IMOTIONS®

DATA PROCESSING AGREEMENT

This Data Protection Agreement ("**Agreement**"), dated ____________________ ("**Agreement Effective Date**") forms part of the Software Licence Agreement (SLA), Master Services Agreement (MSA), or Sales Contract ("**Principal Agreement**") between: ____ (hereinafter referred as the "**Controller**") acting on its own behalf; and iMotions A/S (hereinafter referred as the **"Processor**") acting on its own behalf.

The terms used in this Agreement shall have the meanings set forth in this Agreement. Terms not otherwise defined herein shall have the meaning given to them in the Principal Agreement. Except as modified below, the terms of the Principal Agreement shall remain in full force and effect.

The parties hereby agree that the terms and conditions set out below shall be added as an addendum to the Principal Agreement.

1. Definitions

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

"Sub-processor" means any sub-data Processor (including any third party) appointed by the Processor to Process Controller Personal Data on behalf of the Controller, amounting to (a) those Sub-processors set out in Annex 3 (Authorised Transfers of Controller Personal Data); and (b) any additional Sub-processors consented to in writing by Controller in accordance with Sub-processing section.

"Process/Processing/Processed", "Data Controller", "Data Processor", "Data Subject", "Personal Data", "Special Categories of Personal Data" and any further definition not included under this Agreement or the Principal Agreement shall have the same meaning as in EU General Data Protection Regulation 2016/679 of the European Parliament and of the Council ("GDPR").

"Data Protection Laws" means GDPR as well as any local data protection laws, hereunder the Danish Data Protection Act***.***

"Erasure" means the removal or destruction of Personal Data such that it cannot be recovered or reconstructed***.***

"EEA" means the European Economic Area.

"Third Country" means any country outside EU/EEA, except where that country is the subject of a valid adequacy decision by the European Commission on the protection of Personal Data in Third Countries.

"Controller Personal Data" means the data described in Annex 1 and any other Personal Data Processed by Processor on behalf of the Controller pursuant to or in connection with the Principal Agreement**.**

"Personal Data Breach" means a breach of leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Controller Personal Data transmitted, stored or otherwise Processed***.***

"Services" means the services to be supplied by the Processor to the Controller pursuant to the Principal Agreement***.***

"Products" means the products to be supplied by the Processor to the Controller pursuant to the Principal Agreement***.***

"Standard Contractual Clauses" means the standard contractual clauses for the transfer of Personal Data to Sub-processors established in Third Countries, as approved by the European Commission Decision 2021/915/EU, or any set of clauses approved by the European Commission which amends, replaces or supersedes these.

2. The rights and obligations of the Controller

2.1. Controllers within the EU

2.1.1. The Controller is responsible for ensuring that the processing of personal data takes place in compliance with the GDPR (see Article 24 GDPR), the applicable EU or Member State data protection provisions and the Clauses.

2.1.2. The Controller has the right and obligation to make decisions about the purposes and means of the processing of personal data.

2.1.3. The Controller shall be responsible, among other, for ensuring that the processing of personal data, which the data processor is instructed to perform, has a legal basis. This means that the Controller must ensure that consent is collected from the participants and that participants are properly informed about the processing of personal data.

2.2. Controllers outside the EU

2.2.1. The Controller is responsible for ensuring that the processing of personal data takes place in compliance the applicable privacy legislation

2.2.2. The Controller has the right and obligation to make decisions about the purposes and means of the processing of personal data.

3. Data Processing Terms

3.1. In the course of providing the Services and/or Products to the Controller pursuant to the Principal Agreement, the Processor may Process Controller Personal Data on behalf of the Controller as per the terms of this Agreement. The Processor agrees to comply with the following provisions with respect to any Controller Personal Data.

3.2. To the extent required by applicable Data Protection Laws, the Processor shall obtain and maintain all necessary licenses, authorizations and permits necessary to Process Personal Data, including Personal Data mentioned in Annex 1.

3.3. The Processor shall maintain all the technical and organizational measures to comply with the requirements set forth in the Agreement and its Annexes.

