



DATA PROCESSING AGREEMENT FOR LITMOS SERVICES

This Data Processing Agreement (“DPA”), by and between Litmos US, L.P (“Litmos”) and Customer (defined below and together with Litmos, the “Parties”), is incorporated into and forms part of the Litmos Cloud Terms of Service available at www.litmos.com/termsandconditions (“Agreement”). This DPA applies to the Personal Data processed by Litmos in connection with its Service pursuant to the Agreement.

BACKGROUND

- (A) The Customer and Litmos have entered into the Agreement pursuant to which Litmos processes certain Customer Data as a processor for and on behalf of and at the instruction of the Customer.
- (B) Certain Data Protection Laws require that all processing of personal data by a processor must be pursuant to a written contract containing certain provisions.
- (C) This DPA is entered into between the Customer and Litmos to ensure that Litmos’s processing of Customer Data that qualifies as Personal Data complies with the requirements of the applicable Data Protection Laws.

OPERATIVE PROVISIONS

1. DEFINITIONS AND INTERPRETATION

- 1.1 All terms included in this DPA shall be in addition to, and not in replacement of, those terms set forth in the Agreement. In the event of any conflict or inconsistency between the terms in the Agreement and the terms in this DPA, the terms of this DPA will control. All capitalized terms not defined in this DPA shall be read to have the meaning given to those terms in the Agreement.

“Controller” means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of Personal Data, and includes the term “Business” as defined by the California Consumer Privacy Act (“CCPA”).

“Customer” means the entity or company that is the authorized purchaser or User of the Litmos Cloud Services (including Customer’s employees, consultants, contractors, agents and third parties who are authorized by Customer to access and use the Cloud Services subject to the rights granted to Customer pursuant to the Agreement).

“Customer Data” means all electronic data and information submitted by or on behalf of the Customer to the Cloud Services, including any content, materials, data and information that Users enter into the production system of a Cloud Service or that Customer derives from its use of and stores in the Cloud Services (e.g., Customer-specific reports).

“Customer Personal Data” means Personal Data received from or on behalf of Customer, or otherwise obtained in connection with the performance of Litmos’s Services and/or obligations under the Agreement, including Personal Data processed by Litmos, as more particularly specified, listed and checked (for applicability) in **Schedule 1**. Customer Personal Data excludes non-production data over which Litmos is the controller (i.e., data received for account management, billing, and marketing purposes).

“Data Protection Laws” means all applicable laws and rules, policies, guidance or recommendations issued by any governmental, statutory

or regulatory body and any industry code of conduct or guideline, in each case relating to data protection, the processing of personal data and privacy and in force from time to time, including but not limited to the EU General Data Protection Regulation 2016/679 ("EU GDPR"), the retained EU law version of EU Regulation 2016/679 as enacted into UK law ("UK GDPR") and the Data Protection Act 2018 (together the "UK Data Protection Laws"), the *Privacy Act 1988* (Cth) and the Australian Privacy Principles set out in the *Privacy Act 1988* (Cth) ("Australian Law"), and US Data Privacy Laws (defined below).

"Data Subject"	or any similar term as used and defined under applicable Data Protection Laws, including "consumer" as defined under the CCPA, has the meaning set forth in the applicable Data Protection Laws.
"Data Protection Supervisory Authority"	means any regulatory authority responsible for the enforcement, regulation or governance of any Data Protection Laws and any replacement or successor body or person for any such authority from time to time.
"Personal Data"	or any similar term as used and defined under applicable Data Protection Laws, including "Personal Information" as defined under the CCPA, and includes information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household
"Personal Data Breach"	means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Customer Personal Data transmitted, stored or otherwise processed.
"Processing" or "processing" or "process"	means any operation or set of operations which is performed upon Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction, and has the meaning given in applicable Data Protection Laws from time to time (and related expressions, including Process, Processed and Processes shall be construed accordingly).
"Processor"	means the natural or legal person, public authority, agency or other body which processes Personal Data on behalf of the Controller, and includes the term "Service Provider" as defined by the CCPA.
"Restricted Transfer"	means a transfer of Personal Data which is undergoing processing or which is intended to be processed after transfer to a country or territory to which such transfer is prohibited or subject to a requirement to take additional steps to adequately protect the Personal Data for the transfer to be lawful under the Data Protection Laws.
"Security Measures"	means the minimum technical and organizational security measures for Litmos Services as set out in Schedule 2 to this DPA.

