the Appropriate Safeguards
Transferred Data	Any Personal Data which the Parties transfer, or intend to transfer under this IDTA, as described in Table 2: Transfer Details
UK Data Protection Laws	All laws relating to data protection, the processing of personal data, privacy and/or electronic communications in force from time to time in the UK, including the UK GDPR and the Data Protection Act 2018.
UK GDPR	As defined in Section 3 of the Data Protection Act 2018.
Without Undue Delay	Without undue delay, as that phase is interpreted in the UK GDPR.

Alternative Part 4 Mandatory Clauses:

Mandatory Clauses	Part 4: Mandatory Clauses of the Approved IDTA, being the template IDTA A.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 5.4 of those Mandatory Clauses.