DATA PROCESSING ADDENDUM

This Data Processing Addendum ("**DPA**") is an agreement between _____ ("**Customer**" or "**Data Controller**") and Igentify Ltd. ("**Igentify**" or "**Data Processor**"). The Parties agree that this DPA shall be added as an addendum to the End User License Agreement executed between the Parties on _____, according to which Igentify shall provide to the Customer certain data processing services, as described therein (respectively, the "**Services**" and the "**Services Agreement**"). This DPA shall apply where the EU General Data Protection Regulation 2016/679 of the European Parliament and of the Council ("**GDPR**") applies to Personal Data (as such term is defined below) processed by Igentify in order to provide the Services to the Customer. Data Controller and Data Processor shall be collectively referred to as the "**Parties**", and each a "**Party**".

1. **Definitions**. In this DPA, the following terms shall have the meanings set out below and cognate terms shall be construed accordingly:

1.1 "**Affiliate(s)**" means an entity that owns or controls, is owned or controlled by or is or under common control or ownership of either Party, where control is defined as the possession, directly or indirectly, of the power to direct or cause the direction of the management and policies of an entity, whether through ownership of voting securities, by contract or otherwise;

1.2 "**Applicable Laws**" means any applicable law, including Data Protection Laws, to which Data Processor is subject with respect to any Personal Data;

1.3 "**Data Protection Laws**" means the GDPR, as transposed into domestic legislation of each Member State of the European Economic Area and in each case as amended, replaced or superseded from time to time, and if applicable the Israeli privacy law;

1.4 "**EEA**" means the European Economic Area;

1.5 "**Personal Data**" means any information relating to an identified or identifiable natural person ("**Data Subject**") (an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person), which is Processed by Data Processor or any of Data Processor's Sub-processors on behalf of Data Controller as part of the performance of the Services under the Services Agreement, all to the extent that such data is subject to the GDPR;

1.6 "**Personal Data Breach**" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise processed;

1.7 "**Processing**" means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

1.8 "**Standard Contractual Clauses**" means the standard contractual clauses for the transfer of Personal Data laid down by the European Commission, as updated, amended, replaced or superseded from time to time by the European Commission;

1.9 "**Sub-processor**" means any third party (but excluding an employee of Data Processor) appointed by or on behalf of Data Processor to Process Personal Data for the benefit of Data Controller as part of the performance of the Services under the Services Agreement;

1.10 "**Supervisory Authority**" means (a) an independent public authority which is established by a Member State of the European Economic Area pursuant to Article 51 of the GDPR; and (b) any similar regulatory authority responsible for the enforcement of Data Protection Laws; and

1.11 "**Term**" shall have the meaning ascribed to it under Section 11 below.

2. Processing of Personal Data.

2.1 Data Processor, and any person acting under its authority, will carry out the Personal Data Processing activities, including with regard to transfers of Personal Data to a third country or an international organisation, only for the following purposes: (i) to provide the Services during the Term in accordance with the Services Agreement and other reasonable documented instructions provided by the Data Controller, where such instructions are consistent with the terms of the Services Agreement (collectively, the "**Instructions**"); and (ii) as required under Applicable Law, in which case Data Processor shall, to the extent permitted by Applicable Law, inform Data Controller of such legally required Processing of Personal Data, unless that law prohibits such information on important grounds of public interest.

2.2 Data Controller instructs Data Processor (and authorises Data Processor to instruct each of its Sub-processors) to process the Personal Data, as reasonably necessary for the provision of the Services and in accordance with the Services Agreement and this DPA. Additional Instructions outside the scope of this DPA and the Services Agreement require prior written agreement between Data Controller and Data Processor and will include any additional fees that may be payable by the Data Controller to the Data Processor for carrying out such Instructions.

2.3 Data Controller hereby acknowledges that as part of the provision of the Services hereunder, Data Processor may collect, disclose, publish, share and otherwise use fully anonymized, de-identified and de-identifiable data, including statistical data, analytics, trends and other aggregated data which derives from the Personal Data processed by the Data Processor as part of the provision of the Services, all as required for the Data Processor's legitimate purposes, including without limitation in order to provide, maintain, operate and improve the Services and for research purposes. The Data Controller hereby agrees and acknowledges that such processing activities (including the anonymization and de-identification of Personal Data) will not be considered as performed outside the scope of the Instructions provided by the Data Controller hereunder. Data Processor agrees not to use said anonymized data in a form that identifies the Customer or any Data Subject.