4. Processing of Controller Personal Data

4.1. The Processor shall only Process Controller Personal Data for the purposes of the Principal Agreement. The Processor shall not Process, transfer, modify, amend or alter the Controller Personal Data or disclose or permit the disclosure of the Controller Personal Data to any third party other than in accordance with Controller's documented instructions unless Processing is required by EU or Member State law to which Processor is subject. The Processor shall, to the extent permitted by such law, inform the Controller of that legal requirement before Processing the Personal Data and comply with the Controller's instructions to minimize, as much as possible, the scope of the disclosure.

5. Reliability and Non–Disclosure

5.1. The Processor shall take reasonable steps to ensure the reliability of any employee, agent or contractor who may have access to the Controller Personal Data and only grant access to the personal data being processed on behalf of the Controller to persons under the Processor's authority who have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality and only on a need to know basis. The list of persons to whom access has been granted shall be kept under periodic review. On the basis of this review, such access to personal data can be withdrawn, if access is no longer necessary, and personal data shall consequently not be accessible anymore to those persons.

5.2. The Processor must ensure that all individuals which have a duty to Process Controller Personal Data:

5.2.1. Are informed of the confidential nature of the Controller Personal Data and are aware of Processor's obligations under this Agreement and the Principal Agreement in relation to the Controller Personal Data;

5.2.2. Have undertaken appropriate training/certifications in relation to the Data Protection Laws or any other training/certifications requested by Controller;

5.2.3. Are subject to user authentication and logon processes when accessing the Controller Personal Data in accordance with this Agreement, the Principal Agreement and the applicable Data Protection Laws.

5.3. The Processor shall at the request of the Controller demonstrate that the concerned persons under the Processor's authority are subject to the abovementioned confidentiality.

6. Personal Data Security

6.1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the Processor shall implement appropriate technical and organizational measures (Annex 2) to ensure a level of Controller Personal Data security appropriate to the risk in accordance with Article 32 of the GDPR, including but not limited to:

6.1.1. Pseudonymization and encryption;

6.1.2. The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

6.1.3. The ability to restore the availability and access to Controller Personal Data in a timely manner in the event of a physical or technical incident; and

6.1.4. A process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the Processing.

6.2. In assessing the appropriate level of security, the Processor shall take into account the risks that are presented by Processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Controller Personal Data transmitted, stored or otherwise Processed.

7. Sub-Processing

7.1. As of the Agreement Effective Date, the Controller hereby authorizes the Processor to engage those Sub-Processors set out in Annex 3. The Processor has the Controller's general authorisation for the engagement of sub-processors. The Processor shall inform in writing the Controller of any intended changes concerning the addition or replacement of sub-processors at least one month in advance, thereby giving the data Controller the opportunity to object to such changes prior to the engagement of the concerned sub-processor(s). Longer time periods of prior notice for specific sub-processing services can be provided in Annex 3.

7.2. With respect to each Sub-processor, the Processor shall:

7.2.1. Include terms in the contract between the Processor and each Sub-processor which are the same as those set out in this Agreement (back-to-back terms). Upon request, the Processor shall provide a copy of its agreements with Sub-Processors to Controller for its review.

7.2.2. Insofar as that contract involves the transfer of Controller Personal Data outside of the EEA, incorporate the Standard Contractual Clauses or such other mechanism as directed by the Controller into the contract between the Processor and each Sub-Processor to ensure the adequate protection of the transferred Controller Personal Data.

7.2.3. Remain fully liable to the Controller for any failure by each Sub-Processor to fulfill its obligations in relation to the Processing of any Controller Personal Data.

8. Data Subject Rights

8.1. Taking into account the nature of the Processing, the Processor shall assist the Controller by implementing appropriate technical and organizational measures, insofar as this is possible, for the fulfillment of the Controller's obligation to respond to requests for exercising Data Subject rights as laid down in GDPR.

8.2. The Processor shall promptly notify the Controller if it receives a request from a Data Subject, the Supervisory Authority and/or other competent authority under any applicable Data Protection Laws with respect to Controller Personal Data.

8.3. The Processor shall cooperate as requested by the Controller to enable the Controller to comply with any exercise of rights by a Data Subject under any Data Protection Laws with respect to Controller Personal Data and comply with any assessment, enquiry, notice or investigation under any Data Protection Laws with respect to Controller Personal Data or this Agreement, which shall include:

8.4. The provision of all data requested by the Controller within any reasonable timescale specified by the Controller in each case, including full details and copies of the complaint, communication or request and any Controller Personal Data it holds in relation to a Data Subject.

