DATA PROCESSING AGREEMENT

(CONTROLLER TO PROCESSOR)

FOR DNASTREAM SERVICES

VERSION 2.2.1 – FEBRUARY 2024

DNASTREAM Limited, Surrey Technology Centre,
40 Occam Road, The Surrey Research Park, Guildford, Surrey, GU2 7YG
Tel: +44 (0)1483 685540 | Fax: +44 (0)1483 573704
www.dnastream.com

This data processing agreement (**"this Agreement"**) sets forth the obligations of Service Provider and Customer with respect to Processing of Personal Data by Service Provider for Customer in connection with the provision of Services by DNASTREAM to Customer under the Service Agreement.

This Agreement shall be incorporated by reference into the Service Agreement.

IT IS AGREED as follows:

1. Definitions and Interpretation

1.1 In this Agreement, unless the context otherwise requires, the following expressions have the following meanings:

"Customer"	means the party identified as such in the Service Agreement;
"Data Controller"	shall have the meaning given to the term "controller" in Section 6 of the Data Protection Act 2018;
"Data Processor"	shall have the meaning given to the term "processor" in Article 4 of the UK GDPR;
"Data Protection Legislation"	means all applicable legislation in force from time to time in the United Kingdom applicable to data protection and privacy including, but not limited to: a) to the extent the UK GDPR applies, the law of the United Kingdom or a part of the United Kingdom which relates to protection of personal data, including but not limited to the UK GDPR, the Data Protection Act 2018 (and regulations made thereunder) and the Privacy and Electronic Communications Regulations 2003 as amended; b) to the extent the EU GDPR applies, the law of the European Union or any member state of the European Union which relates to protection of personal data; and c) the guidance and codes of practice issued by the Information Commissioner under the UK GDPR or a Supervisory Authority under the EU GDPR which are applicable to a Party;
"Data Subject"	shall have the meaning given to the term "data subject" in Article 4 of the UK GDPR;
"EEA"	means the European Economic Area, consisting of all EU Member States plus Iceland, Liechtenstein, and Norway;
"EU GDPR"	means the General Data Protection Regulation ((EU) 2016/679), as it has effect in European Union law;
"EU SCCs"	means the standard contractual clauses relating to the transfer of Personal Data outside of the EEA as issued by the European Commission to fulfil the requirements in Article 28(3) and (4) of EU GDPR;
"IDT Addendum"	means the International Data Transfer Addendum to the European Commission's SCCs as published by the Information Commissioner from time to time under Section 119A(1) of the Data Protection Act 2018;
"IDT Agreement"	means the International Data Transfer Addendum as published by the Information Commissioner from time to time under Section 119A(1) of the Data Protection Act 2018;
"Information Commissioner"	means the Information Commissioner, as defined in Article 4(A3) of the UK GDPR and Section 114 of the Data Protection Act 2018;

"Model Clauses"	means contractual clauses for the transfer of Personal Data to a third country outside of the UK or EEA to ensure appropriate data protection safeguards that are: a) approved for use pursuant to UK GDPR or otherwise approved for use by the Information Commissioner, including but not limited to IDT Agreement and IDT Addendum; or b) approved for use pursuant EU GDPR or otherwise approved for use by the European Commission, including the EU SCCs; as may from time to time be amended;
"Personal Data Breach"	shall have the meaning given to the term "personal data breach" in Article 4 of the UK GDPR;
"Personal Data"	means all such "personal data", as defined in Article 4 of the UK GDPR, as is, or is to be, processed by the Service Provider on behalf of the Data Controller in connection with the Service Agreement;
"Processing", "Process", "Processes", "Processed"	shall have the meaning given to the term "processing" in Article 4 of the UK GDPR;
"Service Agreement"	means the agreement between Service Provider and Customer for the provision of Services by Service Provider to Customer, into which this Agreement shall be incorporated;
"Services"	means those services described in the Service Agreement which are provided by Service Provider to Customer and which Customer uses for the purposes described in the Service Agreement;
"Service Provider"	means DNASTREAM Limited, a limited company registered in England and Wales under number 5887312 whose registered address is Surrey Technology Centre, 40 Occam Road, The Surrey Research Park, Guildford, GU2 7YG;
"Subprocessor"	means any individual or entity appointed by or on behalf of Service Provider to Process Personal Data in connection with this Agreement;
"Supervisory Authority"	shall have the meaning given to it under Article 4(21) of the EU GDPR;
"Term"	means the term of this Agreement, as set out in Clause 17; and
"UK GDPR"	means the retained EU law version of the General Data Protection Regulation ((EU) 2016/679), as it forms part of the law of England and Wales, Scotland, and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018 and as amended by Schedule 1 to the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 (SI 2019/419).

