

DATA PROCESSING AGREEMENT

This Data Processing Agreement (the “**DPA**”) is entered into by and between _____, a _____, which expression shall mean and include its representatives, successors and affiliates, either in existence or to be incorporated at a later date (“**Customer**” or “**You**”) and MaintainX Inc. (“**MaintainX**”), effective as of _____, (the “**Effective Date**”). Customer and MaintainX may each be referred to as a “**Party**” or together as the “**Parties**”.

RECITALS

WHEREAS, the Parties have entered into a Master Services Agreement, to provide the Services (the “**Agreement**” or “**MSA**”);

WHEREAS, pursuant to the Agreement, the Parties have agreed that it may be necessary for MaintainX to Process certain Customer Personal Data (as defined below) on behalf of Customer, as more fully described in attached Exhibit A; and

WHEREAS, in light of this Processing, the Parties have agreed to enter into this DPA to address the compliance obligations imposed upon Customer pursuant to Applicable Privacy Law. MaintainX is appointed by Customer, as a Processor (as defined under the GDPR), to Process Customer Personal Data on behalf of Customer to the extent necessary to provide the Services in accordance with the terms of this DPA and the Agreement. For the avoidance of doubt, this DPA shall not apply to the extent MaintainX is operating in the capacity as a Controller (as defined under the GDPR) or joint Controller of personal data (as defined under the GDPR), notwithstanding the fact that such data may also constitute Customer Personal Data hereunder.

NOW THEREFORE, in consideration of the foregoing and the mutual covenants and promises set forth herein, and for other good and valuable consideration, the receipt of which the Parties hereby acknowledge, the Parties hereby agree as follows:

AGREEMENT

1. **Definitions.** In addition to the defined terms specified in the first paragraph, recitals and substantive provisions of this DPA, the following terms have the meanings set forth below:

1.1. “**Applicable Privacy Law**” means the relevant data protection and privacy law (including GDPR) to which Customer is subject, and any guidance or statutory codes of practice issued by the relevant Privacy Authority including, without limitation, the GDPR and the United Kingdom’s GDPR;

1.2. “**Claim**” means any third party action, claim, assertion, demand or proceeding;

1.3. “**Customer Personal Data**” means any information, provided or made available to MaintainX by or on behalf of Customer in connection with MaintainX’s performance of the Services, which relates to an identified or identifiable natural person as defined by the Applicable Privacy Law, and including the categories of data listed in the Processing Appendix together with any additional such personal data to which MaintainX has access from time to time in performing the Services under this DPA;

1.4. “**GDPR**” means Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (the “General Data Protection Regulation”), the national laws of EU member states implementing GDPR, and the UK GDPR;

1.5. “**Losses**” means any (a) Claim, and (b) direct loss, damage, cost, charge, fine, fees, levies,

award or expense. For the avoidance of doubt, Losses shall not include any indirect or consequential losses;

1.6. “**Privacy Authority**” means the relevant supervisory authority with responsibility for privacy or data protection matters in the jurisdiction of Customer;

1.7. “**Process**”, “**Processing**” or “**Processed**” means any operation or set of operations which is performed upon Customer Personal Data whether or not by automatic means, including collecting, recording, organising, storing, adapting or altering, retrieving, consulting, using, disclosing, making available, aligning, combining, blocking, erasing and destroying Customer Personal Data;

1.8. “**Services**” means the services provided by MaintainX in relation to the Processing of Customer Personal Data as described in the Agreement; and

1.9. “**Transfer Contract Clauses**” means the model contract clauses set out in the European Commission’s Decision of 4 June 2021 on 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, as may be amended or replaced by the European Commission from time to time.

2. Processing Requirements.

2.1. MaintainX acknowledges and agrees that, for purposes of this DPA, Customer is the sole owner of all Customer Personal Data and only Customer (including on behalf of its end clients, where applicable) shall have the right to direct MaintainX in connection with MaintainX’s Processing of the Customer Personal Data.

2.2. MaintainX represents and warrants, with respect to all Customer Personal Data that it Processes on behalf of Customer, that at all times, unless otherwise expressly permitted under the Agreement:

(a) it shall Process such Customer Personal Data only for the purposes of providing the Services and as may subsequently be agreed between the Parties in writing and, in so doing, shall act solely on the instructions of Customer;

(b) it shall not Process, apply, or use, the Customer Personal Data for any purpose other than as required and necessary to provide the Services; and

(c) it shall not create or maintain identifiable data derived from the Customer Personal Data, except for the purposes of providing the Services. For the avoidance of doubt, nothing set forth herein shall prevent MaintainX from creating aggregate, non-identifiable data which is derived from the Customer Personal Data.

2.3. MaintainX shall have in place, and maintain, appropriate processes and any associated technical measures that will ensure that Customer's reasonable and lawful instructions, as they relate to the Processing of Customer Personal Data, can be complied with.

2.4. MaintainX shall comply with Applicable Privacy Law, to the extent applicable to MaintainX's Processing of the Customer Personal Data.