2.4 Data Processor will notify Data Controller if Data Processor is of the opinion that a written Instruction received from Data Controller is in violation of Applicable Law and/or in violation of contractual duties under the Services Agreement.

2.5 Data Processor shall treat Personal Data as confidential information and will not disclose, make available or transfer the Personal Data to any third party, other than as permitted under this DPA.

2.6 Data Controller shall have sole responsibility for the accuracy, quality and legality of the Personal Data and the means by which Data Controller acquired the Personal Data. Data Controller warrants and undertakes that: (i) the Personal Data has been collected, Processed and transferred in accordance with the laws applicable to Data Controller, including, if required by applicable law, that Data Controller has received all required consents from the applicable Data Subjects for the Processing carried out by the Data Processor under this DPA and the Data Subjects have been informed that their Personal Data could be transmitted to a third country outside of the EU/EEA; and (ii) it will provide Data Processor, 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 Data Controller is established or which may otherwise be relevant to the Personal Data concerned.

2.7 **Exhibit 1** of this DPA sets forth certain information regarding Data Processor's Processing activities of the Personal Data, as required by Article 28(3) of the GDPR.

3. Data Subjects.

3.1 Data Processor shall promptly notify Data Controller if Data Processor receives a request from a Data Subject to exercise the Data Subject's rights under Data Protection Laws, including without limitation the right of access, rectification, restriction of Processing, erasure, data portability, object to the Processing, or its right not to be subject to an automated individual decision making ("**Data Subject Request**"), and shall not respond to such request without Data

Controller's prior written consent, except to confirm that such request relates to Data Controller.

3.2 Taking into account the nature of the Processing, Data Processor has implemented in the Services certain measures to assist the Data Controller in independently fulfilling its obligation to respond to certain Data Subject Requests. However, due to technical limitations and the nature of the Services, not all Data Subject Requests may be exercised independently by the Data Controller via the Services. To the extent that Data Controller, while using the Services, does not have the ability to address a Data Subject Request, Data Controller shall contact the Data Processor via the dedicated "Help Center" link embedded in the Service, and subject to Section 10.1 below, the Data Processor shall, upon Data Controller's request, assist Data Controller in responding to such Data Subject Request.

4. **Supervising Authorities.** Data Processor shall provide reasonable assistance to Data Controller with any data protection impact assessments, and prior consultations with Supervising Authorities, as required by article 35 and 36 of the GDPR or equivalent provisions of any other Data Protection Law, in each case solely in relation to the Processing of Personal Data by Data Processor and all by taking into account the nature of the Processing and information available to the Data Processor. Data Controller acknowledges and agrees that assistance with data protection impact assessments and prior consultations by Data Processor may result in additional fees (which will be notified to Data Controller in advance).

5. **Security Breach Notification.**

5.1 Data Processor shall notify Data Controller without undue delay, and in any case within forty-eight (48) hours, after becoming aware of a Personal Data Breach affecting the Personal Data.

5.2 Data Processor shall provide Data Controller with sufficient information to allow Data Controller to meet any obligations to report or inform Supervising Authorities and Data Subjects of the Personal Data Breach under the Data Protection Laws, taking into account the nature of Processing and the information available to Data Processor, including with the following information: (a) a description of the nature of the Personal Data Breach, including the categories and approximate number of both Data Subjects and Personal Data records concerned; (b) the likely consequences of the Personal Data Breach; and (c) a description of the measures taken, or proposed to be taken, to address the Personal Data Breach, including measures to mitigate its possible adverse effects. To the extent Data Processor does not have full information about the Personal Data Breach at the time of the initial notification, Data Processor shall provide an initial notification and then supplement that with additional information as it becomes available.

6. **Audit.**

6.1 During the Term, Data Processor shall keep records of its Processing activities in accordance with applicable Data Protection Laws.

6.2 During the Term and upon request, Data Processor shall make available to Data Controller all information necessary to demonstrate compliance with the obligations laid down in Article 28 of the GDPR and allow for and contribute to audits, including inspections, conducted by Data Controller or another auditor mandated by Data Controller, all at Data Controller's sole expense and only in order to ensure Data Processor's compliance with the obligations laid down in Article 28 of the GDPR and this DPA. If and to the extent Data Controller engages third parties to conduct the audit, such third parties must be bound to strict confidentiality obligations. Notwithstanding the above, Data Controller shall only be entitled to conduct such inspection during business hours and no more than once during one calendar year, provided that Data Controller shall be entitled to conduct such inspection at any time if it reasonably suspects Data Processor to be in material breach of its obligations under this DPA and that nothing in this Section shall limit the timing and scope of any audit required to be conducted by applicable Data Protection Laws.