1.2 Unless the context otherwise requires, each reference in this Agreement to:

a) "writing", and any cognate expression, includes a reference to any communication effected by electronic or facsimile transmission or similar means;

b) a statute or a provision of a statute is a reference to that statute or provision as amended or re-enacted at the relevant time;

c) "this Agreement" is a reference to this Agreement and each of the Schedules as amended or supplemented at the relevant time;

d) a Schedule is a schedule to this Agreement;

e) a Clause or paragraph is a reference to a Clause of this Agreement (other than the Schedules) or a paragraph of the relevant Schedule; and

f) a "Party" or the "Parties" refers to the parties to this Agreement.

1.3 The headings used in this Agreement are for convenience only and shall have no effect upon the interpretation of this Agreement.

1.4 Any words following the expressions “include”, “includes”, “including”, “in particular” and any similar expressions or words will be construed without limitation and accordingly will not limit the meaning of the words preceding them.

1.5 Words imparting the singular number shall include the plural and vice versa.

1.6 References to any gender shall include any other gender.

1.7 References to persons shall include corporations.

2. Scope and Application of this Agreement

2.1 Customer shall be the Data Controller and Service Provider shall be the Data Processor.

2.2 The provisions of this Agreement shall apply to the Processing of the Personal Data in connection with the applicable Service Agreement, carried out for Customer by Service Provider, and to all Personal Data held by Service Provider in relation to all such Processing at any time.

2.3 The provisions of this Agreement shall be deemed to be incorporated into the Service Agreement as if expressly set out in it. Subject to sub-Clause 2.4, definitions and interpretations set out in the Service Agreement shall apply to the interpretation of this Agreement.

2.4 In the event of any conflict or ambiguity between any of the provisions of this Agreement and the Service Agreement, the provisions of this Agreement shall prevail.

3. Provision of the Services and Processing Personal Data

3.1 Schedule 1 describes the type(s) of Personal Data, the category or categories of Data Subject, the nature of Processing to be carried out, the purpose(s) of Processing, and the duration of Processing.

3.2 Subject to sub-Clause 4.1, Service Provider is only to carry out Services, and only to Process Personal Data received from Customer:

a) for the purposes of those Services and not for any other purpose;

b) to the extent and in such a manner as is necessary for those purposes; and

c) strictly in accordance with the express written authorisation and instructions of Customer (which may be specific instructions or instructions of a general nature or as otherwise notified by Customer to Service Provider).

3.3 Customer shall retain control of Personal Data at all times and shall remain responsible for its compliance with Data Protection Legislation including, but not limited to, its collection, holding, and Processing of Personal Data, having in place all necessary and appropriate consents and notices to enable the lawful transfer of Personal Data to Service Provider, and with respect to the written instructions given to Service Provider.

4. Obligations of Service Provider

4.1 As set out above in Clause 3, Service Provider shall only Process Personal Data to the extent and in such a manner as is necessary for the purposes of providing Services and not for any other purpose. All instructions given by Customer to Service Provider shall be made in writing and shall at all times be in compliance with Data Protection Legislation. Service Provider shall act only on such written instructions from Customer unless Service Provider is required by domestic law to do otherwise (as per Article 29 of the UK GDPR) (in which case, unless prohibited from doing so by law, Service Provider shall inform Customer of the legal requirement in question before Processing Personal Data for that purpose).

4.2 Service Provider shall not Process Personal Data in any manner which does not comply with the provisions of this Agreement or with Data Protection Legislation. Service Provider must inform Customer promptly if, in its opinion, any instructions given by Customer do not comply with Data Protection Legislation.

4.3 Subject to sub-Clause 4.2, Service Provider shall promptly comply with any written request from Customer requiring Service Provider to amend, transfer, delete (or otherwise dispose of), or to otherwise Process Personal Data.

4.4 Service Provider shall promptly comply with any written request from Customer requiring Service Provider to stop, mitigate, or remedy any unauthorised Processing involving Personal Data.