8.5. Where applicable, providing such assistance as is reasonably requested by the Controller to enable the Controller to comply with the relevant request within the timescales prescribed by the Data Protection Laws.

8.6. Implementing any additional technical and organizational measures as may be reasonably required by the Controller to allow the Controller to respond effectively to relevant complaints, communications or requests.

9. Personal Data Breach

9.1. The Processor shall notify the Controller without undue delay and, in any case, within seventy-two (72) hours upon becoming aware of or reasonably suspecting a Personal Data Breach. The Processor will provide the Controller with sufficient information to allow the
Controller to meet any obligations to report a Personal Data Breach under the Data Protection Laws. Such notification shall as a minimum include the following information to the extent it is known by the Processor:

9.1.1. Describe the nature of the Personal Data Breach, the categories and numbers of Data Subjects concerned, and the categories and numbers of Personal Data records concerned;

9.1.2. Communicate the name and contact details of the Processor's Privacy Officer or other relevant contact from whom more information may be obtained;

9.1.3. Describe the estimated risk and the likely consequences of the Personal Data Breach; and

9.1.4. Describe the measures taken or proposed to be taken to address the Personal Data Breach.

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

9.3. In the event of a Personal Data Breach, the Processor shall not inform any third party without first obtaining the Controller’s prior written consent, unless notification is required by EU or Member State law to which the Processor is subject, in which case the Processor shall, to the extent permitted by such law, inform the Controller of that legal requirement, provide a copy of the proposed notification and consider any comments made by the Controller before notifying the Personal Data Breach**.**

10. Data Protection Impact Assessment and Prior Consultation

10.1. The Processor shall provide reasonable assistance to the Controller with any data protection impact assessments which are required under Article 35 of GDPR and with any prior consultations to any supervisory authority of the Controller which are required under Article 36 of GDPR, in each case solely in relation to Processing of Controller Personal Data by the Processor on behalf of the Controller and considering the nature of the Processing and information available to the Processor.

11. Erasure or Return of Controller Personal Data

11.1. Processor shall promptly and, in any event, within 180 (one hundred and eighty) calendar days of the earlier of: (i) cessation of Processing of Controller Personal Data by Processor; or (ii) termination of the Principal Agreement, at the choice of Controller (such choice to be notified to Processor in writing) either:

11.1.1. Return a complete copy of all Controller Personal Data to the Controller by secure file transfer in such format as notified by the Controller to the Processor and securely erase all other copies of Controller Personal Data Processed by the Processor or any Sub-processor; or

11.1.2. Securely wipe all copies of Controller Personal Data Processed by Processor or any Sub-processor, and in each case, provide a written certification to the Controller that it has complied fully with the requirements of this section 10 on Erasure or Return of Controller Personal Data.

11.2. Processor may retain Controller Personal Data to the extent required by Union or Member State law, and only to the extent and for such period as required by Union or Member State law, and always provided that Processor shall ensure the confidentiality of all such Controller Personal Data and shall ensure that such Controller Personal Data is only Processed as necessary for the purpose(s) specified in the Union or Member State law requiring its storage and for no other purpose.

11.3. Processor will not retain any Personal Data for own purposes.

12. Audit Rights

12.1. Processor shall make available to the Controller, upon request, all information necessary to demonstrate compliance with this Agreement and allow for, and contribute to audits, including inspections by the Controller or another auditor mandated by the Controller of any premises where the Processing of Controller Personal Data takes place. The Processor shall permit the Controller, or another auditor mandated by the Controller to inspect, audit and copy any relevant records, processes and systems in order that the Controller may satisfy itself that the provisions of this Agreement are being complied with. The Processor shall provide full cooperation to the Controller with respect to any such audit and shall, at the request of the Controller, provide the Controller with evidence of compliance with its obligations under this Agreement. Processor shall immediately inform the Controller if, in its opinion, an instruction pursuant to this section Audit (Audit Rights) infringes the GDPR or other EU or Member State data protection provisions.