“Sensitive Data”	means any data of a highly sensitive nature that is regulated under Data Protection Laws, which may include, “sensitive personal information” as defined by the CCPA, the “special categories” of personal data under EU GDPR and UK Data Protection Laws and “sensitive information” as defined under the Australian Law.
“Services”	means Services as defined and/or ordered under the Agreement and as further specified, where applicable, in Schedule 1 of this DPA.
“Standard Contractual Clauses”	means the contractual clauses approved by the EU Commission or a Supervisory Authority or other body authorised to do so pursuant to Data Protection Laws, which provide for transfer of Personal Data from the jurisdiction from which the Personal Data originates to another jurisdiction where such transfer would otherwise be a Restricted Transfer, including the specific references to standard contractual clauses in section 10 of this DPA.
“Sub-Processor” or “sub-processor”	means Litmos Affiliates and third parties appointed, engaged or permitted by Litmos, who process Personal Data in connection with the Agreement and in accordance with this DPA (incorporated into this DPA as set out at https://www.litmos.com/termsandconditions).
“Technical and Organizational Security Measures”	means the technical and organizational security measures for the relevant Litmos Services (incorporated into this DPA as set out at https://www.litmos.com/termsandconditions).
“US Data Privacy Laws”	means any and all applicable U.S. privacy law or U.S. state privacy statutes and regulations relating to the protection of Personal Data, whether in existence as of the effective date or promulgated thereafter, as amended or superseded, including without limitation the California Consumer Privacy Act of 2018, Cal. Civ. Code §§ 1798.100 et seq., as amended by the California Privacy Rights Act of 2020, and all regulations issued thereunder (“CCPA”); the Virginia Consumer Data Protection Act of 2021, Va. Code Ann. §§ 59.1-571 et seq. (“VCDPA”), as effective January 1, 2023; the Colorado Privacy Act of 2021, Colo. Rev. Stat. §§ 6-1-1301 et seq. (“CPA”), as will be operative beginning July 1, 2023; the Connecticut Act Concerning Personal Data Privacy and Online Monitoring, Conn. Gen. Stat. §§ 42-515 et seq. (“CTDPA”), as will be operative beginning July 1, 2023; the Utah Consumer Privacy Act of 2021, Utah Code Ann. §§ 13-61-101 et seq. (“UCPA”), as will be operative beginning December 31, 2023; the Texas Data Privacy and Security Act, Tex. Bus. & Com. Code §§ 541 et seq. (“TDPSA”), as will be operative beginning July 1, 2024; the Florida Digital Bill of Rights, Fla. Stat. §§ 501.701 et seq. (“FDBR”), as will be operative beginning July 1, 2024; the Montana Consumer Data Privacy Act, 2023 SB 384 (“MCDPA”), as will be operative beginning October 1, 2024; the Iowa Consumer Data Protection Act, Iowa Code §§ 715D et seq. (“ICDPA”), as will be operative beginning January 1, 2025; the Tennessee Information Protection Act, Tennessee Code Ann. §§ 47-18-3201 et seq. (“TIPA”), as will be operative beginning July 1, 2025; and the Indiana Consumer Data Privacy Act, Indiana Code §§ 24-15 et seq. (“INCDPA”), as will be operative beginning January 1, 2026.

- 1.2 In this DPA (except where the context otherwise requires):
- 1.2.1 the Schedules form part of this DPA and will have the same force and effect as if expressly set out in the body of this DPA and any reference to this DPA will include a reference to the Schedules;
 - 1.2.2 references to any statute or statutory provision will include any subordinate legislation made under it and will be construed as references to such statute, statutory provision and/or subordinate legislation as modified, amended, extended, consolidated, re-enacted and/or replaced and in force from time to time; and
 - 1.2.3 any words following the words "include", "includes", "including", "in particular" or any similar words or expressions will be construed without limitation and accordingly will not limit the meaning of the words preceding them.