4.5 Service Provider shall provide all reasonable assistance (at its own cost) to Customer in complying with its obligations under Data Protection Legislation including, but not limited to, the protection of Data Subjects' rights, the security of Processing, the notification of Personal Data Breaches, the conduct of data protection impact assessments, and in dealings with the Information Commissioner (including, but not limited to, consultations with the Information Commissioner where a data protection impact assessment indicates that there is a high risk which cannot be mitigated).

4.6 For the purposes of sub-Clause 4.5, "all reasonable assistance" shall take account of the nature of Processing carried out by Service Provider and the information available to Service Provider.

4.7 If Service Provider becomes aware of any changes to Data Protection Legislation that may, in its reasonable interpretation, adversely impact its performance of Services and Processing of Personal Data either under the Service Agreement or under this Agreement, Service Provider shall inform Customer promptly.

5. Confidentiality

5.1 Service Provider shall maintain Personal Data in confidence, and in particular, unless Customer has given written consent for Service Provider to do so, Service Provider shall not disclose Personal Data to any third party. Service Provider shall not Process or make any use of Personal Data supplied to it by Customer otherwise than as necessary and for the purposes of the provision of Services to Customer.

5.2 Nothing in this Agreement shall prevent Service Provider from complying with any requirement to disclose or Process Personal Data where such disclosure or Processing is required by domestic law, court, or regulator (including, but not limited to, the Information Commissioner). In such cases, Service Provider shall promptly notify Customer of the disclosure or Processing requirements prior to disclosure or Processing (unless such notification is prohibited by domestic law) in order that Customer may challenge the requirement if it wishes to do so.

5.3 Service Provider shall ensure that all employees and subcontractors who are to access and/or Process Personal Data are informed of its confidential nature and are contractually obliged to keep Personal Data confidential.

6. Employees and Data Protection Officers

6.1 Customer shall appoint a data protection officer in accordance with Article 37 of the UK GDPR, whose details shall from time to time be provided to Service Provider.

6.2 Service Provider has appointed a data protection officer in accordance with Article 37 of the UK GDPR, whose details are as follows: Paul Windsor, dpo@dnastream.com.

6.3 Service Provider shall ensure that all employees who are to access and/or Process Personal Data are given suitable training on Data Protection Legislation, Service Provider's obligations under it, their obligations under it, and its application to their work, with particular regard to Processing of Personal Data under this Agreement.

7. Security of Processing

7.1 Service Provider shall implement appropriate technical and organisational measures as described in Schedule 2 and take all steps necessary to protect Personal Data against unauthorised or unlawful Processing or accidental or unlawful loss, destruction, or damage. Customer acknowledges that Service Provider may update such measures from time to time upon reasonable notice to Customer to reflect improvements or changing practices (provided that the updates do not materially decrease Service Provider's obligations as compared to those previously in place).

7.2 The measures implemented by Service Provider shall be appropriate to the nature of Personal Data to be Processed, to the harm that may result from such unauthorised or unlawful Processing or accidental

or unlawful loss, destruction, or damage (in particular to the rights and freedoms of Data Subjects) and shall have regard for the state of technological development and the costs of implementation.

7.3 The measures implemented by Service Provider may include, as appropriate, pseudonymisation and encryption of Personal Data; the ability to ensure the ongoing confidentiality, integrity, availability, and resilience of Processing systems and services; the ability to restore the availability of and access to Personal Data in a timely manner in the event of a physical or technical incident; and a process for regularly testing, assessing, and evaluating the effectiveness of the technical and organisational measures.

7.4 Service Provider shall, if so requested by Customer (and within the timescales required by Customer) supply further details of the technical and organisational systems in place to safeguard the security of Personal Data held and to prevent unauthorised access.

8. Data Subject Rights and Complaints

8.1 Service Provider shall take appropriate technical and organisational measures and provide all reasonable assistance (at Service Provider's cost) to Customer in complying with its obligations under Data Protection Legislation with particular regard to the following:

a) the rights of Data Subjects under Data Protection Legislation including, but not limited to, the right of access (data subject access requests), the right to rectification, the right to erasure, portability rights, the right to object to Processing, rights relating to automated Processing, and rights to restrict Processing; and

b) compliance with notices served on Customer by the Information Commissioner pursuant to Data Protection Legislation.

8.2 If Service Provider receives any notice, complaint, or other communication relating to Personal Data Processing or to either Party's compliance with Data Protection Legislation, it shall notify Customer immediately in writing.

8.3 If Service Provider receives any request from a Data Subject to exercise any of their rights under Data Protection Legislation including, but not limited to, a data subject access request, it shall notify Customer without undue delay.