13. International Transfers of Controller Personal Data

13.1. Processor shall not Process Controller Personal Data nor permit any Sub-processor to Process the Controller Personal Data in a Third Country, other than with respect to those recipients in Third Countries (if any) listed in Annex 3 (Authorized Transfers of Controller Personal Data), unless authorized in writing by Controller in advance, via an amendment to this Agreement.

13.2. When requested by Controller, Processor shall – on behalf of the Controller – promptly enter into (or procure that any relevant Sub-processor enters into) an agreement including Standard Contractual Clauses and/or another legal basis for the transfer, in respect of any Processing of Controller Personal Data in a Third Country, which terms shall take precedence over those in this Agreement. Processor has already entered into standard contractual clauses with Sub-processors in third countries as listed in Annex 3. A copy of these can be obtained upon request.

14. Codes of Conduct and Certification

14.1. At the request of the Controller, the Processor shall comply with any Code of Conduct approved pursuant to Article 40 of GDPR and obtain any certification approved by Article 42 of the GDPR, to the extent that they relate to the Processing of Controller Personal Data.

15. General Terms

15.1. Subject to this section, the parties agree that this Agreement and the Standard Contractual Clauses shall terminate automatically upon termination of the Principal Agreement or expiry or termination of all service contracts entered into by the Processor with the Controller, pursuant to the Principal Agreement, whichever is later.

15.2. Any obligation imposed on the Processor under this Agreement in relation to the Processing of Personal Data shall survive any termination or expiration of this Agreement.

15.3. This Agreement, shall be governed by Danish law and any dispute shall be settled by the ordinary Danish courts.

15.4. Any breach of this Agreement shall constitute a material breach of the Principal Agreement.

15.5. With regard to the subject matter of this Agreement, in the event of inconsistencies between the provisions of this Agreement and any other agreements between the parties, including but not limited to the Principal Agreement, the provisions of this Agreement shall prevail with regard to the parties' data protection obligations for Personal Data of a Data Subject from a Member State of the European Union.

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

IN WITNESS WHEREOF, this Agreement is entered into and becomes a binding part of the Principal Agreement with effect from the Agreement Effective Date first set out above.

_______________________ ("Controller")

Signature ______________________________

Name _________________________________

Title __________________________________

Date Signed ____________________________

iMotions A/S ("Processor")

Signature ______________________________

Name _________________________________

Title __________________________________

Date Signed ____________________________

ANNEX 1: DETAILS OF PROCESSING OF CONTROLLER PERSONAL DATA

This Annex 1 includes certain details of the Processing of Controller Personal Data as required by Article 28(3) GDPR.

Subject matter and duration of the Processing of Controller Personal Data

The subject matter and duration of the Processing of the Controller Personal Data are set out in the Principal Agreement and this Agreement.

The nature and purpose of the Processing of Controller Personal Data

Controller Personal Data is stored, statistically analyzed, and aggregated to summary statistics that are relevant to the research interest of the Data Controller.

The types of Controller Personal Data to be Processed

Controller Personal Data can contain names, contact information, sociodemographic, biometric and survey data, camera, audio and screen recordings as well as all other kind of information collected by the Data Controller within the scope of his study/ studies that can be relating to an identifiable person who through this (or a combination of the collected) data can be directly or indirectly identified in particular by reference to an identifier.

The categories of Data Subject to whom the Controller Personal Data relates

Respondents - participants in the studies on whom the Controller Personal Data is collected.

Experimenters - persons supervising the studies and of whom, e.g. through audio or camera recordings, Personal Data can be collected during the study.

Unrelated third persons - persons located at the experimental site during data recording without active contribution to the study, whose Personal Data can, e.g. through audio or camera recordings, be collected during the study

ANNEX 2: TECHNICAL AND ORGANIZATIONAL MEASURES

1. Organizational security measures

1.1. Incident response and business continuity

1.1.1 Incidents handling / Personal Data Breaches

1.1.1.1 An incident response plan with detailed procedures is defined to ensure effective and orderly response to incidents pertaining to Personal Data.

1.1.1.2 Processor will report without undue delay to Controller any security incident that has resulted in a loss, misuse or unauthorized acquisition of any Personal Data.