6.3 Data Controller shall provide Data Processor a reasonable prior written notice of any audit or inspection to be conducted under this Section and shall avoid (and ensure that each of its auditors avoids) causing any damage, injury or disruption to Data Processor's premises, equipment,

personnel and business while its personnel are on those premises in the course of such audit or inspection.

6.4 It is agreed that a copy of this DPA may be forwarded to the relevant Supervisory Authority, if required under applicable Data Protection Laws. Furthermore, the Parties agree that such authority has the right to conduct an audit of the Parties with respect to the subject matter of this DPA.

6.5 Nothing in this DPA will require Data Processor either to disclose to Data Controller (and/or its authorized auditors), or provide access to: (i) any data of any other customer of Data Processor; (ii) Data Processor's internal accounting or financial information; (iii) any trade secret of Data Processor; or (iv) any information that, in Data Processor's sole discretion, could compromise the security of any of Data Processor's systems or premises or cause Data Processor to breach obligations under any Applicable Law or its obligations to any third party.

7. Sub-processing.

7.1 Data Controller hereby (i) grants Data Processor a general authorization to engage (and permits each Sub-processor appointed in accordance with this Section to engage) Sub-processors for the purpose of providing the Services; (ii) agrees that Affiliates of Data Processor (including without limitation Igentify Inc.) may be used as Sub-processors; and (iii) confirms that Data Processor may continue to use those Sub-processors already engaged by Data Processor as of the Effective Date of this DPA, which are detailed in Igentify website (www.Igentify.com) under "Igentify Subsidiaries and Sub-Processors".

7.2 Data Processor can at any time and without justification appoint a new Sub-processor, provided that prior to engaging any Sub-processor:

(a) Data Processor will provide a fourteen (14) days' prior notice to Data Controller regarding the engagement of a new Sub-processor, and the Data Controller does not reasonably object to such changes within that timeframe under legitimate and documented grounds. If, in Data Processor's sole discretion, Data Controller's objection to an engagement of a Sub-processor is legitimate, Data Processor shall either refrain from using such Sub-processor in the context of the Processing of Personal Data, or shall notify Data Controller that it is unable to provide the Services without the use of such Sub-processor and therefore it will suspend or restrict the Services (or an applicable part thereof) with immediate effect.

(b) Data Processor ensures that it has in place a sub-processing agreement between Data Processor and the Sub-processor, that is no less protective with respect to Data Controller's interest and protection of Personal Data than this DPA. Upon Data Controller's request, Data Processor shall provide Data Controller with an updated list of Sub-processors.

7.3 Where the Sub-processor fails to fulfil its personal data protection obligations with respect to the Personal Data, Data Processor shall remain fully liable to Data Controller for the performance of that Sub-processor's obligations.

8. Transfers. The Data Processor warrants that where Personal Data is transferred outside of the EEA, it will be processed in accordance with the provisions of the Standard Contractual Clauses or Binding Corporate Rules, unless the processing takes place: (i) in a third country or territory recognised by the EU Commission to have an adequate level of protection; or (ii) by an organisation located in a country which has other legally recognised appropriate safeguards in place, such as the EU-US Privacy Shield framework.

9. Personnel. Data Processor will be responsible for using qualified personnel with data protection training to provide the Services and ensure that Data Processor's access to the Personal Data is limited only to those personnel who require such access to perform the Services. Data Processor shall obligate its personnel to Process the relevant Personal Data only in accordance with this DPA. Data Processor will further ensure that its personnel authorised to Process the Personal Data on its behalf: (i) will do so only on a need-to-know basis; and (ii) have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality,

and that they will keep confidential and will not make available any Personal Data to any third party, other than as permitted herein.

10. **Security.** Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing, as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Data Processor will implement technical and organizational security measures in order to ensure a level of security appropriate to that risk, including, as appropriate, the measures referred to in Article 32(1) of the GDPR, as stipulated in **Exhibit 2** of this DPA. The technical and organizational security measures are aimed at protecting Personal Data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access and against all other unlawful forms of Processing. The technical and organizational security measures are subject to technical progress and development and the Data Processor may update or modify technical and organizational security measures from time to time, provided that such updates and modifications do not result in the degradation of the overall security of the Services.