8.4 Service Provider shall cooperate fully (at Service Provider's cost) with Customer and provide all reasonable assistance in responding to any complaint, notice, other communication, or Data Subject request, including by:

a) providing Customer with full details of the complaint or request;

b) providing the necessary information and assistance in order to comply with a subject access request;

c) providing Customer with any Personal Data it holds in relation to a Data Subject (within the timescales required by Customer); and

d) providing Customer with any other relevant information requested by Customer.

8.5 Service Provider shall act only on Customer's instructions and shall not disclose any Personal Data to any Data Subject or to any other party except as instructed in writing by Customer, or as required by domestic law.

9. Personal Data Breaches

9.1 Service Provider shall immediately (and without undue delay) notify Customer in writing if it suspects or becomes aware of any form of Personal Data Breach including, but not limited to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data.

9.2 If Service Provider becomes aware of a Personal Data Breach, it shall provide the following information to Customer in writing without undue delay:

a) a description of the Personal Data Breach including the category or categories of Personal Data involved, the number (approximate or exact, if known) of Personal Data records involved, and the number (approximate or exact, if known) of Data Subjects involved;

b) the likely consequences of the Personal Data Breach; and

c) a description of the measures it has taken to address the Personal Data Breach, including, where appropriate, measures to mitigate its possible adverse effects.

9.3 In the event of a Personal Data Breach as described above, the Parties shall cooperate with one another to investigate it. Service Provider shall provide all reasonable assistance to Customer including, but not limited to:

a) assisting Customer with its investigation of the Personal Data Breach;

b) providing and facilitating Customer with access to any relevant facilities, operations, and personnel (including, if applicable, former personnel involved in the Personal Data Breach);

c) making available all records, logs, files, reports, and similar as reasonably required by Customer or as otherwise required by Data Protection Legislation; and

d) promptly taking all reasonable steps to mitigate the effects of the Personal Data Breach and to minimise any damage caused by it.

9.4 Service Provider shall use all reasonable endeavours to restore any Personal Data lost, destroyed, damaged, corrupted, or otherwise rendered unusable in the Personal Data Breach as soon as possible after becoming aware of the Personal Data Breach.

9.5 Service Provider shall not inform any third party of any Personal Data Breach as described above without the express written consent of Customer unless it is required to do so by domestic law.

9.6 Customer shall have the sole right to determine whether or not to notify affected Data Subjects, the Information Commissioner, law enforcement agencies, or other applicable regulators of the Personal Data Breach as required by law or other applicable regulations, or at Customer's discretion, including the form of such notification.

9.7 Customer shall have the sole right to determine whether or not to offer any remedy to Data Subjects affected by the Personal Data Breach, including the form and amount of such remedy.

9.8 Subject to the provisions of Clause 16, Service Provider shall bear all reasonable costs and expenses incurred by it and shall reimburse Customer for all reasonable costs and expenses incurred by Customer in responding to the Personal Data Breach, including the exercise of any functions or carrying out of any obligations by tCustomer under any provision of this Clause 9, unless the Personal Data Breach resulted from the Customer's express written instructions, negligence, breach of this Agreement, or other act or omission of Customer, in which case Customer shall instead bear and shall reimburse Service Provider with such costs and expenses incurred by it.

10. Personal Data Transfers Outside of the UK, Switzerland, and the EEA

10.1 Service Provider (and any Subprocessor appointed by it under Clause 11) may not transfer or authorise the transfer of Personal Data to countries outside the UK, Switzerland, and the EEA without the written consent of Customer.

10.2 Where there is a transfer of Personal Data (whether to Service Provider or to a Subprocessor appointed by it under Clause 11) in a country outside of the UK, Switzerland, and the EEA who is not subject to a third country's system covered by UK adequacy regulations issued under Section 17A of the Data Protection Act 2018 or Paragraphs 4 and 5 of Schedule 21 of the Data Protection Act 2018, Service Provider shall enter into Model Clauses appropriate to the transfer of Personal Data with the party receiving Personal Data. Model Clauses shall apply to Personal Data originating from Service Provider (who shall be deemed to be the "Exporter") that is Processed by Service Provider or Subprocessor (who shall be deemed to be the "Importer").

10.3 If there is any conflict between the provisions of Model Clauses and this Agreement, the provisions of Model Clauses shall prevail.