2. PROCESSING OF PERSONAL DATA

- 2.1 The Parties acknowledge and agree that the processing of Customer Personal Data pursuant to the Agreement shall be governed by the terms of this DPA and the Parties shall comply with the Data Protection Laws in connection with the processing of Customer Personal Data pursuant to this DPA. For the avoidance of doubt, Litmos is the Processor (and Service Provider as defined by the CCPA) and Customer is the Controller (and Business as defined by the CCPA); but this DPA does not apply to non-production data over which Litmos is the controller (i.e., data received for account management, billing, and marketing purposes).
- 2.2 The categories of Data Subjects and types of Customer Personal Data anticipated to be processed by Litmos in connection with the performance of Services are set forth in the attached **Schedule 1**. Each Party acknowledges and agrees that any Personal Data Customer discloses to Litmos in connection with the Agreement and this DPA is disclosed for limited business purposes and in accordance with the documented instructions for processing in connection with the performance of Services pursuant to the Agreement and as set forth in the attached **Schedule 1**. Further, the Parties acknowledge and agree to hold in strict confidence Personal Data received or obtained in connection with performing the Services under the Agreement, agree not to disclose such Personal Data, in any form or medium, to any affiliated or non-affiliated person, firm or corporation except as necessary to perform Services under the Agreement, as permitted pursuant to an express exemption or exclusion provided under Data Protection Laws or as may be required by law.
- 2.3 In the event of any conflict between the terms of this DPA and the Agreement, this DPA shall prevail.
- 2.4 The Customer authorises Litmos to process Customer Personal Data during the term of the Agreement as a Processor for the purpose set out in **Schedule 1**.
- 2.5 The Customer warrants to Litmos that:
- 2.5.1 it is compliant with Data Protection Laws and has all necessary rights to authorise Litmos to process Customer Personal Data in accordance with this DPA and the Data Protection Laws; and
 - 2.5.2 its instructions to Litmos relating to processing of Customer Personal Data will not put Litmos in breach of Data Protection Laws.
- 2.6 If Litmos reasonably considers that any instructions from the Customer relating to processing of Customer Personal Data may put Litmos in breach of Data Protection Laws, upon providing Customer notice, Litmos will be entitled not to carry out that processing and will not be in breach of the Agreement, this DPA, or otherwise be liable to the Customer as a result of its failure to carry out that processing.
- 2.7 Litmos:
- 2.7.1 will process Customer Personal Data only on documented instructions from the Customer and will not retain, use, or disclose Customer Personal Data for any purpose other than for the specific purpose of performing the services specified (unless Litmos

or the relevant Sub-Processor is required to process Customer Personal Data to comply with the laws to which Litmos is subject, in which case Litmos will notify the Customer of such legal requirement prior to such processing unless such law prohibits notice to the Customer on public interest grounds). The Parties agree that the Agreement constitutes the documented instruction. For the purpose of this **clause 2.7.1**, the obligations on Litmos to perform the Services are documented instructions;

- 2.7.2 will not sell (as defined by the CCPA) any Customer Personal Data received or obtained in connection with performing the Services as set out in this DPA or share such Customer Personal Data for cross-contextual behavioural advertising;
 - 2.7.3 will not collect, access, use, disclose, process, or retain Customer Personal Data for any purpose other than the specific purpose of performing the Services as set out in the Agreement and this DPA, or another business purpose permitted by applicable law;
 - 2.7.4 will not further collect, access, use, disclose, process, or retain Customer Personal Data for use outside of the direct business relationship between Customer and Litmos;
 - 2.7.5 will not combine Customer Personal Data received or obtained in connection with the Agreement and this DPA with Personal Data it receives from or on behalf of another person or persons, or that it collects from its own interactions, except as otherwise permitted by Data Protection Laws; and
 - 2.7.6 without prejudice to **clause 2.6**, will immediately inform the Customer in writing or via e-mail if, in its reasonable opinion, any instruction received from the Customer infringes any Data Protection Laws.
- 2.8 Litmos certifies that it understands and will comply with all restrictions in **section 2**, and that it will immediately, no later than within five (5) business days, inform Customer if it can no longer comply with obligations under Data Protection Laws, including any applicable obligations under the CCPA, with respect to processing Customer Personal Data. Upon receiving such notice, Customer may take commercially reasonable and appropriate steps to stop and remediate any unauthorized use of such Customer Personal Data.