10.1 **Deletion and Return of Personal Data.** Within ten (10) days following the termination of the Services Agreement and/or this DPA, Data Processor will delete or return to Data Controller, and instruct its Sub-processors to delete or return, all existing copies of the Personal Data which are in its possession. Data Processor may retain the Personal Data to the extent required by Applicable Laws and only to the extent and for such period as required by Applicable Laws and always provided that Data Processor shall ensure the confidentiality of all such Personal Data and shall ensure that such Personal Data is only Processed as necessary for the purpose(s) specified in the Applicable Laws requiring its storage and for no other purpose. In addition, Data Controller hereby agrees that Data Processor may retain one copy of the Personal Data for a period of 7 years following the termination of Processing thereof, solely for the establishment, exercise or defence of legal claims, and provided that such copy of the Personal Data is fully encrypted and under strict access privileges.

11. **Term.** This DPA shall become effective upon execution or acceptance of the Services Agreement ("**Effective Date**") and shall remain in full force until the later of the date when Data Processor ceases to Process the Personal Data or termination of the Services Agreement (the "**Term**"). All provisions of this DPA, which by their language or nature should survive the termination of this DPA, will survive the termination of this DPA.

12. **Limitation of Liability.** Each Party's liability arising out of or related to this DPA, whether in contract, tort or under any other theory of liability, is subject to the 'Limitation of Liability' section of the Services Agreement governing the Services.

13. **Changes to this DPA.** The Parties may amend this DPA from time to time by mutual agreement of both Parties, and subject to compliance with any required obligations under applicable Data Protection Laws.

14. **Miscellaneous.** (i) This DPA represents the complete agreement concerning the subject matter hereof; (ii) except where explicitly agreed otherwise in writing by the Parties, in the event of inconsistencies between the provisions of this DPA and any other agreements between the Parties, including the Services Agreement and any other agreements which may be entered into or purported to be entered into after the date of this DPA, the provisions of this DPA shall prevail; (iii) the Parties to this DPA hereby agree to the governing law and the choice of jurisdiction stipulated in the Services Agreement with respect to any disputes or claims arising under this DPA; (iv) nothing in this DPA reduces either Party's obligations under the Services Agreement in relation to the protection of Personal Data; and (v) should any provision of this DPA be invalid or unenforceable, then the remainder of this DPA shall remain valid and in force. The invalid or unenforceable provision shall be either (a) amended as necessary to ensure its validity and enforceability, while preserving the Parties' intentions as closely as possible or, if this is not possible, (b) construed in a manner as if the invalid or unenforceable part had never been contained therein.

EXECUTION

The Parties have shown their acceptance of the terms of this Data Processing Agreement by executing it below:

SIGNED by: _____

duly authorised for and on behalf-of: _____

SIGNED by _____

duly authorised for and on behalf-of: _IGENTIFY LTD AND AFFILIATES_

EXHIBIT 1

DETAILS OF PROCESSING OF PERSONAL DATA

1. **Subject matter of the Processing:** The subject matter of the Processing of the Personal Data is as set forth in the Services Agreement, and as supplemented by this DPA.
2. **Duration:** As between Igentify and Customer, the duration of the data processing activities under this DPA is determined by the Customer.
3. **The purpose of the Processing**: The purpose of the data processing under this DPA is the provision of the Services, as set forth in the Services Agreement, and as supplemented by this DPA.
4. **Nature of the Processing**: digital genetic test analysis, including machine-generated personalized genetic counselling and such other Services as set forth in the Services Agreement.
5. **Type of Personal Data**: Personal Data related to the Customer's clients (e.g., patients) and other related family members of such clients, including genetic data and any other personal information uploaded to the Services under the Customer's account in Igentify's Services.
6. **Categories of data subjects**: The Data Subjects include the Customer's clients (e.g., patients) and other related family members of such clients.

EXHIBIT 2

TECHNICAL AND ORGANIZATIONAL MEASURES

Description of the technical and organizational security measures implemented by Data Processor according to Section 10 of the DPA:

Domain	Practices
Organization of Information Security	**Security Ownership**. Igentify has appointed security and privacy officers responsible for coordinating and monitoring the security and privacy rules and procedures as follows: - Chief Information Security Officer (CISO) - Data Privacy Officer (DPO) **Security Roles and Responsibilities**. Igentify personnel with access to Personal Data are subject to confidentiality obligations. **Risk Management Program**. Igentify performs a continuous a security and privacy risk assessment on its platform. **Retention**. Igentify retains its security documents pursuant to its retention requirements after they are no longer in effect.
Asset Management	**Asset Inventory**. Igentify maintains an inventory of all Information and Technological assets and access rights to all items in the inventory. Access to the inventory is restricted to authorized Igentify personnel only. **Asset Handling** - Igentify classifies all Personal Data as Confidential. - Igentify strictly restricts and controls access to Personal Data to authorized Igentify personnel only. - Igentify has established procedures that define how to process Personal Data, including instructions for secure anonymization of Personal Data and secure use of anonymized data.
Human Resources Security	**Security Training**. - Igentify trains its personnel about relevant security and privacy procedures according to their respective roles and access rights. - Igentify also informs its personnel of possible consequences of breaching the security rules and procedures.
Physical and Environmental Security	**Physical Access to Facilities**. No Personal Data is stored in Igentify facilities, all production environments being hosted on AWS. Igentify limits access to information systems that can access Personal Data. **Protection from Disruptions**. Igentify uses high availability services in order to protect against loss of data due to infrastructure failure.
Customer Environment Security	**Platform Security** - Igentify establishes security areas by using dedicated AWS Virtual Private Cloud for each customer. - Igentify establishes access authorizations for employees and third parties. - All access to the AWS accounts where Personal Data are hosted is logged, monitored, and tracked. - Personal Data hosted on AWS cloud are secured by appropriate security measures based on AWS best practices. - Personal Data hosted on AWS cloud is encrypted at rest, and when in transit.
Communications and Operations Management	**Operational Policy**. Igentify maintains security documents describing its security measures and the relevant procedures and responsibilities of its personnel who have access to Personal Data. **Data Recovery Procedures** Igentify implements suitable measures in order to ensure that Personal Data are protected from accidental destruction or loss and the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident. This is accomplished by: - Infrastructure redundancy: the cluster and Database are deployed in a minimum of 2 instances. - Database snapshots are stored on highly available storage S3 in AWS.

Domain	Practices
	- Performance of periodical restore tests. **Malicious Software**. Igentify has anti-malware controls to help avoid malicious software gaining unauthorized access to personal workstations, including malicious software originating from public networks. **Data Beyond Boundaries.** Igentify encrypts Personal Data that is transmitted over public networks. **Event Logging**. Igentify logs access and use of information systems containing Personal Data, registering the access ID, time, authorization granted or denied, and relevant activity.
Access Control	**Access Policy**. Igentify maintains a record of security privileges of individuals having access to Personal Data. **Access Authorization** - Igentify maintains and updates a record of personnel authorized to access all Igentify systems. - Igentify identifies those personnel who may grant, alter or cancel authorized access to data and resources. - Igentify ensures that where more than one individual has access to systems processing Personal Data, the individuals have separate identifiers/log-ins. - Igentify performs periodical access rights reviews. **Least Privilege** - Technical support personnel are only permitted to access Personal Data when needed. - Igentify restricts access to Personal Data to only those individuals who require such access to perform their job function. **Integrity and Confidentiality** - Igentify instructs Igentify personnel to disable administrative sessions when not in use - Igentify protects system passwords. **Authentication** - Igentify uses industry standard practices to identify and authenticate users who attempt to access information systems. - Where authentication mechanisms are based on passwords, Igentify requires that the passwords are renewed regularly. - Where authentication mechanisms are based on passwords, Igentify requires the password to be at least eight characters long. - Igentify ensures that de-activated or expired identifiers are not granted to other individuals. - Igentify monitors repeated attempts to gain access to the information system using an invalid password. - Igentify uses best practices to deactivate passwords that have been corrupted or inadvertently disclosed.
Information Security Incident Management	**Incident Response Process** - Igentify maintains a record of security incidents with a description of the incident, the time period, the consequences of the incident, the name of the reporter, and to whom the incident was reported, and the procedure for recovering data when relevant - For each security incident that is a Data Breach, notification by Igentify (as described in the section 5 of this DPA) will be made without undue delay and, in any event, within 48 hours. - Igentify analyses security incidents with the purpose to improve security controls and measures
Business Continuity Management	**Business Continuity** - Igentify maintains a Business Continuity Plan for the information systems that process Personal Data. - Igentify maintains infrastructure redundancy and procedures for backup and data recovery.
Information Security review	**Verification of Compliance with the organization's information security policies and standards** - Igentify performs Penetration Testing on the platform at least once a year. - Igentify regularly monitors the environment infrastructure for compliance. - Igentify performs Information Security internal audit once a year