Data Processing Addendum

Version 3.0

19 January 2022

The undersigned:

(1) _____ with address _____, the Netherlands (the **Controller**); and

(2) Neurolytics B.V., with address Europalaan 400- 4e, 3526KS Utrecht, the Netherlands (the **Processor**),

hereinafter collectively also referred to as the **Parties** and each a **Party**,

Whereas:

(A) Controller and Processor have concluded an agreement (the **Agreement**) on the grounds of which Neurolytics B.V. provides its standard software as a service through the Website and the Webapp for the purpose of providing objective behavioural analysis.

(B) Within the framework of this Agreement, Processor shall process personal data on behalf of and based on written instructions of Controller.

(C) Controller is designated as controller in the sense of article 4(7) of the General Data Protection Regulation (EU) 2016/679 (the **GDPR**).

(D) Processor is designated as processor in the sense of article 4(8) of the GDPR.

(E) the Parties, also taking account of the provisions of article 28(3) of the GDPR, wish to lay down in writing in this data processing agreement a number of conditions to set out the processing of personal data by Processor.

It is hereby agreed as follows:

1 Objectives of the processing

1.1 Purpose

At the request and on behalf of Controller, Processor shall process the (categories of) personal data mentioned in Appendix 1 under the conditions laid down in this data processing agreement. Processing shall take place exclusively within the framework of the Agreement and the purpose(s) mentioned in Appendix 1, as laid down by Controller, by virtue of which Controller can make personal data available to Processor for the processing actions listed in Appendix 1.

1.2 Sub-processor

Processor may engage third parties (sub-processors) for executing this data processing agreement and the Agreement for which Controller is now granting general written consent. The same, or stricter, obligations will be imposed upon said sub-processor regarding data security and processing as mentioned in this data processing agreement. As soon as a change concerning the addition of replacement of these processors is intended, Processor shall inform Controller of these intended changes immediately in writing, after which Controller may express his objections to said changes. In the case of legitimate objections which cannot be resolved, Controller may terminate this data processing agreement and the Agreement in writing.

1.3 Inform

Processor shall inform Controller immediately if Processor is of the opinion that an instruction causes an infringement of the GDPR or of another legal requirement regarding data protection.

2 Data transfer and confidentiality

2.1 Data transfer

Processor shall not transfer the personal data to a third country or international organization without the written instructions or consent from Controller for said transfer, unless Processor is obliged thereto pursuant to a provision of applicable data protection regulation. In that case, prior to said transfer, Processor shall inform Controller of the legal requirement, unless said legislation prohibits such information on important grounds of public interest.

2.2 Confidentiality

Processor shall keep confidential the personal data that comes to its knowledge, unless it is obliged to make notification pursuant to a legal requirement, in which case Processor shall inform Controller of the same prior to said notification. Processor also imposes said confidentiality on any of its employees having access to the personal data.

3 Security and data breach(es)

3.1 Appropriate measures

In accordance with the rules and regulations applicable at that time, Processor shall implement the appropriate technical and organizational measures to secure the personal data against loss or against any form of unlawful processing, taking account of the state of the art and the costs of implementation, considering the risks involved with the processing of and the nature of the data that is to be protected. The security measures that have been taken by Processor are specified in Appendix 1.

3.2 Data breach

In the event of any unauthorized or accidental access to or use, disclosure, alteration, loss or destruction of any personal data, or Processor having reasonable belief that any such access, use, disclosure, alteration, loss or destruction has occurred or is at risk of occurring (which shall include, without limitation, the loss of or the inability to locate definitively any media, device or equipment on which personal data is or may be stored), Processor shall make every effort to in-form the Controller of the same immediately and will promptly take all necessary and appropriate corrective action to remedy the underlying causes of the data breach.

4 Inspection and privacy impact assessment

4.1 Inspection

Controller is entitled, at his own costs, to have the measures and the compliance with the obligations of Processor audited by an independent third party. At the request of Controller, Processor shall make available to Controller all information necessary to demonstrate compliance with the obligations laid down in Article 28 GDPR.

4.2 Privacy impact assessment

At the request of Controller, Processor shall assist Controller with fulfilling his obligations within the framework of a privacy impact assessment and, where appropriate, with the prior consultation of the supervisory authority.

