Neurequity Data Processing Agreement

Version 1.4 – January 2024

1. Definitions and Interpretation

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

Data Controller: the meaning given to the term "data controller" in section 6 of the Data Protection Act 2018.

Data Processor: the meaning given to the term "processor" in Article 4 of the UK GDPR.

Data Protection Legislation: 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 Commissioner under the UK GDPR or a Supervisory Authority under the EU GDPR which are applicable to a Party.

Data Subject: the meaning given to the term "data subject" in Article 4 of the UK GDPR.

EEA: the European Economic Area, consisting of all EU Member States plus Iceland, Liechtenstein, and Norway.

EU GDPR: the General Data Protection Regulation ((EU) 2016/679), as it has effect in European Union law.

Information Commissioner: the Information Commissioner, as defined in Article 4(A3) of the UK GDPR and section 114 of the Data Protection Act 2018.

Personal Data Breach: the meaning given to the term "personal data breach" in Article 4 of the UK GDPR.

Personal Data: all such "personal data", as defined in Article 4 of the UK GDPR, as is, or is to be, Processed by the Data Processor on behalf of the Data Controller described in Schedule 2.

Processing, Process, Processes, Processed: the meaning given to the term "processing" in Article 4 of the UK GDPR.

Sensitive Data: (i) social security number, national identify number, passport number, driving license number, national insurance number, or similar information; (ii) credit or debit card number, financial information, bank account numbers, or similar information; (iii) employment, genetic or biometric or health data; (iv) information relating to race, ethnicity, political or religious affiliation, trade union membership, criminal convictions, or relating to sexual life or sexual orientation; and (v) any other information or combinations of information that falls within the definition of "Special Category Data" under Data Protection Legislation.

Services Agreement: the Neurequity Cloud Portal Agreement entered into by the Parties.

Services: those services described in Schedule 1 which are provided by the Data Processor to the Data Controller and which the Data Controller uses for the purposes described in Schedule 1.

Standard Contractual Clauses: standard contractual clauses for Data Controller to Data Processor transfers or Data Processor to Subprocessor transfers that are:

(a) approved for use pursuant to UK GDPR or otherwise approved for use by the Information Commissioner, including but not limited to the International Data Transfer Agreement and International Data Transfer Addendum; or

(b) approved for use pursuant to EU GDPR, including but not limited to the EU Standard Contractual Clauses.

Subprocessor: any individual or entity (including any third party but personnel of the Data Processor) appointed by or on behalf of the Data Processor to Process Personal Data in connection with this DPA.

Supervisory Authority: the meaning given to it under Article 4(21) of the EU GDPR

Term: the term of this DPA, as set out in Clause 17.

UK GDPR: 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 DPA to:

(a) “Customer” means the Party identified as such in the Service Agreement;

(b) “Supplier” means the Party identified as such in the Service Agreement;

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

(d) a statute or a provision of a statute is a reference to that statute or provision and shall include all subordinate legislation made under that statute or statutory provision as at the date of this DPA;

(e) “this DPA” is a reference to this data processing agreement and each of the Schedules as amended or supplemented at the relevant time;

(f) a Schedule is a schedule to this DPA;

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

(h) a "Party" or the "Parties" refers to the parties to the Service Agreement.

1.3 Clause, Schedule and paragraph headings shall not affect the interpretation of this DPA.

1.4 A person includes an individual, corporate or unincorporated body (whether or not having separate legal personality) and that person's legal and personal representatives, successors or permitted assigns.

1.5 A reference to a company shall include any company, corporation or other body corporate, wherever and however incorporated or established.

1.6 Unless the context otherwise requires, words in the singular shall include the plural and in the plural shall include the singular.

1.7 Unless the context otherwise requires, a reference to one gender shall include a reference to the other genders.

2. Scope and Applications of this DPA

2.1 The Parties acknowledge and agree that with regard to the Processing of Personal Data under the Service Agreement, the Customer and the Supplier are each an independent Data Controller, and the Supplier is a Data Processor.

2.2 The provisions of this DPA shall apply to the Processing of the Personal Data described in Schedule 2, carried out for the Customer by the Supplier, and to all Personal Data held by the Supplier in relation to all such Processing whether such Personal Data is held at the commencement date of the Service Agreement or received afterwards.

2.3 The provisions of this DPA 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 DPA.

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

3. Provision of the Services and Processing Personal Data

3.1 Schedule 2 describes the type of Personal Data, the category or categories of Data Subject, the nature of the Processing to be carried out, the purpose of the Processing, and the duration of the Processing.

