DATA PROCESSING AGREEMENT

This Data Processing Agreement (“Agreement”) forms an integral part of the Merchant Terms.

It is entered into by and between:

UAB "Maneuver LT", a company registered in Lithuania, bearing company registration number 304785124, having its company address at Žalgirio street 92-510, LT-09303 Vilnius, Lithuania, hereinafter referred to as **"Company" or “Processor”**, and

the Merchant, being any legal entity or individual entrepreneur that has opened a business account with Genome and accepted the Merchant Terms, hereinafter referred to as **"Client"** or **"You" or “Controller”**;

By accepting the Merchant Terms, the Merchant also enters into this Data Processing Agreement, which shall apply to the extent that Company processes personal data on behalf of the Merchant.

In consideration of the mutual obligations set out herein, and in further consideration of the promises, covenants, conditions and mutual obligations hereinafter contained, the Company and the Client agree and covenant as follows:

1. Definitions

1.1 In this **Agreement**, the following terms shall have the meanings set out below and cognate terms shall be construed accordingly:

1.1.1 "Applicable Laws" means (a) European Union or Member State laws with respect to any Merchant’s Customer Data in respect of which Controller is subject to EU Data Protection Laws; and (b) any other applicable law with respect to any Merchant’s Customer Data in respect of which Controller is subject to any other Data Protection Laws;

1.1.2 "Controller Affiliate" means an entity that owns or controls, is owned or controlled by or is or under common control or ownership with Controller, 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;

1.1.3 "Merchant’s Customer Data" means any Personal Data Processed by a Contracted Processor on behalf of a Controller Group Member pursuant to or in connection with this Agreement;

1.1.4 "Contracted Processor" means Processor or a Subprocessor;

1.1.5 "Data Protection Laws" means EU Data Protection Laws and, to the extent applicable, the data protection or privacy laws of any other country;

1.1.6 "EEA" means the European Economic Area;

1.1.7 "EU Data Protection Laws" means EU Directive 95/46/EC, as transposed into domestic legislation of each Member State and as amended, replaced or superseded from time to time, including by the GDPR and laws implementing or supplementing the GDPR;

1.1.8 "GDPR" means EU General Data Protection Regulation 2016/679;

1.1.9 "Restricted Transfer" means:

1.1.9.1 a transfer of Merchant’s Customer Data from any Controller Group Member to a Contracted Processor; or

1.1.9.2 an onward transfer of Merchant’s Customer Data from a Contracted Processor to a Contracted Processor, or between two establishments of a Contracted

Processor,

1.1.9.3 in each case, where such transfer would be prohibited by Data Protection Laws (or by the terms of data transfer agreements put in place to address the data transfer restrictions of Data Protection Laws) in the absence of the Standard Contractual Clauses to be established under section 6.4.3 or 12 below;

1.1.10 "Services" means the services and other activities to be supplied to or carried out by or on behalf of Processor for Controller pursuant to this Agreement;

1.1.11 "Standard Contractual Clauses" means the standard contractual clauses for the transfer of personal data to third countries adopted by the European Commission pursuant to Article 46 of the GDPR, namely the clauses set out in Commission Implementing Decision (EU) 2021/914 of 4 June 2021;

1.1.12 "Subprocessor" means any person (including any third party and any Processor Affiliate, but excluding an employee of Processor or any of its sub-contractors) appointed by or on behalf of Processor or any Processor Affiliate to Process Personal Data on behalf of Controller in connection with this Agreement; and

1.1.13 "Processor Affiliate" means an entity that owns or controls, is owned or controlled by or is or under common control or ownership with Processor, 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 The terms, "Commission", "Controller", "Data Subject", "Member State", "Personal Data", "Personal Data Breach", "Processing" and "Supervisory Authority" shall have the same meaning as in the GDPR, and their cognate terms shall be construed accordingly.

1.3 The word "include" shall be construed to mean include without limitation, and cognate terms shall be construed accordingly.