1.1.2 Business continuity
Processor establishes the main procedures and controls to be followed in order to ensure the required level of continuity and availability of the IT system Processing Personal Data (in the event of an incident/Personal Data Breach).

1.2 Human resources

1.2.1 Confidentiality of personnel: Processor ensures that all employees understand their responsibilities and obligations related to the Processing of Personal Data. Roles and responsibilities are clearly communicated during the pre-employment and/or introduction process.

1.2.2 Training: Processor ensures that all employees are adequately informed about the security controls of the IT system that relate to their everyday work. Employees involved in the Processing of personal data are also properly informed about relevant data protection requirements and legal obligations through regular awareness campaigns, hereunder in relation to general awareness, internet and e-mail use, setting passwords, using encryption, etc.

2. iMotions Technology Overview

iMotions products are a Windows desktop application (“iMotions Lab”) and a cloud-based software-as-a-service application (“iMotions Online”). iMotions Lab offers optional remote processing options to process facial expression or gaze mapping data (“Batch processing”) as well as the optional distribution of studies through a weblink to remotely collect data from respondents (“iMotions Online Data Collection”). iMotions lab also offers an optional, cloud-based study manager (“iMotions Lab Management”). iMotions can also execute projects on behalf of a customer (“iMotions Enablement Services”).

2.1 iMotions Lab

As a consequence of the Controllers installation of iMotions Lab on the Controller’s PC, no personal data will be processed by iMotions A/S. Thus, no data processor relation is established, and the Controller’s own security measures apply.

2.2 Batch processing

If enabled in their license, users of iMotions Lab can upload batch processing jobs to the cloud containing, but not limited to, respondent camera or scene camera recordings.
Cloud batch processing is hosted with Microsoft Azure in the East US (Virginia), Central US (Iowa) and North Europe (Ireland) regions. Where data is being processed depends on system availability at the time the data is being uploaded, with the main data storage location being in the East US.

2.2.1 Batch processing infrastructure

The batch processing infrastructure is hosted on Microsoft Azure.
A copy of client data required for batch processing is stored in Azure Blob Storage. Completed batch processing results are downloaded by iMotions Lab from Blob Storage.
The batch processing service and the iMotions Lab application communicate using messages through Azure Service Bus.
The batch processing is executed on Azure virtual machines.

2.2.2 Authentication

User installation (iMotions Lab) uses a shared access key to upload and download data from the cloud processing infrastructure. The shared access key is distributed by iMotions Licensing server and is periodically updated.
Individual client storage location is inferred from a unique client key that is generated based on iMotions license system product key.
iMotions employees use their corporate Microsoft account to access cloud processing infrastructure.
Processing data uploaded to the service can be accessed/read by iMotions employees. However, this access is restricted to key personnel and used only for maintenance and diagnostics.

2.2.3 Encryption

Data is uploaded/downloaded from the desktop application to the blob storage over encrypted https connection.
Data is downloaded/uploaded by the gaze mapping servers to the blob storage over encrypted https connection.
Data is encrypted at rest using Microsoft storage encryption feature.

2.2.4 Backup

A copy of the batch processing data is uploaded by the desktop application to the cloud which is used for gaze mapping and Affdex post-processing.
Data is downloaded from the blob to the virtual machines for running the job and is cleaned up after the job finishes.
Respondent face videos are immediately deleted from blob storage after Affdex post-processing completes.
All other data uploaded from Batch processing, except Affdex videos, stays in the Blob storage for 30 days after which this data and any snapshots are deleted.

2.3 iMotions Online

iMotions Online is a service that allows users to set up studies, collect, and analyze respondent data in a browser-based application. Studies created on iMotions Online are shared with the respondent through a weblink. It consists of a browser-based web application user interface and the servers that it communicates with.

2.3.1 Infrastructure

Studies are created in iMotions Online. A unique link to the study can be created and shared with respondents.