5 Requests of the data subject and/or supervisory authorities

5.1 Data subject

If a data subject requests Processor access to, rectification or erasure of personal data, restriction of processing concerning the data subject, data portability or if the data subject objects to processing, Processor shall forward the request to Controller. Controller shall handle the request in question themselves.

5.2 Appropriate measures

Processor shall, insofar as is possible, taking account of the nature of the processing, assist Controller by means of appropriate and organizational measures with handling requests from data subjects and/or requests from the supervisory authority.

6 Duration of the data processing agreement

6.1 Duration

This data processing agreement commences on the date of signing and its term is at least equal to the term as agreed by the Parties in the Agreement. As soon as the Agreement ends, this data processing ends simultaneously.

6.2 Termination

The instruction to process the personal data ends on termination of the Agreement, or as soon as Controller has notified Processor in writing that the processing assignment ends. After the end of the provision of services relating to processing, Processor shall, at the discretion of Controller, delete all personal data or return all personal data to Controller and delete all existing copies, unless the storage of the personal data is required by law.

7 Law and jurisdiction

7.1 Governing law

This agreement shall be governed by and construed in accordance with the laws of the Netherlands.

7.2 Jurisdiction

All disputes arising out or in connection with this agreement shall exclusively be settled by the competent court in Utrecht, the Netherlands.

In evidence whereof this agreement was signed by:

	Neurolytics B.V.
Data controller	*Data Processor*
Name	*Name*
Position	*Position*
Date	*Date*
Signature	*Signature*

APPENDIX 1: CATEGORIES, PURPOSES, PROCESSING ACTIONS AND PROTECTION MEASURES

I. Processor processes at the instructions of Controller:

Data Subjects	Purposes of processing	Type of data processed	Processing activities
Candidates & employees	Personal data processed for providing reports & analytics	- Name - Email - Video recordings during the scan - Audio recordings during the scan - Written communication - Job title (if provided by client for analytics) - Location data as identified through IP address - Results from analysis as in report - Login information - Text based submissions - Date & time of usage - Performance (if provided by client for analytics)	- Collecting, recording, storing personal data to provide access to the (candidate) Scan and to provide the results to the Client - Recording of personal data during the Scan to collect data needed for analysis - Use of collected data for analysis - Consultation and analysis of personal data to provide analytical insights - Erasure or destruction of personal data on request of the Controller or on Termination of the agreement
Users on Platform (employees, contractors, other representatives assigned by Controller)	Personal data processed to provide the Service via the Platform	- Name - Email - Phone number (if provided) - Job title - Video recordings with audio (in case this is provided for the Speaking module) - Location data as identified through IP address - Written communication - Login information - Date & time of usage	- Collecting, recording, storing personal data to provide access to the Platform - Recording and using personal data to provide Support and Services - Erasure or destruction of personal data on request of the Controller or on Termination of the agreement

II. Processor has taken the following measures for the protection of the personal data that is to be processed on behalf of Controller:

- Neurolytics has processes in place for quality assurance of the Services. Such processes include automated testing and pre-deployment manual testing of features and bug fixes.
- All new code for the Services and/or Features is reviewed by at least one senior developer before it's released to a production environment. The review includes a check for the use of secure coding practices.
- Encryption is used for all transfer of Personal Data by the Service over the internet.
- All passwords for the Services are stored using an industry standard hashing algorithm.
- A specialized Third-Party penetration tester will regularly test the security of the Services provided under the Terms.
- All Personal Data in the Service is backed up daily or continuously in increments.
- Employees of Neurolytics receive access rights to Personal Data in the Service only on a need-to-know basis. Access rights are revoked subsequently.
- The Service shall only be hosted in Third-Party data centers that have a high level of security and availability, such as ISO 27001 certified data centers.
- Neurolytics will have reasonable measures in place for the Service to protect its servers from DDOS attacks.
- The infrastructure for the provision of the Service shall be protected by one or more firewalls.

APPENDIX 2: LIST OF SUB-PROCESSORS

The Data Controller agrees that the Data Processor engages the parties listed below as Sub Processors:

Sl. No.	Name of the Sub Processor	Purpose of Sub Processing	Location of Sub Processing
1.	Amazon Web Services	Cloud Storage and Cloud Computing	Ireland
2.	Hotjar	Record screen activity to be able to provide technical support	EU