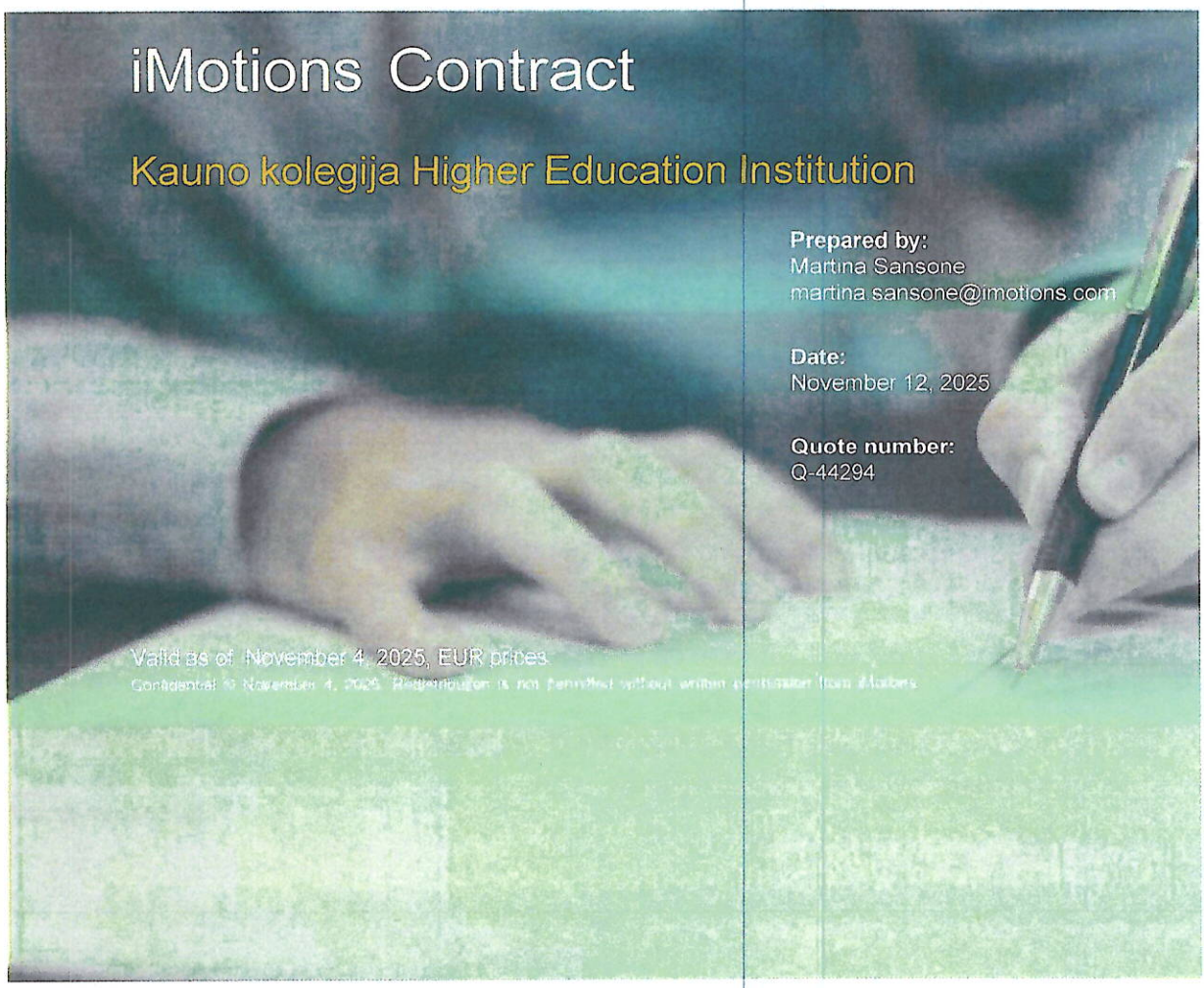
IMOTIONS


iMotions Contract
Kauno kolegija Higher Education Institution
Prepared by:
Martina Sansone
martina.sansone@imotions.com
Date:
November 12, 2025
Quote number:
Q-44294
Valid as of November 4, 2025, EUR prices
Confidential © November 4, 2025. Reproduction is not permitted without written permission from iMotions