2.5. MaintainX shall provide to Customer such co-operation, assistance and information as Customer may reasonably request to enable it to comply with its obligations under any Applicable Privacy Law and co-operate and comply with the directions or decisions of a relevant Privacy Authority, in each case within such reasonable time as would enable Customer to meet any time limit imposed by the Privacy Authority. MaintainX shall provide Customer with all reasonable assistance and information with respect to any notifications to, or registration with, Privacy Authorities as required by Applicable Privacy Law.

2.6. The Parties acknowledge and agree that MaintainX shall not be entitled to reimbursement of any costs which MaintainX may incur as a result of or in connection with complying with Customer's instructions for the purposes of providing the Services and/or with any of its obligations under this DPA or any Applicable Privacy Law; provided, however, that Customer shall reimburse MaintainX for its reasonable costs associated with MaintainX's compliance with (a) its obligations set forth in Section 2.5 above, and/or (b) the directions or decisions of any Privacy Authority, in each case to the extent such obligations arise as a result of Customer's failure to comply with Applicable Privacy Law. If MaintainX does not follow the Customer's instructions on Processing of Customer's Personal Data, the Customer reserves the right to terminate the relevant Services immediately on written notice to MaintainX, without penalty or indemnification, provided that prior to such termination, Customer has provided MaintainX with detailed written notice of MaintainX's failure to follow Customer's instructions and MaintainX does not comply with such instructions within thirty (30) days of receipt of notice.

2.7. MaintainX shall maintain at all times, and provide or make available to Customer, promptly following receipt of Customer's written notice, an accurate and complete written record of the Processing of Customer Personal Data by MaintainX on behalf of Customer (including, without limitation, any Processing undertaken by Sub-Processors).

2.8. To the extent required by Applicable Privacy Law, MaintainX shall designate (a) a data protection officer, and (b) a data protection representative in the EU and/or UK.

3. MaintainX Personnel. MaintainX shall, and shall require each of its Sub-Processors to:

3.1. restrict access to the Customer Personal Data to its personnel who need to access it for purposes of providing the applicable outsourced Services;

3.2. instruct its personnel regarding their confidentiality obligations with respect to the Customer Personal Data; and

3.3. provide its personnel with such information and training as is necessary to ensure that they can Process the Customer Personal Data in accordance with Applicable Privacy Law and the terms set forth herein.

4. Processing and Storage Locations.

4.1. Customer acknowledges and agrees that MaintainX may Process Customer Personal Data in the United States.

4.2. To the extent MaintainX stores Customer Personal Data in a cloud environment, MaintainX shall require the applicable cloud service provider to comply with industry standard best

practises for cloud computing security.

5. Security of Customer Personal Data.

5.1. MaintainX shall maintain, during the term of the Agreement, appropriate technical and organizational security measures to protect the Customer Personal Data against accidental or unlawful destruction or accidental loss, damage, alteration, unauthorized disclosure or access and against all other unlawful forms of Processing, as more fully described in the attached Exhibit B (the "Security Measures").

5.2. MaintainX shall ensure the reliability (as such term is used in the GDPR) of any employees and Sub-Processor personnel who access the Customer Personal Data and ensure that such personnel have undergone appropriate training in the care, protection and handling of Customer Personal Data, and have entered into an agreement, in relation to the Processing of Customer Personal Data, the terms of which are no less onerous than those found in this DPA. MaintainX will remain liable for any unauthorized access to, Processing, or disclosure of Customer Personal Data by each such Sub-Processor as if it had undertaken such action itself.

6. Sub-Processors.

6.1. You expressly and specifically authorize MaintainX to engage another Processor to Process the Personal Data ("**Sub-Processor**"), and specifically consent to the Sub-Processors identified at: <https://www.getmaintainx.com/maintainx-sub-processors>, subject to MaintainX:

(a) providing You with an updated copy of, or link to, the Sub-Processor list in the event MaintainX adds or replaces any Sub-Processor;

(b) including terms in its contract with each Sub-Processor which are materially the same as those set out in this DPA; and

(c) remaining liable to You for any failure by each Sub-processor to fulfil its obligations in relation to the Processing of the Personal Data.

6.2. In relation to any notice received under section 6.1(a), You shall have a period of 30 (thirty) days from the date of the notice to inform MaintainX in writing of any reasonable objection to the use of that Sub-processor. The parties will then, for a period of no more than 30 (thirty) days from the date of Your objection, work together in good faith to attempt to find a commercially reasonable solution for You which avoids the use of the objected-to Sub-processor. Where no such solution can be found, either party may (notwithstanding anything to the contrary in the Agreement) terminate the relevant Services immediately on written notice to the other Party, without penalty or indemnification.

