MathWorks Data Processing Agreement

This Data Processing Agreement ("Agreement") is effective as of the date last written in the signature block immediately below. This Agreement relates to the use of Personal Data provided by the entity listed in the "Data Controller Information Table" below ("Data Controller") to The MathWorks, Inc. ("MathWorks") and its affiliates in connection with the purchase or license of MathWorks products or services (collectively, "MathWorks Products"). As used in this Data Processing Agreement, "Personal Data" refers to data transferred from Data Controller to MathWorks that directly or indirectly identifies a natural person, or otherwise constitutes personal data under Applicable Law; and "Applicable Law" refers to the European Union (EU) General Data Protection Regulation (GDPR), the California Consumer Protection Act (CCPA), or other applicable law, rule, or regulation regarding protection of Personal Data. MathWorks publishes detailed information about its privacy practices in the MathWorks Privacy Policy, available at https://www.mathworks.com/privacy. MathWorks may modify or supplement the terms in this Data Processing Agreement, with consent from Data Controller, to comply with applicable laws, rules, or regulations or if required by a supervisory authority or other governmental or regulatory entity.

Data Controller Information Table	
"*Data Controller*"	
Entity Name:	Mailing Address:
Place of Incorporation (*if incorporated*):	Notice Email Address:

Agreed and Accepted:

MathWorks	**Data Controller**
Signature: Richard Rovner Richard Rovner (Apr 25, 2023 11:14 EDT)	Signature:
Name: Richard Rovner	Name:
Title: Vice President Marketing	Title:
	Date:

Note: If pre-signed by MathWorks, this Data Processing Agreement is legally binding only upon receipt by MathWorks of a fully signed copy, including an email address for notices, by email at privacy@mathworks.com.

1. Types of Data; Data Subjects. The Personal Data to be transferred from Data Controller to MathWorks primarily consists of names and email addresses. The Personal Data may also include contact information such as a mailing address or phone number; organizational information such as a title or role; and payment information such as a credit card number in the case of individuals paying for MathWorks Products on Data Controller's behalf. The data subjects are purchasers, administrators, and end-users of MathWorks Products.

2. Provision and Use of Data. With respect to the Personal Data, Data Controller is the controller and MathWorks is the processor. MathWorks may use the Personal Data for the purposes set forth in Appendix A. Data Controller represents and warrants that it has the full right and authority to transfer the Personal Data to MathWorks and to permit MathWorks' use of the Personal Data hereunder. MathWorks shall only collect and use the Personal Data in accordance with Applicable Law, this Agreement, and any other mutually agreed documented instructions of the Data Controller with respect to the Personal Data.

3. Technical and Organizational Measures. MathWorks shall provide appropriate technical and organizational measures to protect Personal Data against accidental or unlawful destruction; accidental loss or alteration; or unauthorized disclosure or access. A description of MathWorks' technical and organizational measures is set forth in Appendix B. MathWorks shall provide at least the same level of security and privacy protection of the Personal Data as is required by Applicable Law. All persons authorized by MathWorks to access the Personal Data shall be under a commitment or statutory obligation of confidentiality.

4. Data Subject Requests. MathWorks shall provide legally required assistance to Data Controller in responding to individuals exercising their data subject rights under Applicable Law. MathWorks shall notify Data Controller if MathWorks receives a data subject request from personnel of Data Controller. Data Controller agrees that it will respond in writing to MathWorks within seven (7) days after the date of MathWorks' notification with any instructions regarding MathWorks' response to such data subject request. Data Controller further agrees that if MathWorks does not receive such response within such period, or if Data Controller fails to specify an email address to receive MathWorks' notifications, Data Controller will be deemed to have authorized MathWorks to respond to the data subject request directly.

5. Recordkeeping. MathWorks shall maintain written records of its processing activities sufficient to demonstrate compliance with this Agreement and Applicable Law. MathWorks shall make these records available to Data Controller on request, and shall make these records available to auditors or government entities at Data Controller's request or as required to comply with law or a court or government order.