GOODS AND SERVICES CONTRACT No. Q-44294, SUT-16428/2025, REG. No. F25-272

All prices indicated in this contract are exclusive of taxes

1. DESCRIPTION OF GOODS AND SERVICES

iMotions Software Suite

Name	Price	#	Years	Total Price	Note
iMotions Module - Screen-Based Eye Tracking	€3.400,00	1		€3.400,00	Eye tracking research software
iMotions Module - Virtual Reality Eye Tracking	€3.400,00	1		€3.400,00	VR Eye tracking research software
iMotions Module - GSR	€3.400,00	1		€3.400,00	Galvanic Skin Response/Electrodermal Activity research software
iMotions Module - EEG	€3.400,00	1		€3.400,00	Electroencephalography research software
iMotions Module - EMG	€3.400,00	1		€3.400,00	Electromyography research software
iMotions Module - Voice Analysis - audEERING	€3.400,00	1		€3.400,00	Voice Analysis research software
iMotions Module - Respiration	€3.400,00	1		€3.400,00	Inhalation & Exhalation related metrics
iMotions Module - Automated AOIs	€1.900,00	1		€1.900,00	Automated placement of Areas of Interest (AOI)
iMotions Module - Remote Data Collection	€3.400,00	1		€3.400,00	Limited use software - Renewal required for continued use. Fair Usage Policy applies to prevent misuse or excessive use.
iMotions Module - Web Based Eye Tracking	€3.400,00	1		€3.400,00	Web Based Eye Tracking Research Software.
Subtotal				€32.500,00	

Accessories and consumables

Name	Price	Quantity	Total Price	Note
Smart Eye Mobile Testing Stand	€650,00	1	€650,00	Mobile Testing Stand for use with Smart Eye eye trackers and mobile devices.
NeuroElectrics Enobio 8,20,32 Forehead positions (headband and electrodes)	€550,00	1	€550,00	Enobio 8,20,32 headband and 8 foretrodes
Subtotal			€1.200,00	

Hardware

Name	Price	Quantity	Total Price	Note
Smart Eye AI-X 60HZ	€2.790,00	1	€2.790,00	Eye tracking bar (Ships from: Sweden)
Varjo XR-4	€5.990,00	1	€5.990,00	HMD with built-in eye tracking - (Ships from: China)
PLUX Biosignals EDA/ GSR sensor	€140,00	1	€140,00	GSR sensor (Ships from Portugal)
PLUX Biosignals EMG sensor	€140,00	1	€140,00	EMG sensor (Ships from Portugal)
PLUX Biosignals RIP sensor	€795,00	1	€795,00	RIP sensor (Ships from Portugal)
PLUX Biosignals 8-Channel System Kit	€4.425,00	1	€4.425,00	Includes 8-Channel Hub + USB Cable + Charger + Bluetooth Dongle + 200 Electrodes + Carrying Case Ships from EU (Portugal)
NeuroElectrics Enobio 8	€5.270,00	1	€5.270,00	EEG Headset (Ships from: Spain)
Subtotal			€19.550,00	

Hardware Maintenance

Name	Price	Quantity	Total Price	Note
Varjo Base Pro	€2.500,00	1	€2.500,00	Varjo Base Pro perpetual license
Subtotal			€2.500,00	

Shipping and Handling

Name	Price	Quantity	Total Price	Note
Shipping and Handling (Hardware)	€850,00	1	€850,00	Incoterms: DAP (Delivery At Place)
Subtotal			€850,00	

Training

Name	Price	Quantity	Total Price	Note
iMotions VR Additional Set Up	€1.400,00	1	€1.400,00	VR set up, 2-3 hours
Subtotal			€1.400,00	

Grand TOTAL **€ 58.000,00**

2. PUBLIC INSTITUTION DETAILS

Contract No.: Q-44294, SUT-16428/2025,

REG. No. F25-272

Valid until: 28 November 2026

Contact:

Bill to: Kauno kolegija Higher Education Institution
Pramones av. 20
Kaunas LT-50468
Lithuania

Ship to: Kauno kolegija Higher Education Institution
Gedimino st. 41
Kaunas LT-44240
Lithuania

License Validity The iMotions Software Suite is valid starting from 29 November 2024 to 28 November 2025. If the iMotions Software Suite is not renewed by the end of this period, Customer will lose the ability to collect data using iMotions' Software and will be limited to analysis only functionality on previously collected data.
The expected annual cost of the iMotions Software Suite after this period is €1.800,00 (subject to the attached Terms & Conditions).