2. Authority

Processor warrants and represents that, before any Processor Affiliate Processes any Merchant’s Customer Data on behalf of Controller, Processor's entry into this Agreement as agent for and on behalf of that Processor Affiliate will have been duly and effectively authorised (or subsequently ratified) by that Processor Affiliate.

3. Processing of Merchant’s Customer Data

3.1 Processor and each Processor Affiliate shall:

3.1.1 comply with all applicable Data Protection Laws in the Processing of Merchant’s Customer Data; and

3.1.2 not Process Merchant’s Customer Data other than on the Controller’s documented instructions unless Processing is required by Applicable Laws to which the relevant Contracted Processor is subject, in which case Processor or the relevant Processor Affiliate shall to the extent permitted by Applicable Laws inform the Controller of that legal requirement before the relevant Processing of that Personal Data.

3.2 Controller:

3.2.1 instructs Processor and each Processor Affiliate (and authorises Processor and each Processor Affiliate to instruct each Subprocessor) to:

3.2.1.1 Process Merchant’s Customer Data; and

3.2.1.2 in particular, transfer Merchant’s Customer Data to any country or territory,

3.3 as reasonably necessary for the provision of the Services and consistent with this Agreement. Annex 1 to this Agreement sets out certain information regarding the Contracted Processors' Processing of the

Merchant's Customer Data as required by article 28(3) of the GDPR (and, possibly, equivalent requirements of other Data Protection Laws). Controller may make reasonable amendments to Annex 1 by written notice to Processor from time to time as Controller reasonably considers necessary to meet those requirements.

4. Processor and Processor Affiliate Personnel

Processor and each Processor Affiliate shall take reasonable steps to ensure the reliability of any employee, agent or contractor of any Contracted Processor who may have access to the Merchant's Customer Data, ensuring in each case that access is strictly limited to those individuals who need to know / access the relevant Merchant's Customer Data, as strictly necessary for the purposes of this Agreement, and to comply with Applicable Laws in the context of that individual's duties to the Contracted Processor, ensuring that all such individuals are subject to confidentiality undertakings or professional or statutory obligations of confidentiality.

5. Security

5.1 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, Processor and each Processor Affiliate shall in relation to the Merchant's Customer Data implement appropriate technical and organizational measures to ensure a level of security appropriate to that risk, including, as appropriate, the measures referred to in Article 32(1) of the GDPR.

5.2 In assessing the appropriate level of security, Processor and each Processor Affiliate shall take account in particular of the risks that are presented by Processing, in particular from a Personal Data Breach.

5.3 Processor warrants and represents that, before the processing Merchant's Customer Data, Contracted Processor has implemented the technical and organisational security measures specified in Annex 2.

6. Subprocessing

6.1 The Controller grants to the Processor and each Processor Affiliate a general authorisation to engage Subprocessors for the Processing of Merchant's Customer Data under this Agreement.

6.2 The Processor shall maintain an up-to-date list of authorised Subprocessors and shall inform the Controller of any intended changes concerning the addition or replacement of Subprocessors. The Controller shall ensure that its Customers are informed, through the Controller's Privacy Notice or otherwise, that Subprocessors may be engaged for the provision of the Services.

6.3 The Processor shall ensure that each Subprocessor is bound by a written agreement imposing data protection obligations no less protective than those set out in this Agreement, including Article 28(3) GDPR requirements.

6.4 The Processor and each Processor Affiliate shall carry out adequate due diligence before appointing a Subprocessor to ensure that such Subprocessor can provide appropriate technical and organisational measures to meet the requirements of GDPR and this Agreement.

6.5 Where the engagement of a Subprocessor involves a Restricted Transfer, the Processor shall ensure that appropriate safeguards are in place, including the execution of the European Commission-approved Standard Contractual Clauses where required.