3. Sub-Processors

- 3.1 Notwithstanding any provision in the Agreement to the contrary, the Customer authorises Litmos to engage Sub-Processors, including those listed at <https://www.litmos.com/termsandconditions>, which Litmos reserves the right to modify at any time.
- 3.2 If Litmos appoints a Sub-Processor, Litmos will
 - 3.2.1 put a written contract in place between Litmos and the Sub-Processor that specifies the Sub-Processor's processing activities and imposes on the Sub-Processor no less protective terms to those imposed on Litmos in this DPA, to the extent applicable to the nature of the Services provided by such Sub-Processor. Litmos will remain liable to the Customer for performance of the Sub-Processor's obligations;

4. Litmos Personnel

- 4.1 Litmos will ensure that any individual authorised to undertake processing of Customer Personal Data:
 - 4.1.1 is subject to confidentiality obligations or is under an appropriate statutory obligation of confidentiality; and
 - 4.1.2 complies with **section 2.7.1** of this DPA.

5. Deletion of Return of Personal Data

- 5.1 At the Customer's request, Litmos will hand over to another data processor, delete or return to the Customer all Customer Personal Data after the end of the provision of Services relating to

processing, and delete any remaining copies. Litmos will be entitled to retain any Customer Personal Data required to comply with any applicable law.

6. Technical and Organisational Security Measures

6.1 Litmos will implement the Technical and Organizational Security Measures in relation to the processing of Customer Personal Data as set out at <https://www.litmos.com/termsandconditions> and ensure:

6.1.1 such that the processing will meet the requirements of Data Protection Laws and ensure the protection of the rights of Data Subjects;

6.1.2 such that Litmos will provide the same level of privacy protection to any Customer Personal Data as provided, and required, under Data Protection Laws, including the CCPA, to the extent applicable. Customer may take commercially reasonable and appropriate steps to ensure that Litmos uses Customer Personal Data in a manner consistent with this DPA and Customer's obligations under the CCPA; and

6.1.3 so as to ensure a level of security in respect of Customer Personal Data processed by it that is appropriate to the risks that are presented by the processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Customer Personal Data transmitted, stored or otherwise processed.

7. Personal Data Breach

7.1 Litmos will notify the Customer without undue delay after becoming aware of a Personal Data Breach, providing Customer with the available information to allow Customer to assess and meet any obligations to report the Personal Data Breach under the Data Protection Laws.

7.2 Litmos will cooperate with Customer (at the Customer's cost) and take such reasonable commercial steps as are necessary to assist in the investigation, mitigation, and remediation of such Personal Data Breach impacting Customer Data.

7.3 Where and in so far as it is not possible to provide sufficient information referred to in **clause 7.1** at the same time, the information may be provided in phases without undue further delay. Litmos's obligation to report or respond to a Personal Data Breach under this **section 7** is not and will not be construed as an acknowledgment by Litmos of any fault or liability of Litmos with respect to a Personal Data Breach.

8. Data Subject Rights, Audit and Inspection Rights

8.1 Litmos will provide reasonable assistance to the Customer (at the Customer's cost) in:

8.1.1 complying with its obligations under the Data Protection Laws relating to the security of processing Customer Personal Data, including compliance with Article 32 and Article 36 of the EU and UK GDPR;

8.1.2 responding to requests for exercising Data Subjects' rights under the Data Protection Laws, including by appropriate technical and organisational measures, insofar as this is possible; and

8.1.3 conducting privacy impact assessments of any processing operations and consulting with Data Protection Supervisory Authorities, Data Subjects and their representatives accordingly.

8.2 Litmos will allow for and contribute to audits, including inspections, conducted by the Customer or another auditor mandated by the Customer, provided that the Customer gives Litmos at least 30 business days prior written notice of each such audit and that each audit is carried out at the Customer's cost, during regular business hours, so as to cause the minimum disruption to Litmos' business and without the Customer or its auditor having any access to any data belonging to a person other than the Customer. Any materials disclosed during such audits and the results of and/or outputs from such audits will be kept confidential by the Customer and the provisions of Section 8 (Confidentiality) of the Agreement will apply to them.