1.Under this Agreement, an annual "iMotions" software package is purchased for the period following the expiry of the current license, i.e., from 29 November 2025 to 28 November 2026.

2. The total contract price is EUR 59,800.00 (fifty-nine thousand eight hundred euros and 00 cents). The price is final and shall remain unchanged throughout the term of the Agreement.

3. Kaunas kolegija Higher Education Institution undertakes to pay the Price for the *iMotions* software packages and hardware no later than within 30 calendar days from the date of the invoice issuance. The Supplier shall submit the invoice to Kaunas kolegija Higher Education Institution through the general information system for invoice

administration "SABIS" (https://sabis.nbfc.lt/).

Delivery Software will be delivered via email within 72 hours of receipt of the signed agreement. Hardware delivery times can be viewed in the order form price summary.

Payment Terms Net 30

Signatures

Vendor: iMotions

Signature: [redacted]

Representative: Peter Hartzbech

Title: CEO

Date: 12/11/2025

Consumer name: Kauno kolegija Higher Education Institution

Signature:

Representative: Andrius Brusokas

Title: Director

Date: 14/11/2025

KAUNO KOLEGIJA

3. GENERAL TERMS AND CONDITIONS

This agreement is between iMotions A/S (Kristen Bernikows Gade 6, 4th Floor, 1105 Copenhagen, Denmark) and you, the above stated customer entering into this agreement (Customer), effective as of the date of the last signature above. The iMotions software, modifications, enhancements, documentation and license keys provided to Customer (Software) are licensed and are not sold.

1. SCOPE. This agreement and its appendices describe the licensing of the Software and/or the hardware purchased/ rented and/or services provided to Customer under the Order Form.

1.1. This Agreement is concluded as a "green procurement" contract, in accordance with Subparagraph 4.4.3 of the Description of the Application Procedure for Environmental Criteria, approved by the Order No. D1-508 of the Minister of Environment of 28 June 2011 "List of Products to which Environmental Criteria Apply in Public Procurement, Environmental Criteria, and the Procedure for Applying Environmental Criteria to Goods, Services, or Works by Contracting Authorities." This procurement is considered green because the purchased item is software and licenses.

2. LICENSE. Subject to the other terms of this agreement, iMotions grants Customer, under an order, a non-exclusive, non-transferable license, for the duration specified on the Order Form and up to the number of Seat licenses purchased to:

A. Use the Software only in Customer's business purposes for commercial licenses, or in the case of academic licenses for academic research purposes only, and
B. Make one copy of the Software for archival and backup purposes.
C. The "iMotions Module - Eye Tracking Glasses" may be used with one hardware brand specified by the Customer at purchase. The Customer may request to change this brand subject to iMotions' prior written approval and any required re-configuration. Use with any additional brand requires purchase of a separate module. iMotions does not guarantee compatibility with all brands.

Seat means each single personal computer.

For the avoidance of doubt, if Customer has purchased an academic license, then it may not use the Software for any commercial purposes, unless it is part of a research project belonging to and executed by an academic institution. Contact iMotions regarding purchasing a commercial license, if Customer wants to use the Software for commercial purposes.

3. RESTRICTIONS. Customer may not:

A. Transfer, assign, sublicense, rent, create derivative works of the Software;
B. Reverse engineer, decompile, disassemble, or translate the Software; or
C. Evaluate the Software for the purpose of competing with iMotions or operate the Software other than in accordance with its technical documentation and applicable law.

4. PAYMENT. Customer will pay all fees due on receipt of an invoice, unless otherwise provided on the order form, plus applicable taxes, customs related fees. If payments are not made on the agreed dates, iMotions reserves the right to suspend the license until payments are received. For payments made by credit card, there is a 2.9% fee on all purchases above 2500 USD/EUR.

5. PRICING. All prices quoted on the Order Form are only valid until the "Expires" date on the "Order Form". Any future renewal costs of iMotions Software License mentioned on the "OrderForm" are subject to change.

