DATA PROTECTION ADDENDUM - CONTROLLER

This Data Protection Addendum ("Addendum") establishes minimum data protection and cybersecurity standards and related requirements for Customer as that term is defined in the Terms and Conditions for IDT Services (the "Agreement) in connection with the provision of personal data provided to use the IDT rhAmpSeq CRISPR Analysis Tool, between Integrated DNA Technologies, Inc. ("IDT") and Customer, each a "Party" and collectively the "Parties" and is entered into and effective as of the date Customer accepted the Agreement and the terms of this Data Protection Addendum. Capitalized terms not herein defined have the same meaning as set forth in the Agreement.

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

WHEREAS, the Parties acknowledge and agree that Customer is the Controller as defined in the General Data Protection Regulation of the European Union;

WHEREAS, the Parties acknowledge and agree that IDT provides these services through a service provider's ("Service Provider") hosted web platform;

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

1. Definitions.

(A) "Applicable Law" means any law, rule or regulation applicable to the Agreement, the Services, Customer or IDT, and applicable industry standards concerning privacy, data protection, confidentiality, information security, availability and integrity, or the handling or Processing (including retention and disclosure) of Personal Data, as may be amended, regulated, restated or replaced from time to time.

(B) "Covered Information" means, in any form, format or media, any (a) confidential information of Customer; and/or (b) Personal Data of Customer.

(C) "Customer" the entity that accepted the terms of the Agreement through an individual acting on its behalf together with its affiliates that provide Covered Information to receive the Services provided by IDT.

(D) "Data Subject" means the identified or identifiable person to whom Personal Data relates.

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

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

(G) "Personal Data" means all data or information, in any form or format, that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, to an identified or identifiable natural person including but not limited to DNA sequencing information.

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

(I) "Processor" means the entity which Processes Personal Data on behalf of the Controller, including as applicable any Service Provider.

(J) "Services" means those services that IDT performs pursuant to the Agreement.

(K) "Service Provider" means the service provider hosting the web platform Processing Covered Information provided by Customer.

(L) "System" means any system, network, platform, database, computer, or telecommunications or other information system owned, controlled or operated by or on behalf of either Party or any of its Affiliates for the purpose of Processing Covered Information pursuant to the Agreement.

2. Processing of Personal Data. The parties acknowledge and agree that with regard to the Processing of Personal Data, Customer is the Controller, IDT is the Processor and IDT shall Process Personal Data in accordance with the requirements of Data Protection Laws and Regulations, including any applicable requirement to provide notice to Data Subjects of the use of IDT as Processor. For the avoidance of doubt, Customer's instructions for the Processing of Personal Data shall comply with Data Protection Laws and Regulations. Customer shall have the sole responsibility for the accuracy, quality and legality of Personal Data and the means by which Customer acquired Personal Data. Customer specifically acknowledges that its use of the Services will not violate the rights of any Data Subject that has opted-out from sales or other disclosures of Personal Data, to the extent applicable under the CCPA.

3. IDT Processing Personal Data. IDT shall treat Personal Data as Confidential Information and shall Process Personal Data on behalf of and only in accordance with Customer's documented instructions for the following purposes; (i) Processing in accordance with the Agreement; (ii) Processing initiated by Users in their use of the Services; and (iii) Processing to comply with other documented reasonable instructions provided by Customer where such instructions are consistent with the terms of the Agreement.

4. Customer General Requirements. If Customer provides Covered Information to IDT to Process Covered Information in connections with the provision of Services, Customer shall:

(A) obtain any and all necessary rights in and consents required to Process the Covered Information;

(B) evaluate the sufficiency of the data protection and cybersecurity standards provided by IDT to its own satisfaction;

(C) provide any Covered Information to IDT in accordance with Applicable Law;

(D) be responsible for the compliance of its personnel with the terms of this Addendum.

(E) promptly notify IDT of:

(1) any request, inquiry, complaint, notice or communication received from any third party, including a data subject or a supervisory authority, with respect to any Personal Data, and provide instructions to IDT in responding to such request, inquiry, complaint, notice or communication to the extent permitted by Applicable Law. Without limiting the generality of the foregoing, Customer shall notify IDT in writing within five (5) business days of receipt of any Data Subject Request relating to Personal Data Processed by IDT pursuant to the Agreement; and

(2) any substantial changes to the Customer's notices, policies or procedures that would impede IDT's ability to fulfil the terms of this Addendum regarding protection of Personal Data.