9. International Processing/Restricted Transfers

- 9.1 Litmos may make an international transfer of Personal Data which is undergoing processing or which is intended to be processed after transfer to a country in accordance with this DPA outside the country in which the Customer is located or as permitted under Data Protection Laws, or where there is otherwise no prevailing Data Protection Laws which restrict a transfer to that country.
- 9.2 Litmos may make a Restricted Transfer if it demonstrates or implements an appropriate safeguard for that Restricted Transfer which enables that transfer to occur (and not be prohibited) in accordance with Data Protection Laws. Such appropriate safeguards may include:
- 9.2.1 an appropriate safeguard as directed by the Customer, as determined by the Customer in accordance with Data Protection Laws;
 - 9.2.2 consent of the Data Subject, as appropriate; or
 - 9.2.3 the execution of an agreement for the transfer of Personal Data, in accordance with the provisions of the Data Protection Laws.
- 9.3 The qualifications to making a Restricted Transfer at **clause 9.2** will not apply if:
- 9.3.1 the Customer's instructions pursuant to **clause 2.7.1** require Litmos to make a Restricted Transfer and Litmos requires the Customer to demonstrate that an appropriate safeguard in accordance with Data Protection Laws has been put in place prior to such Restricted Transfer; or
 - 9.3.2 Litmos or the relevant Sub-Processor is required to make a Restricted Transfer to comply with laws to which Litmos is subject, in which case Litmos will notify the Customer of such legal requirement prior to such Restricted Transfer unless such law prohibits notice to the Customer on public interest grounds.

10. Standard Contractual Clauses

- 10.1 To the extent contractual terms are required to lawfully make a Restricted Transfer, Customer (as "data exporter") and Litmos (its Affiliates or authorised Sub-Processors), as appropriate, (as "data importer") hereby:
- 10.1.1 enter into the Standard Contractual Clauses for Personal Data covered by the EU GDPR or UK GDPR (or other Data Protection Laws that so require it) and agree that the Standard Contractual Clauses apply in respect of any Restricted Transfer; or
 - 10.1.2 agree that any such Personal Data will be processed by Litmos in accordance with, and as though Litmos is bound by, the Australian Privacy Principles (other than Australian Privacy Principle 1) set out in the *Privacy Act 1988 (Cth)*.
- 10.2 In respect of any Restricted Transfers from the European Economic Area, the Parties agree to the following:
- 10.2.1 The "EU Standard Contractual Clauses" shall mean the standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679, as set out in the European Commission's Implementing Decision 2021/914 of 4 June 2021, as may be amended, replaced or superseded by the European Commission from time to time.
 - 10.2.2 The EU Standard Contractual Clauses will be incorporated into this DPA by reference and shall apply to the extent required under Data Protection Laws.
 - 10.2.3 The specific modules and Annexes of the EU Standard Contractual Clauses, which are so incorporated, are set out in **Schedule 3** of this DPA.
 - 10.2.4 The Parties agree that execution of this DPA or the agreement into which it is incorporated constitutes signature and acceptance and incorporation of the EU Standard Contractual Clauses.

- 10.3 In respect of any Restricted Transfers from the United Kingdom, the Parties agree to the following:
- 10.3.1 The Standard Contractual Clauses shall mean the UK Addendum where "UK Addendum" means the International Data Transfer Addendum to EU Transfer Contract Clauses in force 21st March 2022, as may be amended, replaced or superseded by the ICO from time to time (including when formally issued by the ICO under section 119A(1) of the UK Data Protection Act 2018).
 - 10.3.2 The UK Addendum will be incorporated into this DPA by reference and shall apply to the extent required under Data Protection Laws.
 - 10.3.3 Tables 1 to 4 (inclusive) to the UK Addendum shall be deemed completed with the information as set out in **Schedule 3** of this DPA.
 - 10.3.4 The Parties agree that execution of this DPA or the agreement into which it is incorporated constitutes signature and acceptance and incorporation of the UK Addendum.
- 10.4 **Section 9.1** shall not apply to a Restricted Transfer unless its effect, together with other reasonably practicable compliance steps, is to allow the relevant Restricted Transfer to take place without breach of applicable Data Protection Law.

11. ENTIRE AGREEMENT

- 11.1 This DPA, together with the Agreement, constitutes the entire agreement between the Parties as it relates to the processing of Customer Personal Data and supersedes any previous agreements, arrangements, undertakings or proposals, written or oral, between the Parties in relation to its subject matter.
- 11.2 The Parties agree that this DPA may be amended from time to time. The Parties agree to renegotiate in good faith any necessary amendments to this DPA in order to reflect changes in the law so as to remain consistent with the relevant Data Protection Laws, as well as to provide for new purposes for, and categories of, processing Customer Personal Data. For the avoidance of doubt, Litmos may revise **Schedule 1** to reflect the addition or removal of service options.