6. MUTUAL CONFIDENTIALITY.

a. Definition of Confidential Information. Confidential Information means all non-public information disclosed by a party (Discloser) to the other party (Recipient), whether orally or in writing, that is designated as confidential or that reasonably should be understood to be confidential given the nature of the information and the circumstances of disclosure (Confidential Information).
b. Protection of Confidential Information. The Recipient must use the same degree of care that it uses to protect the confidentiality of its own confidential information (but in no event less than reasonable care) not to disclose or use any Confidential Information of the Discloser for any purpose outside the scope of this agreement. The Recipient must make commercially reasonable efforts to limit access to Confidential Information of Discloser to those of its employees and contractors who need such access for purposes consistent with this agreement and who have signed confidentiality agreements with Recipient no less restrictive than the confidentiality terms of this agreement.

c. Exclusions. Confidential Information excludes information that: (i) is or becomes generally known to the public without breach of any obligation owed to Discloser, (ii) was known to the Recipient prior to its disclosure by the Discloser without breach of any obligation owed to the Discloser, (iii) is received from a third party without breach of any obligation owed to Discloser, or (iv) was independently developed by the Recipient without use or access to the Confidential Information. The Recipient may disclose Confidential Information to the extent required by law or court order, but will provide Discloser with advance notice to seek a protective order.

7. PROPRIETARY RIGHTS. The Software, workflow processes, user interface, initial designs, technical documentation, and other technologies provided by iMotions as part of the Software are the proprietary property of iMotions and its licensors, and all right, title and interest in and to such items, including all associated intellectual property rights, remain only with iMotions and its licensors. The Software is protected by applicable copyright and other intellectual property laws. Customer may not remove any product identification, copyright, trademark or other notice from the Software. iMotions reserves all rights not expressly granted.

8. WARRANTY, REMEDY, and DISCLAIMER. For new license purchases (not any renewals of term based licenses), iMotions warrants that the Software will perform in substantial accordance with its product documentation for a period of 90 days from the date of the order form. This warranty will not apply to any problems caused by software not licensed to Customer by iMotions, use other than in accordance with the technical documentation, or misuse of the Software. The warranty only covers problems reported to iMotions during the warranty period or 30 days after. Customer will cooperate with iMotions in resolving any warranty claim.

a. EXCLUSIVE REMEDY AND SOLE LIABILITY. IMOTIONS WILL USE COMMERCIALLY REASONABLE EFFORTS TO REMEDY COVERED WARRANTY CLAIMS WITHIN A REASONABLE PERIOD OF TIME OR REPLACE THE SOFTWARE, OR IF IMOTIONS CANNOT DO SO IT WILL REFUND TO CUSTOMER THE LICENSE FEE PAID. THIS REMEDY IS CUSTOMER'S EXCLUSIVE REMEDY, AND IMOTIONS' SOLE LIABILITY FOR THESE WARRANTY CLAIMS.

b. DISCLAIMER OF WARRANTIES. IMOTIONS disclaims all other express and implied warranties, including without limitation the implied warranty of merchantability, non-infringement, and fitness for a particular purpose. customer understands that the Software may not be error free, and use may be interrupted. IMOTIONS SPECIFICALLY DISCLAIMS ANY LIABILITY FOR DECISIONS MADE BY Customer OR ANY THIRD PARTY BASED ON ANY DATA or the results of any study.

c. The Customer is responsible for ensuring its compliance with laws and shall ensure that its use of the Software is compliant with this agreement and applicable laws and regulations, such as the EU AI Act and data privacy laws. Customer's use cases are the sole responsibility of Customer. iMotions disclaims all liability for Customer's decisions regarding certain use cases compliance with applicable laws..

9. RESALE OF THIRD PARTY SOFTWARE AND HARDWARE.

a. Applicable terms. If iMotions resells any third-party software or hardware under an order (Third Party Technology), then such software or hardware is exclusively governed by terms on Attachment A and not the terms applicable to the Software.

b. Liability. The Service interfaces with or integrates with certain third-party services and products. iMotions does not control and is not liable for any unavailability of such third party services

10. TERMINATION. This agreement expires at the end of the license period specified in the accompanying order form, unless this agreement terminates otherwise in accordance with this section. Either party may terminate this agreement upon a material breach of the other party after a 30 day notice/cure period, if the breach is not cured during such time period. Upon termination of this agreement or a license, Customer must discontinue using the Software, de-install and destroy or return the Software and all copies, within 5 days. Upon iMotions' request, Customer will provide written certification of such compliance.