6.6 The Processor shall remain fully liable to the Controller for the performance of the Subprocessor's obligations as if performed by the Processor itself.

7. Data Subject Rights

7.1 Taking into account the nature of the Processing, Processor and each Processor Affiliate shall assist Controller by implementing appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Controller’s obligations, as reasonably understood by Controller, to respond to requests to exercise Data Subject rights under the Data Protection Laws.

7.2 Processor shall:

7.2.1 promptly notify Controller if any Contracted Processor receives a request from a Data Subject under any Data Protection Law in respect of Merchant’s Customer Data; and

7.2.2 ensure that the Contracted Processor does not respond to that request except on the documented instructions of Controller or as required by Applicable Laws to which the Contracted Processor is subject, in which case Processor shall to the extent permitted by Applicable Laws inform Controller of that legal requirement before the Contracted Processor responds to the request.

7.3 Controller warrants that it will obtain prior consent from Data Subjects or has another relevant legal basis (e.g. contract or legitimate interest) to collect, use and process their personal data if such information transferred to the Company (Processor). If Client (Controller) discloses personal data without relevant legal basis, it shall be responsible for that unauthorized disclosure in accordance with Data Protection Laws.

7.4 Controller should check if its privacy policy duly discloses its data practices and complies with Data Protection Laws.

8. Personal Data Breach

8.1 Processor shall notify Controller without undue delay upon Processor or any Subprocessor becoming aware of a Personal Data Breach affecting Merchant’s Customer Data, providing Controller with sufficient information to allow Controller to meet any obligations to report or inform Data Subjects of the Personal Data Breach under the Data Protection Laws.

8.2 Such notification shall as a minimum:

8.2.1 describe the nature of the Personal Data Breach, the categories and numbers of Data Subjects concerned, and the categories and numbers of Personal Data records concerned;

8.2.2 communicate the name and contact details of Processor's Data Protection Officer or other relevant contact from whom more information may be obtained;

8.3 Processor shall co-operate with Controller and take such reasonable commercial steps as are directed by Controller to assist in the investigation, mitigation and remediation of each such Personal Data Breach.

9. Data Protection Impact Assessment and Prior Consultation

Processor and each Processor Affiliate shall provide reasonable assistance to Controller with any data protection impact assessments, and prior consultations with Supervising Authorities or other competent data privacy authorities, which Controller reasonably considers to be required by article 35 or 36 of the GDPR or equivalent provisions of any other Data Protection Law, in each case solely in relation to Processing of Merchant’s Customer Data by, and taking into account the nature of the Processing and information available to, the Contracted Processors.

10. Deletion or return of Merchant’s Customer Data

10.1 Subject to sections 10.2 and 10.3 Processor and each Processor Affiliate shall promptly and in any event within 10 (ten) business days of the date of cessation of any Services involving the Processing of Merchant’s Customer Data (the "Cessation Date"), delete (for avoidance of any doubt, “delete” here means to remove or obliterate Personal Data such that it cannot be recovered or reconstructed) and procure the deletion of all copies of those Merchant’s Customer Data.

10.2 Subject to section 10.3, Controller may in its absolute discretion by written notice to Processor within 10 (ten) business days of the Cessation Date require Processor and each Processor Affiliate to (a) return a complete copy of all Merchant’s Customer Data to Controller by secure file transfer in such format as is reasonably notified by Controller to Processor; and (b) delete and procure the deletion of all other copies of Merchant’s Customer Data Processed by any Contracted Processor. Processor and each Processor Affiliate shall comply with any such written request within 10 (ten) business days of the Cessation Date.

10.3 Each Contracted Processor may retain Merchant’s Customer 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 Processor and each Processor Affiliate shall ensure the confidentiality of all such Merchant’s Customer Data and shall ensure that such Merchant’s Customer Data is only Processed as necessary for the purpose(s) specified in the Applicable Laws requiring its storage and for no other purpose.