11. Subprocessors

11.1 Service Provider shall not appoint any new Subprocessor without the prior written consent of Customer. Customer gives general consent for Service Provider to appoint the Subprocessors listed in Schedule

3, as may be amended from time to time by the Service Provider in accordance with this Agreement.

11.2 If Service Provider intends to appoint a Subprocessor to Process any Personal Data, Service Provider shall:

a) promptly notify Customer of its intention to appoint a Subprocessor or notify Customer without undue delay of the appointment of a Subprocessor if direct involvement of such Subprocessor is necessary for maintaining the availability and security of Services;

b) enter into a written agreement with each Subprocessor, which shall impose upon the Subprocessor the same obligations, on substantially the same terms, as are imposed upon Service Provider by this Agreement, particularly with regard to technical and organisational security measures required to comply with Data Protection Legislation, which shall permit both Service Provider and Customer to enforce those obligations, and which shall terminate automatically on the termination of this Agreement for any reason;

c) at the written request of Customer, provide copies of such agreements or, as applicable, the relevant parts thereof;

d) ensure that all Subprocessors comply fully with their obligations under the abovementioned agreement and under Data Protection Legislation; and

e) maintain control over all Personal Data transferred to Subprocessors.

11.3 If Customer objects to the appointment of a new Subprocessor on a reasonable basis related to Processing of Personal Data:

a) Customer must notify Service Provider in writing within fifteen (15) days after receiving an appointment notice; otherwise, Service Provider shall deem the appointment of the new Subprocessor authorised by Customer;

b) upon receipt of an objection notice from the Customer, Service Provider shall use reasonable efforts to make available to Customer an alternative Subprocessor;

c) if Service Provider cannot address Customer's objection pursuant to the foregoing efforts, Service Provider shall notify Customer within fifteen (15) days of receipt of Customer's objection notice. Customer may then, by written notice to Service Provider within thirty (30) days of Service Provider's notice, terminate this Agreement and the Service Agreement but Customer shall not be entitled to any refund of prepaid fees covering the terminated portion of the Service Agreement and shall pay all fees payable up to the date of termination of the Service Agreement.

11.4 If a Subprocessor fails to meet its data protection obligations, Service Provider shall remain fully liable to Customer for the Subprocessor's compliance with its data protection obligations.

11.5 Service Provider shall be deemed to legally control any and all Personal Data that may be at any time controlled practically by, or be in the possession of, any Subprocessor appointed by it under this Clause 11.

12. Return and/or Deletion or Disposal of Personal Data

12.1 Service Provider shall, at the written request of Customer (and at Customer's choice), securely delete (or otherwise dispose of) Personal Data or return it to Customer in the format(s) reasonably requested by Customer in accordance with the Service Agreement within a reasonable time after the earlier of the following:

a) the termination of the Service Agreement, for any reason; or

b) Processing of that Personal Data by the Service Provider is no longer required for the performance of Service Provider's obligations under the Service Agreement.

12.2 Subject to sub-Clause 12.3, Service Provider shall not retain all or any part of Personal Data after deleting (or otherwise disposing of) or returning it under sub-Clause 12.1.

12.3 If Service Provider is required to retain copies of all or any part of Personal Data by law, regulation, government, or other regulatory body, it shall inform Customer of such requirement(s) in writing, including precise details of Personal Data that it is required to retain, the legal basis for the retention,

details of the duration of the retention, and when the retained Personal Data will be deleted (or otherwise disposed of) once it is no longer required to retain it.

12.4 Upon the deletion (or disposal) of Personal Data, Service Provider shall certify the completion of the same in writing to Customer within thirty (30) days of the deletion (or disposal).

13. Information

13.1 Service Provider shall make available to Customer any and all such information as is reasonably required and necessary to demonstrate Service Provider's compliance with Data Protection Legislation and this Agreement.

14. Audits

14.1 Service Provider shall, on reasonable prior notice, allow Customer or a third-party auditor appointed by Customer ("Auditing Party") to audit Service Provider's compliance with its obligations under this Agreement and with Data Protection Legislation.

14.2 Service Provider shall provide all necessary assistance (at Customer's cost) in the conduct of such audits including, but not limited to:

a) access (including physical and remote) to, and copies of, all relevant information kept by Service Provider;

b) access to all of its personnel who are to access and/or Process any Personal Data including, where reasonably necessary, arranging interviews between Customer or Auditing Party and such personnel; and

c) reasonable access to and the inspection of all infrastructure, equipment, software, and other systems used to store and/or Process Personal Data.