11. ANNUAL SUPPORT. If listed on the Order Form iMotions' annual technical support and maintenance services ("Support and Upgrade") are provided as specified in the order form. Support is provided under the Support policies then in effect. iMotions may change its Support terms and pricing, but Support will not materially degrade during any Support term. More details about Support are located at https://help.imotions.com

12. CUSTOMER SUPPORT PROGRAM. If listed on the Order Form, the services under iMotions' Customer Support Program ("CSP") are provided for the time period as specified in the order form. The CSP services are provided under the policies then in effect. iMotions may change its CSP terms and pricing from time to time, but the services provided under the CSP will not materially degrade during any term. More details about the CSP are located at https:// help.imotions.com. Due to the ever evolving nature of the iMotions' software, being a member of the CSP is required to maintain the proper operation and usefulness of the software.

13. LIMIT ON LIABILITY.

a. EXCLUSION OF INDIRECT DAMAGES. IMOTIONS IS NOT LIABLE FOR ANY INDIRECT, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF OR RELATED TO THIS AGREEMENT (INCLUDING, WITHOUT LIMITATION, COSTS OF DELAY; LOSS OF OR UNAUTHORIZED ACCESS TO DATA OR INFORMATION; AND LOST PROFITS, REVENUE OR ANTICIPATED COST SAVINGS), EVEN IF IT KNOWS OF THE POSSIBILITY OF SUCH DAMAGE OR LOSS.

b. TOTAL LIMIT ON LIABILITY. IMOTIONS' TOTAL LIABILITY ARISING OUT OF OR RELATED TO THIS AGREEMENT (WHETHER IN CONTRACT, TORT OR OTHERWISE) DOES NOT EXCEED THE AMOUNT PAID OR PAYABLE BY CUSTOMER FOR THE LICENSE TO THE SOFTWARE BUT IN THE CASE OF TERM BASED LICENSES WHAT CUSTOMER HAS PAID FOR THE LICENSE IN THE 12 MONTH PERIOD PRIOR TO THE EVENT WHICH GAVE RISE TO THE CLAIM.

14. DEFENSE OF THIRD PARTY CLAIMS. iMotions will defend or settle any third party claim against Customer to the extent that such claim alleges that the Software violates a copyright, patent, trademark or other intellectual property right, if Customer, promptly notifies iMotions of the claim in writing, cooperates with iMotions in the defense, and allows iMotions to solely control the defense or settlement of the claim.

a. Costs. iMotions will pay infringement claim defense costs it incurs in defending Customer, and iMotions negotiated settlement amounts, and court awarded damages.

b. Process. If such a claim appears likely, then iMotions may modify the Software, procure the necessary rights, or replace it with the functional equivalent. If iMotions determines that none of these are reasonably available, then iMotions may terminate the Software license and refund (as applicable) any prepaid and unused term based license fees or the license fee for other licenses (amortized over a 5-year period from the date of the order).

c. Exclusions. iMotions has no obligation for any claim arising from: iMotions' compliance with Customer's specifications; a combination of the Software with other technology or aspects where the infringement would not occur but for the combination; or technology or aspects not provided by iMotions. THIS SECTION CONTAINS CUSTOMER'S EXCLUSIVE REMEDIES AND IMOTIONS' SOLE LIABILITY FOR INTELLECTUAL PROPERTY INFRINGEMENT CLAIMS.

15. GOVERNING LAW AND EXCLUSIVE FORUM. This agreement is governed by the laws of Denmark (without regard to conflicts of law principles) for any dispute between the parties or relating in any way to the subject matter of this agreement. The Customer submits to this personal jurisdiction and venue. Nothing in this agreement prevents either party from seeking injunctive relief in a court of competent jurisdiction. The prevailing party in litigation is entitled to recover its attorneys' fees and costs from the other party.