5. IDT General Requirements. If IDT Processes Covered Information in connection with the provision of Services, IDT shall:

(A) process Covered Information in accordance with Applicable Law, and solely as permitted by the Agreement and for no other purpose;

(B) maintain the confidentiality of all Covered Information to which it has access as a result of the execution of this Addendum;

(C) be responsible for the compliance of its personnel with the terms of this Addendum;

(D) not disclose Covered Information to third parties:

(1) except in connection with the provision of Services, or

(2) unless required by Applicable Law, in which case IDT shall, to the extent permitted, notify Customer promptly in writing before complying with any such disclosure request and comply with all reasonable directions of Customer with respect to such disclosure.

(E) To the extent legally permitted, promptly notify Customer of:

(1) any request from a Data Subject to exercise the Data Subject's right of access, right to rectification, restriction of Processing, erasure ("right to be forgotten"), data portability, objection to the Procession, or its right not to be subject to an automated individual decision making, each such request being a "Data Subject Request". Taking into account the nature of the Processing, IDT may assist Customer by appropriate technical and organization measures, insofar as this is possible, for the fulfilment of Customer's obligation to respond to a Data Subject Request under Data Protection Laws and Regulations. In addition, to the extent Customer, in its use of the Services, does not have the ability to address a Data Subject Request, IDT may upon Customer's request provide commercially reasonable efforts to assist Customer in responding to such Data Subject Requests, to the extent IDT is legally permitted to do so and the response to such Data Subject Request is required under Data Protection Laws and Regulations. To the extent legally permitted. Customer shall be responsible for the costs arising from IDT's provision of such assistance.

(2) any substantial changes to the IDT's notices, policies or procedures that would impede IDT's ability to fulfil the terms of this Addendum regarding protection of Personal Data;

(F) reasonably assist and cooperate with Customer, including by providing information requested by Customer, to allow Customer to comply with its obligations under Applicable Law;

(G) retain Covered Information only for as long as necessary to perform the Services, and at the end of the provision of the Services, delete or return the Covered Information to Customer unless expressly required otherwise by Applicable Law.

(H) If IDT suspects or becomes aware of a Data Security Incident:

(1) provide Customer written notice without undue delay and no later than twenty-four (24) hours after becoming aware of such suspected or confirmed Data Security Incident;

(2) undertake an investigation of such Data Security Incident and reasonably cooperate with Customer, its regulators and law enforcement agencies;

(3) not make any public announcements relating to such Data Security Incident without Customer's prior written approval, which shall not be unreasonably withheld; and

(4) take all reasonable corrective action in a timely manner, at the expense of IDT, to remediate and prevent a recurrence of such Data Security Incident.

6. Cyber and Information Security. IDT shall establish, maintain and comply with:

(A) Administrative, technical, and physical safeguards designed to ensure the security, confidentiality, reliability and integrity of Covered Information, as well as any Systems, facilities, or software that IDT or Service Provider accesses or supports in connection with the Agreement. Such safeguards should:

(1) be commensurate with the type and amount of Covered Information Processed by IDT, having regard to the state of the art and industry standards, and should, at a minimum, protect Covered Information and Systems against reasonably anticipated threats or hazards, including from unauthorized access, loss, theft, destruction, use, modification, collection, attack, or disclosure;

(2) address the security controls set forth in the Center for Internet Security's Critical Security Controls, formerly known as the SANS Top 20; and

(B) A written security program and policy that meets or exceeds the requirements imposed under Applicable Law and aligns with established industry practices. Such security program and policy should address, at a minimum, the following:

(1) identification of appropriately defined organizational roles related to information security;

(2) controls with respect to the employment of and access given to Covered Information by employees, agents and subcontractors of IDT including background checks, security clearances that assign specific access privileges to individuals, and training regarding the handling of Covered Information;

(3) an appropriate network security program that includes, without limitation, encryption and network and application partitioning;

(4) access identification and authentication;

(5) maintenance and media disposal;

(6) audit and accountability;

(7) physical and environmental protection;

(8) system and communication security;

(9) incident response and planning; and

(10) the integrity and reliability of facilities, systems and services, including critical asset identification, configuration and change management for software systems, and contingency planning/redundancy.

7. International Transfers. IDT shall not transfer any Personal Data from any jurisdiction to any other jurisdiction without having in place a transfer agreement or other mechanism appropriate to comply with Applicable Law. The Standard Contractual Clauses embodied in Annex 1, where executed, shall constitute such a transfer agreement where recognized by Applicable Law, unless another lawful basis for the transfer applies.

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

ANNEX 1

Standard contractual clauses for the transfer of personal data from the Community to third countries

Data Transfers Agreement

between

DATA EXPORTER

Name:…….