12. SEVERANCE

- 12.1 If any provision (or part of a provision) of this DPA is found by any court or administrative body of competent jurisdiction to be invalid, unenforceable or illegal, the other provisions will remain in force.
- 12.2 If any invalid, unenforceable or illegal provision would be valid, enforceable or legal if some part of it were deleted, the provision will apply with whatever modification is necessary to give effect to the commercial intention of the Parties.

13. GOVERNING LAW AND JURISDICTION

- 13.1 Without prejudice to clauses 17 (Governing law) and 18 (Choice of forum and jurisdiction) of the Standard Contractual Clauses,
- 13.1.1 this DPA and any non-contractual obligations arising out of or in connection with it are governed by the laws of the Agreement.
 - 13.1.2 the courts agreed in the Agreement shall have exclusive jurisdiction to determine any dispute arising out of or in connection with this DPA (including in relation to any non-contractual obligations).

SCHEDULE 1

Personal Data Processing Purposes & Details

Business Purposes for which Personal Data may be processed:

The Personal Data processed and/or transferred will be subject to the following basic processing activities, which may be supported remotely, as further detailed and specified in the Agreement:

- to host internal and external training programs for customers and end users;
- to record and monitor compliance training;
- to provide content related to training activities;
- to provide professional services related to training programs; and
- to support any issues raised related to the performance of the training programs, platform and training content.

Nature of Processing Activities:

- use of Personal Data to set up, operate, monitor and provide the Service (including operational and technical support);
- continuous improvement of service features and functionalities provided as part of the Service including automation, transaction processing and machine learning;
- provision of embedded Professional Services;
- communication to Authorized Users;
- storage of Personal Data in dedicated data centers (multi-tenant architecture);
- release, development and upload of any fixes or upgrades to the Service;
- back up and restoration of Personal Data stored in the Service;
- computer processing of Personal Data, including data transmission, data retrieval, data access;
- network access to allow Personal Data transfer;
- monitoring, troubleshooting and administering the underlying Service infrastructure and database;
- security monitoring, network-based intrusion detection support, penetration testing; and
- execution of instructions of Customer in accordance with the Agreement.

Duration of Processing Activities:

- Full term of the agreement.

Instructions for Processing:

- As instructed in the Agreement and this Addendum or as otherwise indicated in writing by Company.

Categories of Personal Data:

The Personal Data processed and/or transferred concerns the following categories of data:

Category	Examples (examples may be present in more than one category)	Processed under this Agreement	Business Purpose for Processing
A. Identifiers	A real name, alias, postal address, unique personal identifier, online identifier, Internet Protocol address, email address, account name, Social Security number, driver's license number, passport number, or other similar identifiers	Yes	Name and email address to record and monitor compliance training and store results.
B. Personal Data	Information that identifies, relates to, describes, or is capable of being associated with, a particular individual, including, but not limited to, a name, signature, Social Security number, physical characteristics or description, address, telephone number, passport number, driver's license or state identification card number, insurance policy number, education, employment, employment history, bank account number, credit card number, debit card number, or any other financial information, medical information, or health insurance information.	Yes	Name and email address to record and monitor compliance training and store results.

	Some personal data included in this category may overlap with other categories		
C. Protected classification characteristics	Familial status, disability, sex, national origin, religion, color, race, sexual orientation, gender identity and gender expression, marital status, veteran status, medical condition, ancestry, source of income, age, or genetic information	No	
D. Commercial information	Records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies	No	
E. Biometric information	Genetic, physiological, behavioral, and biological characteristics or activity patterns used to extract a template or other identifier or identifying information, such as fingerprints, faceprints, voiceprints, iris or retina scans, keystroke, gait, or other physical patterns, and sleep, health, or exercise data	No	
F. Internet or other similar network activity	Browsing history, search history, information on a Consumer's interaction with a website, application, or advertisement	Yes	IP addresses to record and monitor compliance training, support and store results.
G. Geolocation data	Physical location or movements	Yes	General location information to record and monitor compliance training and store results, as well as restrict embargoed locations.
H. Sensory data	Audio, electronic, visual, thermal, olfactory, or similar information	No	
I. Professional or employment-related information	Current or past job history or performance evaluations	No	
J. Non-public education information	Education records directly related to a student maintained by an educational institution or party acting on its behalf, such as grades, transcripts, class lists, student schedules, student identification codes, student financial information, or student disciplinary records	No	
K. Inferences drawn from other personal data	Profile reflecting a person's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes	No	