14.3 The requirement for Customer to give notice under sub-Clause 14.1 shall not apply if Customer has reason to believe that Service Provider is in breach of any of its obligations under this Agreement or under Data Protection Legislation, or if it has reason to believe that a Personal Data Breach has taken place or is taking place.

14.4 Service Provider must inform Customer promptly if, in its opinion, any instructions given by the Auditing Party do not comply with Data Protection Legislation.

14.5 Any audit performed by the Auditing Party shall not cause any damage, injury, or disruption to Service Provider's premises, equipment, or business operations.

15. Warranties

15.1 Customer hereby warrants and represents that:

a) Personal Data and its use with respect to the Service Agreement and this Agreement shall comply with Data Protection Legislation in all respects including, but not limited to, its collection, holding, and Processing; and

b) Customer has, and will continue to have, all necessary rights, permissions and consents with regard to the Processing of Personal Data.

15.2 Service Provider hereby warrants and represents that:

a) Personal Data shall be Processed by Service Provider (and by any Subprocessor appointed by it under Clause 11) in compliance with Data Protection Legislation and any and all other relevant laws, regulations, enactments, orders, standards, and other similar instruments;

b) it has no reason to believe that Data Protection Legislation in any way prevents it from complying with its obligations under the Service Agreement; and

c) it will implement and maintain appropriate technical and organisational measures to protect the Personal Data against unauthorised or unlawful Processing or accidental or unlawful loss, destruction, or damage, as set out in Clause 7 and described in Schedule 2.

16. Liability and Indemnity

16.1 Customer shall be liable for, and shall indemnify (and keep indemnified) Service Provider in respect of,

any and all actions, proceedings, liabilities, costs, claims, losses, expenses (including reasonable legal fees and payments on a solicitor and client basis), or demands, suffered or incurred by, awarded against, or agreed to be paid by, Service Provider and any Subprocessor appointed by Service Provider under Clause 11 arising directly or in connection with:

a) any non-compliance by Customer with Data Protection Legislation;

b) any Personal Data Processing carried out by Service Provider (or any Subprocessor appointed by Service Provider under Clause 11) in accordance with instructions given by Customer to the extent that the instructions infringe Data Protection Legislation; or

c) any breach by Customer of its obligations or warranties under this Agreement;

but not to the extent that the same is or are contributed to by any non-compliance by Service Provider or any Subprocessor appointed by Service Provider under Clause 11 with Data Protection Legislation or its breach of this Agreement.

16.2 Service Provider shall be liable for, and shall indemnify (and keep indemnified) Customer in respect of, any and all actions, proceedings, liabilities, costs, claims, losses, expenses (including reasonable legal fees and payments on a solicitor and client basis), or demands, suffered or incurred by, awarded against, or agreed to be paid by, Customer arising directly or in connection with:

a) any non-compliance by Service Provider (or any Subprocessor appointed by Service Provider under Clause 11) with Data Protection Legislation;

b) any Personal Data Processing carried out by Service Provider (or any Subprocessor appointed by Service Provider under Clause 11) which is not in accordance with instructions given by Customer to the extent that the instructions are in compliance with Data Protection Legislation; or

c) any breach by Service Provider of its obligations or warranties under this Agreement;

but not to the extent that the same is or are contributed to by any non-compliance by Customer with Data Protection Legislation or its breach of this Agreement.

16.3 Customer shall not be entitled to claim back from Service Provider under sub-Clause 16.2 or on any other basis any sums paid in compensation by Customer in respect of any damage to the extent that Customer is liable to indemnify Service Provider under sub-Clause 16.1.

16.4 Nothing in this Agreement (and in particular, this Clause 16) shall relieve either Party of, or otherwise affect, the liability of either Party to any Data Subject, or for any other breach of that Party's direct obligations under Data Protection Legislation. Furthermore, Service Provider hereby acknowledges that it shall remain subject to the authority of the Information Commissioner and shall co-operate fully therewith, as required, and that failure to comply with its obligations as a Data Processor under Data Protection Legislation may render it subject to the fines, penalties, and compensation requirements set out in Data Protection Legislation.

16.5 Nothing in this Clause 16 shall be deemed to be limited, excluded, or prejudiced by any other provision(s) of this Agreement.