3.2 Subject to sub-Clause 4.1, the Supplier is only to carry out the Services, and only to Process the Personal Data received from the 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 the Customer (which may be specific instructions or instructions of a general nature or as otherwise notified by the Customer to the Supplier).

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

4. The Supplier's Obligations

4.1 As set out above in Clause 3, the Supplier shall only Process the Personal Data to the extent and in such a manner as is necessary for the purposes of the Services and not for any other purpose. All instructions given by the Customer to the Supplier shall be made in writing and shall at all times be in compliance with the Data

Protection Legislation. The Supplier shall act only on such written instructions from the Customer unless the Supplier is required by domestic law to do otherwise (as per Article 29 of the UK GDPR) (in which case, the Supplier shall inform the Customer of the legal requirement in question before Processing the Personal Data for that purpose unless prohibited from doing so by law).

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

4.3 The Supplier shall promptly comply with any written request from the Customer requiring the Supplier to amend, transfer, delete (or otherwise dispose of), or to otherwise Process the Personal Data.

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

4.5 The Supplier shall provide all reasonable assistance (at its own cost) to the Customer in complying with its obligations under the 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 the Processing carried out by the Supplier and the information available to the Supplier.

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

5. Confidentiality

5.1 The Supplier shall maintain the Personal Data in confidence, and in particular, unless the Customer has given written consent for the Supplier to do so, the Supplier shall not disclose the Personal Data to any third party. The Supplier shall

not Process or make any use of any Personal Data supplied to it by the Customer otherwise than as necessary and for the purposes of the provision of the Services to the Customer.

5.2 Nothing in this DPA shall prevent the Supplier 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, the Supplier shall notify the Customer of the disclosure or Processing requirements prior to disclosure or Processing (unless such notification is prohibited by domestic law) in order that the Customer may challenge the requirement if it wishes to do so.

5.3 The Supplier shall ensure that all of its employees and sub-contractors who are to access and/or Process any of the Personal Data are informed of its confidential nature and are contractually obliged to keep the Personal Data confidential.

6. The Supplier's Employees, Sub-contractors and Data Protection Officers

6.1 The Customer shall have appointed a data protection officer in accordance with Article 37 of the UK GDPR, whose details shall be provided to the Supplier at or as soon as possible after the commencement date of the Service Agreement.

6.2 The Supplier shall have appointed a data protection officer in accordance with Article 37 of the UK GDPR, whose contact details are as follows: dpo@neurequity.com.

6.3 The Supplier shall ensure that all of its employees and sub-contractors who are to access and/or Process any of the Personal Data are given suitable training on the Data Protection Legislation, the Data Processor's obligations under it, their obligations under it, and its application to their work, with particular regard to the Processing of the Personal Data under this DPA.

7. Security of Processing

7.1 The Supplier shall implement appropriate technical and organisational measures as described in Schedule 3 and take all steps necessary to protect the Personal Data against unauthorised or unlawful Processing or accidental or unlawful loss, destruction, or damage. The Customer acknowledges that the Supplier may update such measures from time to time upon reasonable notice to the Customer to reflect improvements or changing practices (provided that the updates do not materially decrease the Supplier's obligations as compared to those effective at the commencement date of the Service Agreement).

7.2 The measures implemented by the Supplier shall be appropriate to the nature of the Personal Data, 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 the Supplier may include, as appropriate, pseudonymisation and encryption of the 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 the 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 The Supplier shall, if so requested by the Customer (and within the reasonable timescales required by the Customer) supply further details of the technical and organisational systems in place to safeguard the security of the Personal Data held and to prevent unauthorised access.

8. Data Subject Rights and Complaints

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

(a) the rights of Data Subjects under the 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 the Customer by the Information Commissioner pursuant to the Data Protection Legislation.

8.2 In the event that the Supplier receives any notice, complaint, or other communication relating to the Personal Data Processing or to either Party's compliance with the Data Protection Legislation, it shall notify the Customer immediately in writing.

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

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

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

(d) providing the Customer with any other necessary information requested by the Customer.

8.5 The Supplier shall act only on the instructions of the Customer and shall not disclose any Personal Data to any Data Subject or to any other party except as instructed in writing by the Customer, or as required by domestic law.

9. Personal Data Breaches

9.1 The Supplier shall immediately (and without undue delay) notify the Customer in writing if it 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, the Personal Data.