10.4 Processor shall provide written certification to Controller that it and each Processor Affiliate has fully complied with this section 10 within 10 (ten) business days of the Cessation Date.

11. Audit rights

11.1 Subject to sections 11.2 to 11.3, Processor and each Processor Affiliate shall make available to Controller on request all information necessary to demonstrate compliance with this Agreement, and shall allow for and contribute to audits, including inspections, by Controller or an auditor mandated by Controller in relation to the Processing of the Merchant’s Customer Data by the Contracted Processors.

11.2 Information and audit rights of the Controller only arise under section 11.1 to the extent that this Agreement does not otherwise give them information and audit rights meeting the relevant requirements of Data Protection Law (including, where applicable, article 28(3)(h) of the GDPR).

11.3 Controller undertaking an audit shall give Processor or the relevant Processor Affiliate reasonable notice of any audit or inspection to be conducted under section 11.1 and shall make (and ensure that each of its mandated auditors makes) reasonable endeavours to avoid causing (or, if it cannot avoid, to minimise) any damage, injury or disruption to the Contracted Processors' premises, equipment, personnel and business while its personnel are on those premises in the course of such an audit or inspection. A Contracted Processor need not give access to its premises for the purposes of such an audit or inspection:

11.3.1 to any individual unless he or she produces reasonable evidence of identity and authority;

11.3.2 outside normal business hours at those premises, unless the audit or inspection needs to be conducted on an emergency basis and Controller undertaking an audit has given notice to Processor or the relevant Processor Affiliate that this is the case before attendance outside those hours begins; or

11.3.3 for the purposes of more than one audit or inspection, in respect of each Contracted Processor, in any calendar year, except for any additional audits or inspections which:

11.3.3.1 Controller undertaking an audit reasonably considers necessary because of genuine concerns as to Processor's or the relevant Processor Affiliate’s compliance with this Agreement; or

11.3.3.2 Controller is required or requested to carry out by Data Protection Law, a Supervisory Authority or any similar regulatory authority responsible for the enforcement of Data Protection Laws in any country or territory,

11.3.4 where Controller undertaking an audit has identified its concerns or the relevant requirement or request in its notice to Processor or the relevant Processor Affiliate of the audit or inspection.

12. General Terms

12.1 The parties to this Agreement hereby submit to the competent courts of Lithuania with respect to any disputes or claims howsoever arising under this Agreement, including disputes regarding its existence, validity or termination or the consequences of its nullity. This Agreement and all non-contractual or other obligations arising out of or in connection with it are governed by the laws of Lithuania.

12.2 Nothing in this Agreement reduces Processor's or any Processor Affiliate's obligations under this Agreement in relation to the protection of Personal Data or permits Processor or any Processor Affiliate to Process (or permit the Processing of) Personal Data in a manner which is prohibited by this Agreement.

12.3 Subject to section 12.2, with regard to the subject matter of this Agreement, in the event of inconsistencies between the provisions of this Agreement and any other agreements between the parties, including this Agreement and including (except where explicitly agreed otherwise in writing, signed on behalf of the parties) agreements entered into or purported to be entered into after the date of this Agreement, the provisions of this Agreement shall prevail.

12.4 Controller may propose any variations to this Agreement which Controller reasonably considers to be necessary to address the requirements of any Data Protection Law.

12.5 If Controller gives notice under section 12.4, the parties shall promptly discuss the proposed variations and negotiate in good faith with a view to agreeing and implementing those or alternative variations designed to address the requirements identified in Controller's notice as soon as is reasonably practicable.

12.6 Processor shall not require the consent or approval of any Processor Affiliate to amend this Agreement pursuant to this section 12.5 or otherwise.

12.7 Should any provision of this Agreement be invalid or unenforceable, then the remainder of this Agreement shall remain valid and in force. The invalid or unenforceable provision shall be either (i) amended as necessary to ensure its validity and enforceability, while preserving the parties' intentions as closely as possible or, if this is not possible, (ii) construed in a manner as if the invalid or unenforceable part had never been contained therein.