Address and Country of Establishment:…….

hereinafter "data **exporter**"

and

DATA IMPORTER

Name:…….

Address and Country of Establishment:…….

hereinafter "data **importer**"

each a "party"; together "the parties".

Definitions

For the purposes of the clauses:

a) "personal data", "special categories of data/sensitive data", "process/processing", "controller", "processor", "data subject" and "supervisory authority/authority" shall have the same meaning as in Directive 95/46/EC of 24 October 1995 (whereby "the authority" shall mean the competent data protection authority in the territory in which the data exporter is established);

b) "the data exporter" shall mean the controller who transfers the personal data;

c) "the data importer" shall mean the controller who agrees to receive from the data exporter personal data for further processing in accordance with the terms of these clauses and who is not subject to a third country's system ensuring adequate protection;

d) "clauses" shall mean these contractual clauses, which are a free-standing document that does not incorporate commercial business terms established by the parties under separate commercial arrangements.

The details of the transfer (as well as the personal data covered) are specified in Annex B, which forms an integral part of the clauses.

I. Obligations of the data exporter

The data exporter warrants and undertakes that:

a) The personal data have been collected, processed and transferred in accordance with the laws applicable to the data exporter.

b) It has used reasonable efforts to determine that the data importer is able to satisfy its legal obligations under these clauses.

c) It will provide the data importer, when so requested, with copies of relevant data protection laws or references to them (where relevant, and not including legal advice) of the country in which the data exporter is established.

d) It will respond to enquiries from data subjects and the authority concerning processing of the personal data by the data importer, unless the parties have agreed that the data importer will so respond, in which case the data exporter will still respond to the extent reasonably possible and with the information reasonably available to it if the data importer is unwilling or unable to respond. Responses will be made within a reasonable time.

e) It will make available, upon request, a copy of the clauses to data subjects who are third party beneficiaries under clause III, unless the clauses contain confidential information, in which case it may remove such information. Where information is removed, the data exporter shall inform data subjects in writing of the reason for removal and of their right to draw the removal to the attention of the authority. However, the data exporter shall abide by a decision of the authority regarding access to the full text of the clauses by data subjects, as long as data subjects have agreed to respect the confidentiality of the confidential information removed. The data exporter shall also provide a copy of the clauses to the authority where required.

II. Obligations of the data importer

The data importer warrants and undertakes that:

a) It will have in place appropriate technical and organisational measures to protect the personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, and which provide a level of security appropriate to the risk represented by the processing and the nature of the data to be protected.

b) It will have in place procedures so that any third party it authorises to have access to the personal data, including processors, will respect and maintain the confidentiality and security of the personal data. Any person acting under the authority of the data importer, including a data processor, shall be obligated to process the personal data only on instructions from the data importer. This provision does not apply to persons authorised or required by law or regulation to have access to the personal data.

c) It has no reason to believe, at the time of entering into these clauses, in the existence of any local laws that would have a substantial adverse effect on the guarantees provided for under these clauses, and it will inform the data exporter (which will pass such notification on to the authority where required) if it becomes aware of any such laws.

d) It will process the personal data for purposes described in Annex B, and has the legal authority to give the warranties and fulfil the undertakings set out in these clauses.

e) It will identify to the data exporter a contact point within its organisation authorised to respond to enquiries concerning processing of the personal data, and will cooperate in good faith with the data exporter, the data subject and the authority concerning all such enquiries within a reasonable time. In case of legal dissolution of the data exporter, or if the parties have so agreed, the data importer will assume responsibility for compliance with the provisions of clause I(e).

f) At the request of the data exporter, it will provide the data exporter with evidence of financial resources sufficient to fulfil its responsibilities under clause III (which may include insurance coverage).

g) Upon reasonable request of the data exporter, it will submit its data processing facilities, data files and documentation needed for processing to reviewing, auditing and/or certifying by the data exporter (or any independent or impartial inspection agents or auditors, selected by the data exporter and not reasonably objected to by the data importer) to ascertain compliance with the warranties and undertakings in these clauses, with reasonable notice and during regular business hours. The request will be subject to any necessary consent or approval from a regulatory or supervisory authority within the country of the data importer, which consent or approval the data importer will attempt to obtain in a timely fashion.

h) It will process the personal data, at its option, in accordance with:

i. the data protection laws of the country in which the data exporter is established, or

ii. the relevant provisions of any Commission decision pursuant to Article 25(6) of Directive 95/46/EC, where the data importer complies with the relevant provisions of such an authorisation or decision and is based in a country to which such an authorisation or decision pertains, but is not covered by such authorisation or decision for the purposes of the transfer(s) of the personal data, or

iii. the data processing principles set forth in Annex A.