9.2 If the Supplier becomes aware of a Personal Data Breach, it shall provide the following information to the 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 undertake an investigation into it. The Supplier shall provide all reasonable assistance (at the Supplier's cost) to the Customer including, but not limited to:

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

(b) providing and facilitating the 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 the Customer or as otherwise required by the 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 The Supplier 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 The Supplier shall not inform any third party of any Personal Data Breach as described above without the express written consent of the Customer unless it is required to do so by domestic law.

9.6 The 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 applicable law, or at the discretion of the Customer, including the form of such notification.

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

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

10.1 The Supplier may transfer or authorise the transfer of Personal Data to a Subprocessor in a country outside the UK, Switzerland, and the EEA.

10.2 Where there is a transfer of Personal Data to a Subprocessor 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 Section17A of the Data Protection Act 2018 or Paragraphs 4 and 5 of Schedule 21 of the Data Protection Act 2018, the Supplier shall enter into Standard Contractual Clauses with the Subprocessor for the transfer of the Personal Data. The Standard Contractual Clauses shall apply to the Personal Data originating from the Supplier (who for the purposes of the Standard Contractual Clauses shall be deemed to be the "data exporter") that is Processed by the Subprocessor (who for the purposes of the Standard Contractual Clauses shall be deemed to be the "data importer").

10.3 If there is any conflict between the Standard Contractual Clauses and this DPA, the Standard Contractual Clauses shall prevail.

11. Subprocessors

11.1 The Supplier shall not appoint any new Subprocessor without the prior written consent of the Customer. The Customer gives general consent for the Supplier to appoint the Subprocessors listed in Schedule 4, as may be amended from time to time by the Supplier in accordance with this DPA.

11.2 In the event that the Supplier intends to appoint a Subprocessor to Process any of the Personal Data, the Supplier shall:

(a) promptly notify the Customer of its intention to appoint a Subprocessor or notify the 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 the Service;

(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 the Supplier by this DPA, particularly with regard to technical and organisational security measures required to comply with the Data Protection Legislation, which shall permit both the Supplier and the Customer to enforce those obligations, and which shall terminate automatically on the termination of this DPA for any reason;

(c) at the written request of the 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 the Data Protection Legislation; and

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

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

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

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

(c) if the Supplier cannot address the Customer's objection pursuant to the foregoing efforts, the Supplier shall notify the Customer within fifteen (15) days of receipt of the objection notice issued by the Customer, and the Customer may then, by written notice to the Supplier within thirty (30) days of the Supplier's notice, terminate the Service Agreement however, the Customer shall not be entitled to any refund of prepaid fees covering the terminated portion of the Service Agreement.

11.4 In the event that a Subprocessor fails to meet its data protection obligations, the Supplier shall remain fully liable to the Customer for the Subprocessor's compliance with its data protection obligations.

11.5 The Supplier 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 The Supplier shall, at the written request of the Customer (and at the Customer's choice) securely delete (or otherwise dispose of) the Personal Data or return it to the Customer in accordance with the Service Agreement after the earlier of the following:

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

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

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

12.3 If the Supplier is required to retain copies of all or any part of the Personal Data by law, regulation, government, or other regulatory body, it shall inform the Customer of such requirement(s) in writing, including precise details of the 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 the Personal Data, the Supplier shall certify the completion of the same in writing to the Customer within 30 days of the deletion (or disposal).

13. Information

13.1 The Supplier shall make available to the Customer any and all such information as is reasonably required and necessary to demonstrate the Supplier's compliance with the Data Protection Legislation and this DPA.

14. Audits

14.1 The Supplier shall, on reasonable prior notice, allow the Customer or a third-party auditor appointed by the Customer to audit the Supplier's compliance with its obligations under this DPA and with the Data Protection Legislation.

14.2 The Supplier shall provide all necessary assistance (at the 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 the Supplier;

(b) access to all of its employees and sub-contractors who are to access and/or Process any of the Personal Data including, where reasonably necessary, arranging interviews between the Customer and such employees and sub-contractors; and

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

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

14.4 The Supplier must inform the Customer promptly if, in its opinion, any instructions given by the Customer, or any third-party auditor appointed by the Customer, do not comply with the Data Protection Legislation.

14.5 Any audit performed by the Customer, or a third-party auditor appointed by the Customer, shall not cause any damage, injury, or disruption to the Supplier's premises, equipment, or business operations.