17. Term and Termination

17.1 This Agreement shall come into force on the commencement date of the Service Agreement and shall continue in force for the longer of:

a) the period that the Service Agreement remains in effect; or

b) the period that Service Provider has any Personal Data in its possession or control.

17.2 Any provision of this Agreement which, expressly or by implication, is to come into force or remain in force on or after the termination or expiry of the Service Agreement shall remain in full force and effect.

17.3 In the event that changes to Data Protection Legislation necessitate the re-negotiation of any part this Agreement, either Party may require such re-negotiation.

18. Notices

18.1 All notices under or in connection with this Agreement shall be in writing.

18.2 All notices given to Customer under or in connection with this Agreement must be addressed to Customer's registered address or sent to the email address or facsimile number advised from time to time by Customer to the Service Provider and marked for the attention of the data protection officer.

18.3 All notices given to Service Provider under or in connection with this Agreement must be addressed to Service Provider's registered address or sent to the email address or facsimile number advised from time to time by Service Provider to the Customer and marked for the attention of the data protection officer.

18.4 Notices shall be deemed to have been duly given:

a) when delivered, if delivered by courier or other messenger (including registered mail) during normal business hours of the recipient; or

b) when sent, if transmitted by facsimile or e-mail and a successful transmission report or return receipt is generated; or

c) on the fifth business day following mailing, if mailed by national ordinary mail, postage prepaid.

In each case notices shall be addressed as indicated above.

19. Law and Jurisdiction

19.1 This Agreement (including any non-contractual matters and obligations arising therefrom or associated therewith) shall be governed by, and construed in accordance with, the laws of England and Wales.

19.2 Any dispute, controversy, proceedings or claim between the Parties relating to this Agreement (including any non-contractual matters and obligations arising therefrom or associated therewith) shall fall within the jurisdiction of the courts of England and Wales.

Schedule 1 – Personal Data

Data Subjects

Data Subjects may include Customer's representatives and end users including employees, contractors, collaborators and customers of the Customer. Data Subjects may also include individuals attempting to communicate or transfer personal information to users of Services provided by Service Provider. Service Provider acknowledges that, depending on Customer's use of Services, Customer may elect to include Personal Data from any of the following types of Data Subjects in Personal Data:

- Employees, contractors and temporary workers (current, former, prospective) of Customer;
- Customer's collaborators/contact persons (natural persons) or employees, contractors or temporary workers of legal entity collaborators/contact persons (current, former, prospective);
- End users of Services provided by Service Provider (e.g., customers, suppliers, etc.) and other Data Subjects that are users of Customer's services;
- Partners, stakeholders or individuals who actively collaborate, communicate or otherwise interact with Customer and/or use communication tools such as apps and websites provided by Customer that interact or integrate with Services provided by Service Provider;
- Stakeholders or individuals who passively interact with Customer (e.g., because they are the subject of correspondence, research or mentioned in documents or correspondence from or to Customer); or
- Professionals with professional privilege (e.g., lawyers, notaries, etc.).

Categories of Personal Data

Personal Data that is included in system transactions, documents and other data in an electronic form in the context of Services provided by Service Provider to Customer. Service Provider acknowledges that, depending on Customer's use of Services, Customer may elect to include Personal Data from any of the following categories:

- Basic personal data (for example first name, last name, initials, place of birth, home address, work address, mobile phone number, email address, gender, date of birth), including basic personal data about family members and dependents;
- Authentication data (for example username, password or PIN code, security questions, audit trail);
- Contact information (for example addresses, email, phone numbers, social media identifiers; emergency contact details);
- Unique identification numbers and signatures (for example Social Security number, NI number, bank account number, passport and ID card number, driving license number and vehicle registration data, IP addresses, employee number, signature, unique identifier in tracking cookies or similar technology);
- Pseudonymous identifiers;
- Financial and insurance information (for example insurance number, bank account name and number, invoice number, credit check information);
- Location data (for example, IP address, Cell ID, geo-location network data, location data derived from the use of features included in Services);
- Photos, video and audio;
- Device identification (for example IMEI number, SIM card number, MAC address);
- Profiling (for example based on observed behaviour or pseudonymous profiles based on visited URLs, click streams, browsing logs, IP-addresses, domains, apps installed, or profiles based on marketing preferences);
- HR and recruitment data (for example declaration of employment status, recruitment information (such as curriculum vitae, employment history, education history details), job and position data, including worked hours, assessments and salary, work permit details, availability, terms of employment, tax details, payment details, insurance details and location and organisations);

- Education data (for example education history, current education, grades and results, learning achievements, skills, learning disabilities);
- Citizenship and residency information (for example citizenship, naturalisation status, marital status, nationality, immigration status, passport data, details of residency or work permit);
- Information processed for the performance of a task carried out in the public interest or in the exercise of an official authority; or
- Any other Personal Data as identified in Data Protection Legislation where such Personal Data is necessary for Service Provider to provide Services to Customer.