6. Subprocessors. Data Controller authorizes the transfer of Personal Data by MathWorks to third parties ("Subprocessors") for the limited purposes described in this Agreement. All such transfers shall be subject to a written contract providing that: (i) the Subprocessor must meet all of the obligations relating to data privacy and security under this Agreement, including without limitation the obligation to provide at least the same level of security and privacy protection of the Personal Data as is required of MathWorks; (ii) the Subprocessor may only process the Personal Data according to MathWorks' instructions, which must be consistent with Data Controller's instructions to MathWorks; and (iii) MathWorks shall remain fully liable for meeting its obligations hereunder relating to the Personal Data to the same extent that MathWorks would be liable for performing the services of each Subprocessor directly. A list of Subprocessors as of the effective date of this Agreement is set forth in Appendix C. MathWorks will notify Data Controller of changes at least thirty (30) days in advance. Data Controller may object within thirty (30) days by notifying MathWorks in writing about its objection, in which case MathWorks will make a good faith effort to address Data Controller's objection.

7. Audit. MathWorks shall make available to Data Controller all information necessary to demonstrate compliance with the obligations laid down in Applicable Law and this Agreement, and shall allow for and contribute to audits, including inspections, conducted by Data Controller or another auditor mandated by Data Controller.

8. Breach Notification; Failure to Meet Obligations. If MathWorks becomes aware of a breach of Personal Data or determines that it can no longer meet its obligations hereunder, MathWorks shall notify Data Controller without undue delay. MathWorks shall cooperate with Data Controller and provide reasonable assistance as requested by Data Controller in accordance with GDPR Articles 32 to 36 or other Applicable Law.

9. Deletion of Personal Data. After the end of the provision of services relating to processing of Personal Data, including termination of licenses to MathWorks Products, at the choice of Data Controller, MathWorks shall delete or return the Personal Data to the Data Controller, and shall delete existing copies of Personal Data provided by Data Controller unless storage is required by law.

10. Notice. MathWorks shall email any notices required under this Agreement to the email address specified in the Data Controller Information Table above. If no email address is provided, or Data Controller wishes to change the email address for notices, Data Controller must provide a signed writing to MathWorks containing the updated email address and stating that it is for receipt of notices under this Agreement.

11. Compliance with Law; Transfer Mechanism. MathWorks shall comply with Applicable Law in processing Personal Data. Standard contractual clauses mandated by government entities for cross-border transfers of the Personal Data ("Standard Clauses") and supplemental information (e.g., additional descriptions of technical and organizational measures), available in the MathWorks Trust Center at https://www.mathworks.com/company/aboutus/policies_statements/trust-center.html, apply to any such transfers under this Agreement and are incorporated by reference. Where required by law, the terms of Standard Clauses supersede the terms of this Agreement in the event of a conflict. For transfers of Personal Data of European Union and United Kingdom individuals, the EU Addendum (incorporating the EU Standard Contractual Clauses) and UK Addendum attached hereto as Appendix D shall apply to the extent required by law.

[Appendices follow]

Appendix A

Permitted Purposes

MathWorks may use Personal Data transferred to it by Data Controller for the following purposes:

- To provide products, services, and support requested by Data Controller or on its behalf.
- To process and ship orders that Data Controller places or that are placed on its behalf, and to provide Data Controller with documentation or other material in support of such orders.
- To authenticate and secure Data Controller or its users' accounts or use of MathWorks products and services.
- To manage licenses and ascertain use of MathWorks products and services.
- To administer and improve MathWorks products and services, including websites.
- To enable delivery of consulting or training services and participation in seminars, trade shows, and other events.
- To provide any communication or material necessary to respond to an order for a product or service, a request for support or information, or an application for a seminar, trade show, or other event.
- To solicit optional feedback in the form of surveys measuring customer satisfaction with MathWorks products, services, and events.
- To notify Data Controller of new products, updates, or other information related to purchases or Data Controller's information requests.
- To provide important information regarding the renewal of agreements, version upgrades, and other notifications about products and services that Data Controller licenses or uses.
- To send materials and communications about MathWorks and its products, services, and events and, in some cases, on behalf of related third-party products, services, and events. Individuals may opt out of receiving these materials and communications.
- To allow Data Controller and its users to integrate MathWorks products and services with third party services at Data Controller's or its users' request.
- To enforce MathWorks' agreements or comply with obligations imposed by applicable laws, regulations, or a court or administrative order. MathWorks may be required to disclose an individual's personal information in response to a lawful request by public authorities, including to meet national security or law enforcement requirements.