Respondents use their own web browser to participate in the study. Data is collected in the browser, which may require the respondent to accept access to their webcam and recording of their screen. No study data is saved on respondents' computers after it has been uploaded to iMotions Online.
Data collected from the respondents is stored on iMotions Online.
iMotions Online is hosted with Amazon Web Services in Germany (Frankfurt) or the US East (N. Virginia) region.
Content delivery network uses CloudFront.
Servers and workers use Elastic Compute Cloud (EC2). Database uses Relational Database Service (RDS).
File storage uses Simple Storage Service (S3).
The Data Controller can be set up by iMotions employees to have their data hosted in the Germany (Frankfurt) region instead of the default US East (N. Virginia) region.
Respondent recordings are then processed to extract eye tracking data and facial coding data from the recorded videos. Processing is executed on iMotions' local server hosted in Denmark (Copenhagen) but will be offloaded to Amazon Web Services if additional server capacities are required.
Once the study is completed and processed, it can be further processed and analyzed on iMotions Online.

2.3.2 Authentication

Users have individual accounts that only let them access the data for their own company. Users can enable two factor authentication for logging in to their accounts. This can be further customized by adding/removing access to specific features from users individually (i.e. role-based security).
The login process happens via OAuth2 username-password flow (a.k.a. "resource owner credentials grant"), and the provided access token is then used to authenticate all subsequent communication between the browser and REST API.
Users' passwords are stored in the database in salted and hashed form with bcrypt. iMotions employees use their corporate G Suite accounts to login instead.
Files from file storage that are intended to be viewed directly in the browser have a key embedded in their URL that is only available from an authenticated API endpoint.

2.3.3 Encryption

Data is encrypted in transit by using HTTPS for all communication, including browser to CDN, CDN to load balancer, load balancer to server and server to database/file storage. Accidentally accessing the web application with HTTP will automatically redirect to HTTPS.
Data is encrypted at rest in the database with Amazon's RDS encryption feature. This also includes backups.
Data is encrypted at rest in the file storage with Amazon's S3 server-side encryption feature. Credentials used by servers are stored in encrypted form in Amazon Parameter Store.
Data on iMotions' local server is encrypted at rest using full disk encryption (FDE).

2.3.4 Backup

Database backups are performed automatically with Amazon's RDS backup feature and are retained for 14 days.

2.4. iMotions Online Data Collection (ODC)

iMotions ODC is a service that allows users to distribute studies created in iMotions Lab through a weblink to collect respondent data in a browser-based application.

2.4.1 Infrastructure

Studies are created by the user in iMotions Lab (see section 2.1 of Annex 2).

From here, studies are uploaded to iMotions Online (see section 2.3 of Annex 2). A unique link to the study can be created and shared with respondents.

Respondents use their own web browser to participate in the study. Data is collected in the browser, which requires the respondent to accept access to their webcam and recording of their screen. No study data is saved on respondents' computers after it has been uploaded to the iMotions Cloud.

Data collected from the respondents is stored in iMotions Online, hosted with Amazon Web Services (see section 2.3 of Annex 2).

Respondent recordings are then processed to extract eye tracking data and, if enabled, facial coding data from the recorded videos. Processing is executed on iMotions' local server (see section 2.3.1 of Annex 2) but will be offloaded to Amazon Web Services if additional server capacities are required. If online extraction of facial coding data is not enabled for the company account, this can be accomplished after downloading the study.

Once the study is completed and processed, it is then downloaded to the user's locally installed iMotions Desktop license for further processing and analyses.

2.4.2 Authentication

For authentication on iMotions Online, please see section 2.3.2 of Annex 2.

For authentication on iMotions Lab, please see section 2.1. of Annex 2.

2.4.3 Encryption

For encryption on iMotions Online, please see section 2.3.3 of Annex 2.

For encryption on iMotions Lab, please see section 2.1. of Annex 2.

Data transfer between iMotions Online and iMotions Lab is encrypted using SSL/HTTPS encryption.

Data collected from the respondent is encrypted using SSL/HTTPS encryption when sending it to iMotions Online.

2.4.4 Backup

For backup on iMotions Online, please see section 2.3.4 of Annex 2.

For backup on iMotions Lab, please see section 2.1. of Annex 2.

2.5 iMotions Lab Management

iMotions Lab Management is a service to deploy a study across different data collection stations, and to merge data from these data collection stations into a single study.

2.5.1 *Infrastructure*

Studies are created by the user in iMotions Lab (see section 2.1 of Annex 2).