Data importer to indicate which option it selects: iii;

Initials of data importer:_____;

i) It will not disclose or transfer the personal data to a third party data controller located outside the European Economic Area (EEA) unless it notifies the data exporter about the transfer and

i. the third party data controller processes the personal data in accordance with a Commission decision finding that a third country provides adequate protection, or

ii. the third party data controller becomes a signatory to these clauses or another data transfer agreement approved by a competent authority in the EU, or

iii. data subjects have been given the opportunity to object, after having been informed of the purposes of the transfer, the categories of recipients and the fact that the countries to which data is exported may have different data protection standards, or

iv. with regard to onward transfers of sensitive data, data subjects have given their unambiguous consent to the onward transfer

III. Liability and third party rights

a) Each party shall be liable to the other parties for damages it causes by any breach of these clauses. Liability as between the parties is limited to actual damage suffered. Punitive damages (i.e. damages intended to punish a party for its outrageous conduct) are specifically excluded. Each party shall be liable to data subjects for damages it causes by any breach of third party rights under these clauses. This does not affect the liability of the data exporter under its data protection law.

b) The parties agree that a data subject shall have the right to enforce as a third party beneficiary this clause and clauses I(b), I(d), I(e), II(a), II(c), II(d), II(e), II(h), II(i), III(a), V, VI(d) and VII against the data importer or the data exporter, for their respective breach of their contractual obligations, with regard to his personal data, and accept jurisdiction for this purpose in the data exporter's country of establishment. In cases involving allegations of breach by the data importer, the data subject must first request the data exporter to take appropriate action to enforce his rights against the data importer; if the data exporter does not take such action within a reasonable period (which under normal circumstances would be one month), the data subject may then enforce his rights against the data importer directly. A data subject is entitled to proceed directly against a data exporter that has failed to use reasonable efforts to determine that the data importer is able to satisfy its legal obligations under these clauses (the data exporter shall have the burden to prove that it took reasonable efforts).

IV. Law applicable to the clauses

These clauses shall be governed by the law of the country in which the data exporter is established, with the exception of the laws and regulations relating to processing of the personal data by the data importer under clause II(h), which shall apply only if so selected by the data importer under that clause.

V. Resolution of disputes with data subjects or the authority

a) In the event of a dispute or claim brought by a data subject or the authority concerning the processing of the personal data against either or both of the parties, the parties will inform each other about any such disputes or claims, and will cooperate with a view to settling them amicably in a timely fashion.

b) The parties agree to respond to any generally available non-binding mediation procedure initiated by a data subject or by the authority. If they do participate in the proceedings, the parties may elect to do so remotely (such as by telephone or other electronic means). The parties also agree to consider participating in any other arbitration, mediation or other dispute resolution proceedings developed for data protection disputes.

c) Each party shall abide by a decision of a competent court of the data exporter's country of establishment or of the authority which is final and against which no further appeal is possible.

VI. Termination

a) In the event that the data importer is in breach of its obligations under these clauses, then the data exporter may temporarily suspend the transfer of personal data to the data importer until the breach is repaired or the contract is terminated.

b) In the event that:

i. the transfer of personal data to the data importer has been temporarily suspended by the data exporter for longer than one month pursuant to paragraph (a);

ii. compliance by the data importer with these clauses would put it in breach of its legal or regulatory obligations in the country of import;

iii. the data importer is in substantial or persistent breach of any warranties or undertakings given by it under these clauses;

iv. a final decision against which no further appeal is possible of a competent court of the data exporter's country of establishment or of the authority rules that there has been a breach of the clauses by the data importer or the data exporter; or

v. a petition is presented for the administration or winding up of the data importer, whether in its personal or business capacity, which petition is not dismissed within the applicable period for such dismissal under applicable law; a winding up order is

made; a receiver is appointed over any of its assets; a trustee in bankruptcy is appointed, if the data importer is an individual; a company voluntary arrangement is commenced by it; or any equivalent event in any jurisdiction occurs

then the data exporter, without prejudice to any other rights which it may have against the data importer, shall be entitled to terminate these clauses, in which case the authority shall be informed where required. In cases covered by (i), (ii), or (iv) above the data importer may also terminate these clauses.

c) Either party may terminate these clauses if (i) any Commission positive adequacy decision under Article 25(6) of Directive 95/46/EC (or any superseding text) is issued in relation to the country (or a sector thereof) to which the data is transferred and processed by the data importer, or (ii) Directive 95/46/EC (or any superseding text) becomes directly applicable in such country.

d) The parties agree that the termination of these clauses at any time, in any circumstances and for whatever reason (except for termination under clause VI(c)) does not exempt them from the obligations and/or conditions under the clauses as regards the processing of the personal data transferred.