Appendix B

Technical and Organizational Measures

The information security program at MathWorks draws from several industry-standard frameworks, including ISO 27001 and the NIST Cybersecurity Framework. It is the policy of MathWorks to protect customer, employee, partner, and corporate information from unauthorized access. MathWorks has full-time information and product security departments that regularly report to executive management. MathWorks uses risk management techniques to align security activities with relevant risks to our business and data. Security responsibilities get broad communication within the organization. MathWorks maintains an internal quality assurance function to assess the performance of internal controls and regularly reports results to executive management.

Security Policies

MathWorks maintains policies to support our information security program. These policies address acceptable use of technology, data storage, access control, incident response, employee training, as well as privacy and protection of personally identifiable information. Executive management reviews and approves policies on a regular basis.

Organization of Information Security

MathWorks has full-time departments for information and product security. Responsibilities are assigned by executive management. Security teams report on objectives and performance of the program. To reduce opportunities for unauthorized access to assets, teams take care to segregate their duties.

Human Resources Security

MathWorks conducts background verification checks on candidates for employment. All MathWorks employees are required to acknowledge a confidentiality agreement upon hire. Management communicates security responsibilities to employees and contractors. MathWorks maintains an information security awareness and training program. Training is given as part of new hire orientation and on a regular basis thereafter. Specialized information security training is provided based on job functions.

Asset Management

MathWorks maintains asset inventories to support information security objectives. Acceptable use of assets is defined in policies that are communicated to employees. MathWorks reclaims corporate assets upon termination of employment. MathWorks defines criteria for classifying information assets based on criticality and sensitivity to unauthorized access. Standards support asset classification by enumerating information security requirements. MathWorks uses asset disposal vendors to securely dispose of assets upon retirement.

Access Control

MathWorks implements access control policies and procedures to follow the principles of least privilege and need-to-know. Access to MathWorks managed information requires a username and password. Remote access to the MathWorks private network requires multifactor authentication. Password composition requirements observe industry best practices. Procedures document the process for provisioning and deprovisioning user access. Allocation and use of privileged access rights use restrictions. MathWorks has policies, procedures, and technology to support the management of secrets, including passwords, API keys, and digital certificates.

Cryptography

MathWorks maintains cryptographic standards to protect information, encrypting information both at-rest and in-transit. MathWorks maintains a secure file transfer portal for communicating with external parties based on use case.

Physical and Environmental Security

Access to MathWorks offices and information processing facilities is restricted. Sensitive areas like data centers and telecommunications rooms are further restricted to authorized personnel based on job requirements. MathWorks headquarters has 24x7 guard presence and security alarm monitoring. MathWorks managed data centers have standard environmental protections against fire, water, power loss, and other environmental hazards.

Operations Security

MathWorks maintains documented operating procedures to support information security objectives. Procedures define processes for configuring operating systems and network equipment, maintenance, change management, malware protection and removal, and incident response. Development and test environments are segregated from production. MathWorks has a comprehensive log monitoring process that collects logs centrally checks them for anomalous behavior. MathWorks maintains a vulnerability assessment and remediation program.

Communications Security

MathWorks implements security controls on network perimeters, including on-premises and cloud infrastructure. Network segmentation controls limit access to required endpoints and protocols. MathWorks wireless networks use enterprise security controls to encrypt communications and limit access to authorized users only.

Systems Acquisition, Development, and Maintenance

MathWorks follows security procedures to acquire, develop, and maintain information systems. Our secure software development standards draw from several best practices, including OWASP, Microsoft Secure Development Lifecycle, the BSA Framework for Secure Software, and the NIST Secure Software Development Framework (SSDF). Our processes include developer training, application security best practices, secure coding standards, security testing, and application security vulnerability assessments.