L. Categories of Consumers (include current, past or prospective)	<ul style="list-style-type: none"> • Employees, workers and staff members; • Customers of the data exporter, including representatives, employees or agents of the customers; • Suppliers of the data exporter, including representatives, employees or agents of the suppliers; and • End users as identified by customers to receive a training program. 	Yes	For employees, workers and staff members, as well as their customers and suppliers, to record and monitor compliance training and store results.
M. Subcontractors	<i>If YES, see approved subcontractor list at https://www.litmos.com/termsandconditions.</i>	Yes	
N. Sensitive Identification Numbers	Social security, driver's license, state identification card, or passport number	No	
O. Sensitive Account Information	Account log-in, financial account, debit card, or credit card number in combination with any required security or access code, password, or credentials allowing access to an account	No	
P. Sensitive Location Information	Precise geolocation as defined by Data Protection Laws and Regulations	No	
Q. Sensitive Demographic Information	Racial or ethnic origin, religious, political or philosophical beliefs, criminal background or union membership	No	
R. Communication Contents	Mail, email, and text messages contents (except where we are the intended recipient of the communication)	No	
S. Genetic Data	Genetic tests, genetic predisposition to disease, descriptions of genetic makeup or other genetic data	No	
T. Identifying Biometric Data	Biometric data, such as fingerprints, iris scans, face geometry scans, or voice patterns, processed for the purposes of uniquely identifying a Consumer	No	
U. Health Data	Personal data collected and analyzed concerning a Consumer's health or treatment of their health	No	
V. Sex Life or Orientation	Personal data collected and analyzed concerning a Consumer's sex life or sexual orientation	No	
O. Sensitive Account Information	Account log-in, financial account, debit card, or credit card number in combination with any required security or access code, password, or credentials allowing access to an account	No	

SCHEDULE 2

Technical and Organizational Security Measures

This Schedule 2 applies to describe the applicable Technical and Organizational Security Measures for the purposes of the New Standard Contractual Clauses and applicable Data Protection Laws.

Litmos will apply and maintain the Technical and Organizational Security Measures as set forth at www.litmos.com/termsandconditions.

To the extent that the provisioning of the Service comprises Relevant Transfers to which Standard Contractual Clauses under Clause 10 apply, the Technical and Organizational Security Measures describe the measures and safeguards which have been taken to fully take into consideration the nature of the personal data and the risks involved. If local laws affect compliance with the clauses, this may trigger the application of additional safeguards applied during transmission and to the processing of the personal data in the country of destination (if applicable: encryption of data in transit, encryption of data at rest, anonymization, pseudonymization).

It is agreed that all Security Measures shall be reviewed from time to time to take into account any improvements in technology, as well as to ensure that the Security Measures are still adequate and appropriate given any changes to or on processing of the Agreement.

SCHEDULE 3

Standard Contractual Clauses Module Two and Annexes

This Schedule forms an integral part of the DPA. Capitalized terms not otherwise defined herein shall have the meaning given to them in the DPA.

In accordance with Section 4 of the DPA, the Parties to the DPA agree that the EU Standard Contractual Clauses and UK Addendum are incorporated into the DPA where applicable and shall apply as follows:

1. Module Two – Transfer Controller to Processor

Provision of the EU Standard Contractual Clauses	European Economic Area Restricted Transfers	United Kingdom Restricted Transfers
7 Docking clause	The data exporter and data importer agree that the optional docking clause applies.	The data exporter and data importer agree that the optional docking clause applies.
9 Use of sub-processors	<p>The data exporter and data importer agree that Option 2 GENERAL WRITTEN AUTHORISATION shall apply to the data importer’s processing of personal data, in accordance with the list of sub-processors set out in Schedule 1 of this DPA.</p> <p>The list of agreed sub-processors shall apply for the duration of the Services provision by the data importer, which may be updated in accordance with the written procedure agreed between the data exporter and data importer, and Clause 9 (a), Option 2, of EU Standard Contractual Clauses. The parties agree that the time period set forth in Clause 9 (a), Option 2 shall be thirty (30) days.</p>	<p>The data exporter and data importer agree that Option 2 GENERAL WRITTEN AUTHORISATION shall apply to the data importer’s processing of personal data, in accordance with the list of sub-processors set out in Schedule 1 of this DPA.</p> <p>The list of agreed sub-processors shall apply for the duration of the Services provision by the data importer, which may be updated in accordance with the written procedure agreed between the data exporter and data importer, and in accordance with Clause 9 (a), Option 2, of the Standard Contractual Clauses. The parties agree that the time period set forth in Clause 9 (a), Option 2 shall be thirty (30) days.</p>
Clause 11 Redress	The data importer does not agree to submit to an independent dispute resolution body.	The data importer does not agree to submit to an independent dispute resolution body.
Clause 17 Governing law	The Standard Contractual Clauses to which this module relates shall be governed by the laws of the Netherlands.	The Standard Contractual Clauses to which this module relates shall be governed by the laws of England and Wales.
Clause 18 Choice of forum and jurisdiction	The choice of forum and jurisdiction of the Standard Contractual Clauses to which this module relates shall be the courts of the Netherlands.	The choice of forum and jurisdiction of the Standard Contractual Clauses to which this module relates shall be the courts of England and Wales.
<u>Annex I A</u> List of parties	<p>Data Exporter: Customer entity which is party to the Standard Contractual Clauses (controller).</p> <p>Data Importer: Litmos entity which is party to the Standard Contractual Clauses (processor).</p>	<p>Data Exporter: Customer entity which is party to the Standard Contractual Clauses (controller).</p> <p>Data Importer: Litmos entity which is party to the Standard Contractual Clauses (processor).</p>

	Please refer to Schedule 1 of the DPA for additional information on the identity and contact details of the data exporter and data importer and, where applicable, of their data protection officer and/or representative in the European Union.	Please refer to Schedule 1 of the DPA for additional information on the identity and contact details of the data exporter and data importer and, where applicable, of their data protection officer and/or representative in the European Union.
<u>Annex I B</u> Description of Transfer	As set out in Schedule 1 of this DPA. The data exporter expressly instructs the data importer to process the personal data to enable the data importer to provide the Services contracted by the data exporter, including the purposes set out in Schedule 1 of this DPA.	As set out in Schedule 1 of this DPA. The data exporter expressly instructs the data importer to process the personal data to enable the data importer to provide the Services contracted by the data exporter, including the purposes set out in Schedule 1 of this DPA.
<u>Annex I C</u> Competent Supervisory Authority	<p>If the data exporter is established in an EU Member State: the supervisory authority with responsibility for ensuring compliance by the data exporter with GDPR as regards the data transfer will act as competent supervisory authority;</p> <p>If the data exporter is not established in an EU Member State, but falls within the territorial scope of application of GDPR (i.e., Article 3(2) GDPR) and has appointed a representative in the EU (i.e., Article 27(1) GDPR): the supervisory authority of the Member State in which the representative is established will act as competent supervisory authority;</p> <p>If the data exporter is not established in an EU Member State, but falls within the territorial scope of application of GDPR without however having to appoint a representative in the EU: the supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under the Standard Contractual Clauses in relation to the offering of goods or services to them, or whose behavior is monitored, are located, will act as competent supervisory authority.</p>	UK Information Commissioner or such replacement body appointed under the Data Protection Act 2018.
<u>Annex II</u> Technical and Organisational Measures including Technical and Organisational Measures to Ensure the Security of the Data	As set out in Schedule 2 of this DPA.	As set out in Schedule 2 of this DPA.
<u>Annex III</u> List of sub-processors	As set out at https://www.litmos.com/termsandconditions .	As set out at https://www.litmos.com/termsandconditions .

2. United Kingdom Restricted Transfers

In respect of United Kingdom Restricted Transfers only, the EU Standard Contractual Clauses are supplemented and amended by the UK Addendum with the Part 1 Tables to the UK Addendum completed as follows:

1. Table 1 shall be deemed completed with the information included in Section 1 above and information from **Schedule 1** of this DPA;
2. In Table 2, the first option shall be selected and the relevant version of the "Approved EU SCCs", as defined in the UK Addendum, shall be those referred to in the DPA incorporating the amendments to them set out in the table above;
3. Table 3 shall be deemed completed as set out in Section 1 above and the table above;
and
4. Table 4 shall be deemed completed such that the exporter and importer have the right to end the UK Addendum as set out in Section 19 of Part 2 of the UK Addendum.