VII. Variation of these clauses

The parties may not modify these clauses except to update any information in Annex B, in which case they will inform the authority where required. This does not preclude the parties from adding additional commercial clauses where required.

VIII. Description of the Transfer

The details of the transfer and of the personal data are specified in Annex B. The parties agree that Annex B may contain confidential business information which they will not disclose to third parties, except as required by law or in response to a competent regulatory or government agency, or as required under clause I(e). The parties may execute additional annexes to cover additional transfers, which will be submitted to the authority where required. Annex B may, in the alternative, be drafted to cover multiple transfers.

ANNEX A of the Standard Contractual Clauses

DATA PROCESSING PRINCIPLES

1. Purpose limitation: Personal data may be processed and subsequently used or further communicated only for purposes described in Annex B or subsequently authorised by the data subject.

2. Data quality and proportionality: Personal data must be accurate and, where necessary, kept up to date. The personal data must be adequate, relevant and not excessive in relation to the purposes for which they are transferred and further processed.

3. Transparency: Data subjects must be provided with information necessary to ensure fair processing (such as information about the purposes of processing and about the transfer), unless such information has already been given by the data exporter.

4. Security and confidentiality: Technical and organisational security measures must be taken by the data controller that are appropriate to the risks, such as against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, presented by the processing. Any person acting under the authority of the data controller, including a processor, must not process the data except on instructions from the data controller.

5. Rights of access, rectification, deletion and objection: As provided in Article 12 of Directive 95/46/EC, data subjects must, whether directly or via a third party, be provided with the personal information about them that an organisation holds, except for requests which are manifestly abusive, based on unreasonable intervals or their number or repetitive or systematic nature, or for which access need not be granted under the law of the country of the data exporter. Provided that the authority has given its prior approval, access need also not be granted when doing so would be likely to seriously harm the interests of the data importer or other organisations dealing with the data importer and such interests are not overridden by the interests for fundamental rights and freedoms of the data subject. The sources of the personal data need not be identified when this is not possible by reasonable efforts, or where the rights of persons other than the individual would be violated. Data subjects must be able to have the personal information about them rectified, amended, or deleted where it is inaccurate or processed against these principles. If there are compelling grounds to doubt the legitimacy of the request, the organisation may require further justifications before proceeding to rectification, amendment or deletion. Notification of any rectification, amendment or deletion to third parties to whom the data have been disclosed need not be made when this involves a disproportionate effort. A data subject must also be able to object to the processing of the personal data relating to him if there are compelling legitimate grounds relating to his particular situation. The burden of proof for any refusal rests on the data importer, and the data subject may always challenge a refusal before the authority.

6. Sensitive data: The data importer shall take such additional measures (e.g. relating to security) as are necessary to protect such sensitive data in accordance with its obligations under clause II.

7. Data used for marketing purposes: Where data are processed for the purposes of direct marketing, effective procedures should exist allowing the data subject at any time to "opt-out" from having his data used for such purposes.

8. Automated decisions: For purposes hereof "automated decision" shall mean a decision by the data exporter or the data importer which produces legal effects concerning a data subject or significantly affects a data subject and which is based solely on automated processing of personal data intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct, etc. The data importer shall not make any automated decisions concerning data subjects, except when:

   a)

      i. such decisions are made by the data importer in entering into or performing a contract with the data subject, and

ii. the data subject is given an opportunity to discuss the results of a relevant automated decision with a representative of the parties making such decision or otherwise to make representations to that parties.

or

b) where otherwise provided by the law of the data exporter.

ANNEX B of the Standard Contractual Clauses

DESCRIPTION OF THE TRANSFER

Data subjects
The personal data transferred concerns the following categories of data subjects:

……

……

Purposes of the transfer(s)
The transfer is made for the following purposes:

……

……

Categories of data
The personal data transferred concern the following categories of data:

……

……

Recipients
The personal data transferred may be disclosed only to the following recipients or categories of recipients:

……

……

Sensitive data
The personal data transferred concern the following categories of sensitive data:

……

……

Additional Useful Information
(storage limites and other relevant information, as applicable)

……

……

Contact points for data protection enquiries