15. Warranties

15.1 The Customer hereby warrants and represents that:

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

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

(c) it shall not submit to the Supplier any Sensitive Data and that, notwithstanding any other provision to the contrary, the Supplier shall have no liability under the Service Agreement or this DPA for any Sensitive Data submitted in violation of the foregoing.

15.2 The Supplier hereby warrants and represents that:

(a) the Personal Data shall be Processed by the Supplier (and by any Subprocessors appointed under Clause 11) in compliance with the 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 the Data Protection Legislation in any way prevents it from complying with its obligations under the Service Agreement; and

(c) it will implement 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 3.

16. Liability and Indemnity

16.1 The Customer shall be liable for, and shall indemnify (and keep indemnified) the Supplier 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, the Supplier and any Subprocessor appointed by the Supplier under Clause 11 arising directly or in connection with:

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

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

(c) any breach by the Customer of its obligations or warranties under this DPA;

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

16.2 The Supplier shall be liable for, and shall indemnify (and keep indemnified) the 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, the Customer arising directly or in connection with:

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

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

(c) any breach by the Supplier of its obligations or warranties under this DPA;

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

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

16.4 Nothing in this DPA (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 the Data Protection Legislation. Furthermore, the Supplier 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 the Data Protection Legislation may render it subject to the fines, penalties, and compensation requirements set out in the 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 DPA.

17. Term and Termination

17.1 This DPA 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 the Supplier has any of the Personal Data in its possession or control.

17.2 Any provision of this DPA 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 the Data Protection Legislation necessitate the re-negotiation of any part this DPA, either Party may require such re-negotiation.

Schedule 1 – Services

The following services shall be provided by the Supplier under the Service Agreement:

- Providing access for nominated staff of the Customer to the features of the Neurequity cloud portal in accordance with the Service Agreement

- Providing access for nominated staff of the Customer to the content made available through the Neurequity cloud portal in accordance with the Service Agreement

- Providing the Customer with support services relating to the Neurequity cloud portal in accordance with the Service Agreement

Schedule 2 – Personal Data

Type of Personal Data	Category of Data Subject	Nature of Processing Carried Out	Purpose(s) of Processing	Duration of Processing
First Name Last Name Email Address Timezone	Staff of the Customer including employees, temporary staff, sub-contractors and casual stall	Creating, storing, updating and deleting end user account details for the Neurequity cloud portal Maintaining records of login activity to the Neurequity cloud portal Maintaining records of access to content held in the Neurequity cloud portal Maintaining records of registration for events published on the Neurequity cloud portal	To allow the Customer's staff to access and use the features and content of the Neurequity cloud portal To administer the end user account details for the Neurequity cloud portal To enable the Customer's staff to attend Neurequity events and webinars	For the duration of the Service Agreement or as otherwise required under the Service Agreement or this DPA

Schedule 3 – Technical and Organisational Data Protection Measures

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

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

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

    b. the nature of the Personal Data.

2. In particular, the Supplier shall:

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

        i. defines security needs based on a risk assessment;

        ii. allocates responsibility for implementing the policy to a specific individual (such as the Supplier's data protection officer) or personnel;

        iii. is made available to the Customer on or before the commencement of this DPA;

        iv. is disseminated to all relevant staff; and

        v. provides a mechanism for feedback and review.

    b. ensure that appropriate security safeguards and virus protection are in place to protect the hardware and software which is used in Processing the Personal Data in accordance with best industry practice;

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

    d. prevent unauthorised access to the Personal Data;

    e. protect the Personal Data using appropriate encryption;

f. protect the Personal Data using pseudonymisation, where it is practical to do so;

g. 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;

h. 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);

i. 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 the Supplier's password policy, and that passwords are not shared under any circumstances;

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

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

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

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

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

    iii. notifying the Customer as soon as any such security breach occurs.

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

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

Schedule 4 – List of Subprocessors

The Supplier has appointed the following Subprocessors:

- SwiftXF Limited, Swift Cross Farm, Ripponden, Sowerby Bridge, West Yorkshire, HX6 4LQ

    - Support and maintenance of the underlying software application platform used to deliver the Neurequity cloud service.

    - Assistance with general management and housekeeping of the underlying Microsoft Azure cloud virtual servers (including operating systems and databases) used by the Neurequity cloud service.

- Microsoft Ireland Operations Ltd, One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, D18 P521, Ireland

    - Provision and management of the Microsoft Azure data centre facilities, cloud infrastructure, storage, networks, and associated services used by the Neurequity cloud service.