Supplier Relationships

MathWorks suppliers are contractually obligated to comply with laws and implement required security and privacy safeguards. Before granting access to data or systems, MathWorks conducts a security evaluation of all suppliers.

Information Security Incident Management

MathWorks maintains a program for managing information security incidents. This program includes documented roles and responsibilities, response procedures, reporting requirements, and a root cause analysis process. MathWorks conducts tabletop exercises to practice its response to information security incidents on a regular basis.

Business Continuity Management

MathWorks is organized around critical business practices for development, support, sales, and other corporate activities. As a global organization, MathWorks executes these activities from multiple locations. In the event of a regional disaster or significant system outage, it is our practice to manage critical functions from an alternate location. System availability and recoverability are core design

principles of our information systems architecture. Critical information systems are designed to minimize the risk of downtime and, if needed, recover required functionality to manage key business operations.

Compliance

MathWorks complies with legal, statutory, and regulatory obligations related to information security. MathWorks maintains an internal quality assurance function to assess the performance of internal controls and regularly reports results to executive management.

Appendix C

Subprocessor List

The entities below provide products and services to MathWorks such as technical infrastructure, payment processing, and operational support. They receive customer data from MathWorks as required to provide these products and services.

In addition to the entities listed below, MathWorks may also engage vendors on a time-limited basis to support MathWorks business activities. These vendors may provide consulting or support services, such as technical support for information technology systems. These vendors may also support specific events or engagements for training, consulting, or marketing purposes by, for example, hosting webinars, managing registration lists, and coordinating with event venues. MathWorks affiliates also have access to customer data for MathWorks general business purposes (including marketing, sales, and customer support), subject to an intercompany agreement with The MathWorks, Inc.

To the extent that they receive customer personal data, all affiliates and vendors including the entities listed below are subject to contracts requiring data privacy protections in accordance with the EU General Data Protection Regulation and other applicable laws, referred to below as "contractual terms". As of the date this list is provided, transfers to the subprocessors listed below are also supported by adequacy decisions.

Subprocessor	Country	Purpose	Legal basis for transfer
Oracle America, Inc. 1 Main Street Cambridge, MA 02142	USA	Marketing, analytics, customer management and communications	• Oracle Binding Corporate Rules • Contractual terms
Salesforce.com, Inc. 415 Mission St., 3rd Floor San Francisco, CA 94105	USA	Sales; customer management and support	• Salesforce Binding Corporate Rules • Standard Contractual Clauses for Salesforce affiliates • Contractual terms
Amazon Web Services, Inc. 410 Terry Avenue North Seattle, WA 98109	USA	Host online services	• Standard Contractual Clauses • Contractual terms
Microsoft Corporation One Microsoft Way Redmond, WA 98052	USA	Information technology infrastructure	• Standard Contractual Clauses • Contractual terms
Worldline Sweden AB Textilgatan 31 SE-120 30 Stockholm	Sweden	Payment processing	• EU Member State • Contractual terms
Adobe Systems Incorporated 345 Park Avenue San Jose, CA 95110	USA	Analytics	• Standard Contractual Clauses • Contractual terms