16. MISCELLANEOUS.

a. Entire Agreement. This agreement and the order form constitute the entire agreement between the parties and supersede any prior or contemporaneous negotiations or agreements, whether oral or written, related to this subject matter. Customer is not relying on any representation concerning this subject matter, oral or written, not included in this agreement. No representation, promise or inducement not included in this agreement is binding.

b. Non-Assignment. Neither party may assign or transfer this agreement to a third party, nor delegate any duty, except that the agreement and all orders may be assigned, without the consent of the other party, as part of a merger, or sale of all or substantially all of the business or assets, of a party.

c. Independent Contractors. The parties are independent contractors with respect to each other.

d. Enforceability. If any term of this agreement is invalid or unenforceable, the other terms remain in effect.

e. Order of Precedence. If there is an inconsistency between an order form and this agreement, the order form prevails.

f. Survival of Terms. Any terms that by their nature survive termination of this agreement for a party to assert its rights

and receive the protections of this agreement, will survive (including without limitation, the confidentiality terms). The UN Convention on Contracts for the International Sale of Goods does not apply. UCITA if enacted in this state does not apply.

g. Money Damages Insufficient. Any breach by a party of this agreement or violation of the other party's intellectual property rights could cause irreparable injury or harm to the other party. The other party may seek a court order to stop any breach or avoid any future breach.

h. Compliance Audit. No more than once in any 12-month period and upon at least 30 days advance notice, iMotions (or its representative) may audit Customer's usage of the Software at any Customer facility. Customer will cooperate with such audit. Customer agrees to pay within 30 days of written notification any fees applicable to Customer's use of the Software in excess of the license.

i. Modification Only in Writing. No modification or waiver of any term of this agreement is effective unless signed by both parties.

j. Export Compliance. Customer must comply with all applicable export control laws of the United States, foreign jurisdictions and other applicable laws and regulations.

k. No PO Terms. iMotions rejects additional or conflicting terms of a Customer's form-purchasing document.

l. Open Source Software Licenses. The Software may contain embedded open source software components, which are provided as part of the Software and for which additional terms may be included in the technical documentation.

m. Third Parties. This agreement is not intended nor will it be interpreted to confer any benefit, right or privilege in any person or entity not a party to this agreement. Any party who is not a party to this agreement has no right under any law to enforce any term of this agreement.

n. Tax. You agree to pay directly or reimburse iMotions and Vendor for any taxes (including sales or excise taxes, value added taxes, landing fees, import duties and the like), however designated and whether foreign or domestic, arising out of this agreement, imposed on the licensed materials or the thereof, or iMotions' or Vendor's performance or material under this agreement. Notwithstanding the foregoing, iMotions will be solely responsible for its income tax obligations and all employer reporting and payment obligations with respect to its personnel. All prices shared by iMotions are excluding tax.

17. Person responsible for the execution of the Contract: Project Coordinator Lina Navalinskaitė, e-mail: l[redacted], who, among other things, is authorized to sign the goods acceptance-transfer act and other documents related to the performance of the Contract. The person responsible for the publication of the Contract and its amendments in accordance with the provisions of Article 86(9) of the Law on Public Procurement is Vilma Mykolaitienė, Senior Public Procurement Specialist.

4 ANNEXES

Attachment A

THIRD PARTY HARDWARE - Purchase or Rental

1. HARDWARE. iMotions does not manufacture or provide its own hardware, as iMotions is a software company. iMotions will provide any third-party hardware purchased by Customer under the order (**Hardware**) with iMotions at the locations set forth on the order (**Locations**).

2. DELIVERY
iMotions does not ship hardware directly to the customer. iMotions' partners dropship the hardware directly. Custom fees and charges may apply and are to be paid for by the customer.

3. INSTALLATION. The customer is responsible for the installation of the Hardware, and iMotions will provide certain supplemental Hardware instructions regarding installation and configurations with the iMotions Software.

4. OWNERSHIP

- Purchase. If Customer purchases Hardware from iMotions, title to and ownership of the Hardware transfers to Customer when the fees for the Hardware and delivery as specified on order form are paid in full.

- Rental. If Customer rents Hardware from iMotions, title to and ownership of the Hardware remain with iMotions. If any Hardware that Customer has rented from iMotions is lost, damaged or destroyed, Customer must pay iMotions the then-current list price for the Hardware.

- Rental payments are not refundable.
- Customer must return rented Hardware at its own expense for receipt by iMotions on or before the end date described in the order form. If the hardware is not returned on or before the end date of the rental period, or the rental period has been extended, iMotions reserves the right to charge the customer the then-current list price for the Hardware.

5. ASSIGNMENT OF HARDWARE WARRANTY AND LEVEL 1 TECHNICAL SUPPORT.

- iMotions hereby assigns and transfers the Hardware manufacturer's warranty to Customer.
- iMotions will cooperate with Customer regarding Hardware warranty issues and will provide basic level 1 technical support for the Hardware sold under an order.