From here, studies are uploaded to iMotions Online (see section 2.3 of Annex 2), and then downloaded to other installations of iMotions Lab on Windows desktop PCs.

Data is collected in iMotions Lab. After data collection is done, data is uploaded to and merged on iMotions Online. The merged data is then again downloaded to iMotions Lab.

2.5.2 Authentication

For authentication on iMotions Online, please see section 2.3.2 of Annex 2.

For authentication on iMotions Lab, please see section 2.1. of Annex 2.

2.5.3 Encryption

For encryption on iMotions Online, please see section 2.3.3 of Annex 2.

For encryption on iMotions Lab, please see section 2.1. of Annex 2.

Data transfer between iMotions Online and iMotions Lab is encrypted using SSL/HTTPS encryption.

Data collected from the respondent is encrypted using SSL/HTTPS encryption when sending it to iMotions Online.

2.5.4 Backup

For backup on iMotions Online, please see section 2.3.4 of Annex 2.

For backup on iMotions Lab, please see section 2.1 of Annex 2.

2.6 iMotions Enablement Services

iMotions Enablement Services provide Services to the Data Controller in executing and analysing biosensor studies and delivers reports and insights as agreed upon in the MSA.

2.6.1 Infrastructure

Employees of iMotions Enablement Services collect and store the data on local PCs and portable data storage devices.

Files may be transferred between local PCs on portable storage devices and/or using third party file sharing services as listed in Annex 3.

Back-ups of the data collected for Services purposes may be stored on Servers hosted by Google LLC. Please view the latest version of Google LLC's Terms of Service as well as Data Processing Terms here:

https://cloud.google.com/security/gdpr/resource-center/contracts-and-terms

Data collected for Services purposes may be processed on iMotions Online (see section 2.3 of Annex 2) and/ or iMotions Batch Processing (see section 2.2 of Annex 2).

2.6.2 Authentication

Local PCs are password-protected.

Corporate G Suite accounts with Two-factor-authentication are used to sign in to the Drive hosted by Google LLC.

For the iMotions Batch processing, authentication takes place as described in section 2.2.2. of Annex 2.

2.6.3 Encryption

Local PCs and storage devices are AES password encrypted.

For the iMotions Batch processing, encryption is enabled as described in section 2.2.3 of Annex 2.

2.6.4 Back-ups

If iMotions is responsible for the collection of data for Services purposes, backups are performed regularly. Backups are deleted after the completion of the data collection and post-processing of the study.

2.6.5 Anonymization

Personal data is removed from the data collected for Services purposes as soon as the data is successfully post-processed and no longer necessary for e.g. data cleaning purposes or explanation of data outliers.

Anonymous datasets are stored as agreed upon with the Data Controller.Previous copies of the study containing personal data are removed as soon as an anonymized version of the study data was created.

ANNEX 3: AUTHORIZED TRANSFERS OF CONTROLLER PERSONAL DATA

List of Approved Sub-processors as at the Agreement Effective Date to be included here. Please include (i) full legal name; (ii) Processing activity; (iii) location of service center(s).

Group internal:

No.	**Sub-processor (full legal name)**	**Processing activity**	**Location of service center(s).**	**Safeguards**
1.	iMotions, Inc.	Provision of services under this Agreement	38 Chauncy Street Floor 8, Suite 800 Boston, MA 02111	Standard Contractual Clauses

External:

No.	**Sub-processor (full legal name)**	**Processing activity**	**Location of service center(s).**	**Safeguards**
1.	Amazon Web Services, Inc.	Storage of data	In Germany (Frankfurt) or the East US (Virginia) region	Standard Contractual Clauses
2.	Microsoft Azure Microsoft Corporation	Hosting of cloud batch processing	In the East US (Virginia), Central US (Iowa) and North Europe (Ireland) regions	Standard Contractual Clauses
3.	Google LLC	Data storage	Please refer to: https://www.google.com/about/datacenters/inside/locations/index.html	Standard Contractual Clauses
4.	WeTransfer B.V	Data transfer	In the EU and the US, please refer to: https://wetransfer.com/legal/terms?_ga=2.225064218.1859341274.1546860142-1801721794.1544103225	Standard Contractual Clauses