Subprocessor	Country	Purpose	Legal basis for transfer
Data Intensity, LLC 22 Crosby St. #100 Bedford, MA 01730	USA	Host internal system	• Standard Contractual Clauses • Contractual terms
Sykes Global Services Ltd Nether Road, Galashiels Selkirkshire TD1 3HE	UK	Order fulfillment, shipping, event support	• Standard Contractual Clauses • Contractual terms
Mailgun Technologies, Inc. 535 Mission Street San Francisco, CA 94105	USA	Send transactional emails	• Standard Contractual Clauses • Contractual terms
Mimeo.com, Inc. 16 West 22nd St., Floor 10 New York, NY 10010	USA	Provide access to course materials for online or in-person training	• Standard Contractual Clauses • Contractual terms
Qualaroo, Inc. 929 Colorado Ave Santa Monica, CA 90401	USA	Surveys and analytics	• Standard Contractual Clauses • Contractual terms
Cylynt Limited Glandore Business Centre Fitzwilliam Hall Fitzwilliam Place Dublin 02 D02 T292	Ireland	License compliance	• EU Member State • Standard Contractual Clauses • Contractual terms
Highspot, Inc. 2211 Elliott Ave., Suite 400 Seattle, WA 98121	USA	Sales support and content management	• Standard Contractual Clauses • Contractual terms
ReadyTech Corporation 720 Second St., Suite 111 Oakland, CA 94607	USA	Online learning platform	• Standard Contractual Clauses • Contractual terms
Snowflake Inc. 106 East Babcock St., Suite 3A Bozeman, MT 59715	USA	Information technology infrastructure	• Standard Contractual Clauses • Contractual terms
Treasure Data, Inc. 800 W. El Camino Real, Suite 180 Mountain View, CA 94040	USA	Database management	• Standard Contractual Clauses • Contractual terms
Vonage Business, Inc. 101 Crawfords Corner Road, Suite 2416 Holmdel, NJ 07733	USA	Telecommunication systems and infrastructure	• Standard Contractual Clauses • Contractual terms

Appendix D

European Union Standard Contractual Clauses

STANDARD CONTRACTUAL CLAUSES – MODULE TWO

SECTION I

Clause 1

Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)[1] for the transfer of personal data to a third country.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter 'entity/ies') transferring the personal data, as listed in Annex I.A (hereinafter each 'data exporter'), and

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A (hereinafter each 'data importer')

have agreed to these standard contractual clauses (hereinafter: 'Clauses').

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2

Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other

[1] Where the data exporter is a processor subject to Regulation (EU) 2016/679 acting on behalf of a Union institution or body as controller, reliance on these Clauses when engaging another processor (sub-processing) not subject to Regulation (EU) 2016/679 also ensures compliance with Article 29(4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39), to the extent these Clauses and the data protection obligations as set out in the contract or other legal act between the controller and the processor pursuant to Article 29(3) of Regulation (EU) 2018/1725 are aligned. This will in particular be the case where the controller and processor rely on the standard contractual clauses included in Decision 2021/915.

clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3

Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii) Clause 8.1(b), 8.9(a), (c), (d) and (e);

(iii) Clause 9(a), (c), (d) and (e);

(iv) Clause 12(a), (d) and (f);

(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e);

(viii) Clause 18(a) and (b);

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4

Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6

Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Clause 7

Docking clause

(a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.

(b) Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.

(c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

8.1 **Instructions**

(a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 **Purpose limitation**

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I. B, unless on further instructions from the data exporter.

8.3 **Transparency**

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 **Accuracy**

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 **Duration of processing and erasure or return of data**

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 **Security of processing**

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration,

unauthorised disclosure or access to that data (hereinafter 'personal data breach'). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) (d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 **Sensitive data**

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter 'sensitive data'), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 **Onward transfers**

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union[2] (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

[2] The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purpose of these Clauses.

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 **Documentation and compliance**

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

(d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

———————

Clause 9

Use of sub-processors

(a) The data importer shall not sub-contract any of its processing activities performed on behalf of the data exporter under these Clauses to a sub-processor without the data exporter's prior specific written authorisation. The data importer shall submit the request for specific authorisation at least 30 days prior to the engagement of the sub-processor, together with the information necessary to enable the data exporter to decide on the authorisation. The list of sub-processors already authorised by the data exporter can be found in Annex III. The Parties shall keep Annex III up to date.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects.[3] The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to

[3] This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7.

protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10

Data subject rights

(a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

Clause 11

Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

(c) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(d) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

(e) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(f) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(g) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12

Liability

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.

(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13

Supervision

(a) The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14

Local laws and practices affecting compliance with the Clauses

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards[4];

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

---

[4] As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time-frame. This refers in particular to internal records or other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies.

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

Obligations of the data importer in case of access by public authorities

15.1 **Notification**

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 **Review of legality and data minimisation**

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data

requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17

Governing law

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of Germany.

Clause 18

Choice of forum and jurisdiction

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts of Germany at the registered office of the data exporter.