5. DATA PROCESSING AGREEMENT

This Data Protection Agreement ("**Agreement**"), dated November 4, 2025 ("**Agreement Effective Date**") forms part of the Software Licence Agreement (SLA), Master Services Agreement (MSA), or Sales Contract ("**Principal Agreement**") between: **Kauno kolegija Higher Education Institution**, Pramones av. 20, LT-50468 Kaunas, Lithuania (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 and Lithuanian 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 and Lithuanian law and any dispute shall be settled by the ordinary Danish or Lithuanian 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.

ANNEXES

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 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 Remote Data Collection"). iMotions Lab also offers an optional, cloud-based study manager ("iMotions Lab Management"). iMotions Online, iMotions Remote Data Collection, and iMotions Lab Management can all be accessed through iMotions Cloud. 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 on iMotions Cloud to 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 on iMotions Cloud. 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. 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. Data Retention

No study data is saved on respondents' computers after it has been uploaded to iMotions Online. Webcam videos of the respondent are separated from the study after processing and deleted after 14 days. Data collected from the respondents is stored on iMotions Online. Studies are removed from the study library after 180 days of inactivity and scheduled for permanent deletion after an additional 90 days. If the study has not been reactivated by the user, it is permanently deleted after another 30 days. Log files are stored for 30 days, after which they are zipped and stored encrypted and at rest in a private AWS S3 bucket for 6 months.

2.3.3. 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.

2.3.4. 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).
2.3.5. Backup
Database backups are performed automatically with Amazon's RDS backup feature and are retained for 14 days.

2.4. iMotions Remote Data Collection (RDC)
iMotions RDC is a service that allows users to distribute studies created in iMotions Lab through a weblink generated on iMotions Cloud, 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 Cloud (see section 2.3.1 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 2.3.1 of Annex 2). Respondent recordings are then processed to extract eye tracking data and, if enabled, facial coding data as well as respiration 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. Data retention
Studies are retained on iMotions Cloud until they are removed by the user.
2.4.3. Authentication
For authentication on iMotions Cloud, please see section 2.3.3 of Annex 2. For authentication on iMotions Lab, please see section 2.1. of Annex 2.
2.4.4. Encryption
For encryption on iMotions Cloud, please see section 2.3.4 of Annex 2. For encryption on iMotions Lab, please see section 2.1. of Annex 2. Data transfer between iMotions Cloud 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.
2.4.5. Backup
For backup on iMotions Cloud, please see section 2.3.5 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 Cloud (see section 2.3.1 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. Data retention
Studies are retained on iMotions Cloud until they are removed by the user.
2.5.3. Authentication
For authentication on iMotions Cloud, please see section 2.3.3 of Annex 2. For authentication on iMotions Lab, please see section 2.1. of Annex 2.
2.5.4. Encryption
For encryption on iMotions Cloud, please see section 2.3.4 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.
2.5.5. Backup
For backup on iMotions Cloud, please see section 2.3.5 of Annex 2. For backup on iMotions Lab, please see sectin 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); (iv) Safeguards.

Group internal:

1. iMotions, Inc.; Provision of services under this Agreement; 38 Chauncy Street,Floor 8, Suite 800, Boston, MA 02111; Standard Contractual Clauses
2. Affectiva Inc; Provision of services under this Agreement; 38 Chauncy Street,Floor 8, Suite 800, Boston, MA 02111; Standard Contractual Clauses

External:

1. Amazon Web Services; Inc. Storage of data; Germany (Frankfurt) or the US (Virginia) region; Standard Contractual Clauses
2. Microsoft Azure; 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/abo ut/datacenters/inside/locations/ index.html; Standard Contractual Clauses
4. WeTransfer; Data transfer; In the EU and the US, please refer to: https://wetransfer.com/explore/legal/terms; Standard Contractual Clauses
5. SFDC Ireland Limited; CRM; France, EU; Standard Contractual Clauses
6. Zendesk Inc.; Support Ticket Management; In the US, EU, UK, or APAC region, please refer to: https:// support.zendesk.com/hc/en-us/articles/4408825765530-Data-Hosting-Locations-for-Your-Zendesk-Service-Data; Standard Contractual Clauses.