Special categories of data may be included only where relevant for the provision of Services by Service Provided to Customer (for example 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, data concerning health, data concerning a natural person's sex life or sexual orientation, or data relating to criminal convictions or offences).

Nature of Processing

Such Processing as is necessary to enable Service Provider to provide Services to Customer and meet its obligations or exercise its rights under the Service Agreement. This includes but is not limited to storage, retrieval, analysis, collection and transfer.

Purposes of Processing

Such Processing as is necessary to enable Service Provider to provide Services to Customer and meet its obligations or exercise its rights under the Service Agreement.

Duration of Processing

Service Provider shall Process Personal Data for the duration necessary to:

- Enable it to provide Services to Customer and meet its obligations or exercise its rights under the Service Agreement.
- Comply with applicable law.

Schedule 2 – Technical and Organisational Data Protection Measures

The following are the technical and organisational data protection measures referred to in Clause 7:

1. Service Provider shall ensure that, in respect of all Personal Data it receives from or Processes on behalf of Customer, it maintains security measures to a standard appropriate to:

   1.1 the harm that might result from unlawful or unauthorised Processing or accidental loss, damage, or destruction of Personal Data; and

   1.2 the nature of Personal Data to be Processed.

2. In particular, Service Provider shall:

   2.1 have in place, and comply with, a security policy which:

      a) defines security needs based on a risk assessment;

      b) allocates responsibility for implementing the policy to a specific individual (such as Service Provider's data protection officer) or personnel;

      c) is provided to or otherwise made available to Customer on or before the commencement of this Agreement;

      d) is disseminated to all relevant staff; and

      e) provides a mechanism for feedback and review;

   2.2 ensure that appropriate security safeguards and virus protection are in place to protect the hardware and software which is used in Processing Personal Data in accordance with generally recognised good industry practice;

   2.3 ensure that all hardware and software used in Processing of Personal Data is properly maintained, including but not limited to, the installation of all applicable software updates;

   2.4 prevent unauthorised access to Personal Data;

   2.5 protect Personal Data using appropriate encryption;

   2.6 protect Personal Data using pseudonymisation, where it is practical to do so;

   2.7 ensure that its storage of Personal Data conforms with best industry practice such that the media on which Personal Data is recorded (including paper records and records stored electronically) are stored in secure locations and access by personnel to Personal Data is strictly monitored and controlled;

   2.8 have secure methods in place for the transfer of Personal Data whether in physical form (for example, by using couriers rather than post) or electronic form (for example, by using password-protected or encrypted portable storage);

   2.9 have password protection on all computers and other devices on which Personal Data is stored, ensuring that all passwords are secure and in accordance with Service Provider's password policy, and that passwords are not shared under any circumstances;

   2.10 take reasonable steps to ensure the reliability of personnel who have access to Personal Data;

   2.11 ensure that all employees who are to access and/or Process any Personal Data are given suitable training on Data Protection Legislation, Service Provider's obligations under it, their obligations under it, and its application to their work, with particular regard to Processing of Personal Data under this Agreement;

   2.12 have in place methods for detecting and dealing with breaches of security (including loss, damage, or destruction of Personal Data) including:

      2.12.1 the ability to identify which individuals have worked with specific Personal Data;

      2.12.2 having a proper procedure in place for investigating and remedying breaches of Data Protection Legislation; and

      2.12.3 notifying Customer as soon as any such security breach occurs.

2.13 have a secure procedure for backing up all electronic Personal Data and storing back-ups separately from originals;

2.14 have a secure method of disposal of unwanted Personal Data including for back-ups, disks, print-outs, and redundant equipment; and

2.15 adopt such organisational, operational, and technological processes and procedures as are required to comply with the requirements of ISO/IEC 27001:2013, as appropriate to the nature of Services provided to Customer.

Schedule 3 – List of Subprocessors

Service Provider has appointed the following Subprocessors:

- Enterprise Analytics (PVT) Limited
- Platned Limited
- Xtensys Limited