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

European Union Standard Contractual Clauses Selection and Addendum

This European Union Standard Contractual Clauses Selection and Addendum ("EU Addendum") is part of the Data Processing Agreement between MathWorks and Data Controller ("Agreement") to which it is attached. Capitalized terms used but not defined herein have the meanings given to them in the Agreement.

This EU Addendum applies to the European Union Standard Contractual Clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council based on Commission Implementing Decision (EU) 2021/914 of 4 June 2021 (the "SCCs"), which are incorporated into and made part of the Agreement.

The SCCs shall apply to the extent the parties transfer personal data under the Agreement out of the European Economic Area to third countries not recognized by the European Commission as ensuring an adequate level of protection for personal data, and are deemed to be executed by the parties for such purpose. For clarity, any processing of Personal Data pursuant to an adequacy decision by the European Commission is not subject to the SCCs.

1. Any optional modules or clauses not expressly selected below are not incorporated into the SCCs as adopted by the parties.
2. The parties select Module Two (Controller to Processor).
3. Clause 9(a), Option 2 (General written authorisation) is selected with a time period of thirty (30) days.
4. For purposes of Clause 13 (Supervision) and Annex 1.C of the SCCs, the Data Controller shall maintain accurate records of the applicable Member State(s) and competent supervisory authority, which shall be made available to MathWorks on request.
5. Clause 17 (Governing law), Option 2 is selected ("law of the EU Member State in which the data exporter is established") and the "law of another EU Member State that does allow for third-party beneficiary rights" is specified to be the law of Germany.
6. In Clause 18(b) (Choice of forum and jurisdiction), the EU Member State is specified to be the EU Member State in which the data exporter is established, or Germany in case the data exporter is not established in an EU Member State.
7. The following Annexes are provided with the SCCs.

Annexes to the EU Standard Contractual Clauses

ANNEX I.A

Data exporter
The data exporter is the customer of the data importer, identified as the Data Controller in the Agreement.

Data importer
The data importer is The MathWorks, Inc., a company engaged in the licensing and distribution of software products and services.

ANNEX I.B

Details of transfer, categories, and purpose
The details of transfer, categories of data transferred, and purpose of transfer are described in Section 1 of the Agreement.

No sensitive data
No sensitive data will be transferred under the Agreement.

Duration
The duration of processing is the duration of the Agreement or until the data is no longer needed for the specified purpose, whichever is shorter.

ANNEX I.C

Supervisory authority
Supervisory authority of the Member State in which the data exporter is established, or Germany in case the data exporter is not established in a Member State.

ANNEX II

Technical and organisational measures
The data importer currently follows the security standards listed in Appendix B to the Agreement. The data importer may update or modify these security standards from time to time, provided that any modifications shall provide at least the same level of security of the Personal Data as described in Appendix B.

United Kingdom International Data Transfer Addendum to the EU Standard Contractual Clauses

This Addendum applies where required by the law of the United Kingdom, and is part of the Data Processing Agreement to which the EU SCCs are attached (the "Agreement"). This Addendum provides the information required by the Approved Addendum as issued by the ICO (see Part 2 below). The Parties agree to use the format of the information below, which is not intended to change the content of the Approved Addendum. The Parties further acknowledge that any revised Approved Addendums issued by the ICO in the future shall apply as specified in Section 18 of the Approved Addendum.

Part 1: Tables

For purposes of Tables 1-4:

1. The exporter has the name, address, and contact information identified for the Data Controller in the DPA.
2. The importer is The MathWorks, Inc., 3 Apple Hill Drive, Natick MA 01760 and the key contact for data protection-related issues is privacy@mathworks.com.
3. The version of the Approved EU SCCs is the version marked "Brussels, 4.6.2021 C(2021) 3972 final," Module 2, Controller to Processor (as may be updated by EU authorities).
4. The applicable appendices are attached to the Agreement.
5. Neither party may end the Addendum as set out in Section 19 of the Approved Addendum.

Part 2: Mandatory Clauses

Part 2: Mandatory Clauses of the Approved Addendum, being the template Addendum B.1.0 issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18 of those Mandatory Clauses.