ANNEX 1: DETAILS OF PROCESSING OF MERCHANT'S CUSTOMERS PERSONAL DATA

Subject matter and duration of the Processing of Merchant's Customer's Data

The subject matter and duration of the Processing of the Merchant's Customer Data are set out in this Agreement and in the Merchant Terms. Processing is carried out for the duration of the Merchant's contractual relationship with Company and as long as required by applicable laws.

The nature and purpose of the Processing of Merchant's Customer's Personal Data

Company processes personal data on behalf of the Merchant for the purposes of:

- enabling payment collection service,
- enabling payment processing,
- transmitting transaction-related data to the Merchant,
- complying with applicable financial services regulations.

The types of Merchant's Customer's Personal Data to be Processed

- *First name and last name*
- *Email address*
- *Phone number*
- *Full address (street, house/apartment number, ZIP code, city, country)*

The categories of Data Subject to whom the Merchant's Customer's Personal Data relates

- Customers of the Merchant who initiate transactions using Company's payment services.

The obligations and rights of Merchant's Customer's

The obligations and rights of Merchant's Customer's are set out in this Agreement and the Merchant Terms.

ANNEX 2: SECURITY MEASURES ADOPTED BY THE COMPANY

1. Physical access control

Technical and organisational security measures to prevent unauthorised persons from gaining access to the data processing systems available in premises and facilities (including databases, application servers and related hardware), where Personal Data are processed, include:

- establishing security areas
- restriction of access paths
- establishing access authorisations for employees and third parties
- access control system (ID reader, magnetic card, chip card)
- key management, card-keys procedures
- door locking (electric door openers etc.)
- security staff, janitors
- surveillance facilities, alarm system
- securing decentralized data processing equipment and personal computers

2. Virtual access control

Technical and organisational security measures to prevent data processing systems from being used by unauthorised persons include:

- user identification and authentication procedures
- ID/password security procedures (special characters, minimum length, change of password)
- automatic blocking (e.g. password or timeout)
- monitoring of break-in-attempts and automatic turn-off of the user ID upon several erroneous passwords attempts

3. Data access control

Technical and organisational security measures to ensure that persons entitled to use a data processing system gain access only to such Personal Data in accordance with their access rights, and that Personal Data cannot be read, copied, modified or deleted without authorization, include:

- internal policies and procedures
- control authorisation schemes
- differentiated access rights (profiles, roles, transactions and objects)
- monitoring and logging of accesses
- disciplinary action against employees who access Personal Data without authorisation
- reports of access
- access procedure
- change procedure
- deletion procedure

4. Disclosure control

Technical and organisational security measures to ensure that Personal Data cannot be read, copied, modified or deleted without authorisation during electronic transmission, transport or storage on storage media (manual or electronic), and that it can be verified to which companies or other legal entities Personal Data are disclosed, include:

- tunneling
- logging
- transport security

5. Entry control

Technical and organisational security measures to monitor whether data have been entered, changed or removed (deleted), and by whom, from data processing systems, include:

- logging and reporting systems
- audit trails and documentation

6. Control of instructions

Technical and organisational security measures to ensure that Personal Data are processed solely in accordance with the Instructions of the Controller include:

- unambiguous wording of the contract
- formal commissioning (request form)
- criteria for selecting sub-Processor

7. Availability control

Technical and organisational security measures to ensure that Personal Data are protected against accidental destruction or loss (physical/logical) include:

- backup procedures
- mirroring of hard disks (e.g. RAID technology)
- uninterruptible power supply (UPS)
- remote storage
- anti-virus/firewall systems

8. Separation control

Technical and organisational security measures to ensure that Personal Data collected for different purposes can be processed separately include:

- segregation of functions (production/testing)
- procedures for storage, amendment, deletion, transmission of data for different purposes.