7. Breach Notification.

7.1. Unless otherwise prohibited by applicable law, MaintainX shall notify Customer, as soon as is reasonably possible under the circumstances but in any event no later than within 24 hours after becoming aware, of any accidental, unauthorized, or unlawful destruction, loss, alteration, or disclosure of, or access to, Customer Personal Data ("**Security Breach**"). Such notification shall include, to the extent available, (a) a detailed description of the Security Breach, (b) the type of data that was the subject of the Security Breach and (c) the identity of each affected person (or, where not possible, the approximate number of data subjects and of Customer Personal Data records concerned). MaintainX shall communicate to Customer (i) the name and contact details of MaintainX's chief security officer or other point of contact where more information can be obtained; (ii) a description of the likely consequences of the Security Breach; (iii) a description of the measures taken or proposed to be taken by MaintainX to address the Security Breach, including, where appropriate, measures to mitigate its possible adverse effects; and additionally in such

notification or thereafter (iv) as soon as such information can be collected or otherwise becomes available, any other information Customer may reasonably request relating to the Security Breach or that MaintainX is required to provide to Customer pursuant to this Section 7.1.

7.2. MaintainX shall take prompt action to investigate the Security Breach and shall use industry standard, commercially reasonable, efforts to mitigate the effects of any such Security Breach in accordance with its obligations hereunder and, subject to Customer's prior written agreement, to carry out, at MaintainX's sole cost, any recovery or other action reasonably necessary to remedy the Security Breach. Unless required to do so under Applicable Privacy Law, MaintainX shall not release or publish any filing, communication, notice, press release, or report concerning any Security Breach ("**Notices**") without Customer's prior written approval. MaintainX shall provide written notice to Customer of all corrective actions undertaken by MaintainX following a Security Breach.

8. **Privacy Impact Assessment.** MaintainX shall, promptly upon receipt of written request by Customer, make available to the Customer such information as is reasonably necessary to demonstrate MaintainX's compliance with Applicable Privacy Law and shall assist the Customer, at Customer's expense, in carrying out such privacy impact assessment of the Services as is reasonable in light of the Customer Personal Data that is being processed. MaintainX shall reasonably cooperate with Customer to implement such mitigation actions as are reasonably required to address privacy risks identified in any such privacy impact assessment. Unless such request follows a Security Breach, or is otherwise required by Applicable Privacy Law, Customer shall not make any such request more than once in any 12-month period.
9. **Audit Rights.** MaintainX shall permit Customer and/or its authorized agents to audit its records to the extent reasonably required in order to confirm that MaintainX is complying with its obligations under this DPA or any Applicable Privacy Law, provided always that any such audit does not involve the review of any third party data and that the records and information accessed in connection with such audit is treated as confidential information by Customer. Customer shall bear its own costs in relation to such audit, unless the audit reveals any material non-compliance with MaintainX's obligations under this DPA, in which case the costs of the audit shall be borne by MaintainX.
10. **Deletion of Customer Personal Data.** MaintainX shall, promptly or within no more 60 days, following receipt of a written request from the Customer, return or delete Customer Personal Data from its records and, upon completion of the Services, comply with all reasonable instructions from the Customer with respect to the return or deletion of any remaining Customer Personal Data. In the event MaintainX does not receive such a Customer request, MaintainX shall anonymize all Customer Personal Data after 3 years of inactivity.
11. **Third Party Disclosure Requests.**

11.1. Unless prohibited by applicable law, MaintainX shall, and shall procure that any Sub-Processor shall, inform Customer promptly of any inquiry, communication, request or complaint from:

- (a) any governmental, regulatory or supervisory authority, including Privacy Authorities or the U.S. Federal Trade Commission; and/or
- (b) any data subject,

relating to the Services, any Customer Personal Data or any obligations under Applicable Privacy Law, and shall provide all reasonable assistance to enable Customer to respond to such inquiries, communications, requests or complaints and to meet applicable statutory or regulatory deadlines. MaintainX shall, and shall require that any Sub-Processor shall, not disclose Customer Personal Data to any of the persons or entities listed in (a) or (b) above unless it is (i) legally required to do so and has otherwise complied with the obligations in this Section, or (ii) Customer has expressly authorized it in writing to do so.

11.2. Unless prohibited by applicable law, in the event that MaintainX or any Sub-Processor is required by law, court order, warrant, subpoena, or other legal judicial process (“Legal Request”) to disclose any Customer Personal Data to any person or entity other than Customer, MaintainX shall, and shall procure that any Sub-Processor shall, notify Customer promptly and shall provide all reasonable assistance to Customer to enable Customer to respond or object to, or challenge, any such demands, requests, inquiries or complaints and to meet applicable statutory or regulatory deadlines. MaintainX shall, and shall procure that any Sub-Processor shall, not disclose Customer Personal Data pursuant to a Legal Request unless it is required to do so and has otherwise complied with the obligations in this Section.

12. Transfers of Customer Personal Data Outside of the European Economic Area and United Kingdom.

12.1. Where Customer Personal Data originating in the European Economic Area is Processed by MaintainX outside the European Economic Area, in a territory that has not been designated by the European Commission as ensuring an adequate level of protection pursuant to Applicable Privacy Law, MaintainX and Customer agree that the transfer will be subject to the Transfer Contract Clauses which shall be deemed to apply in respect of such Processing. The Transfer Contract Clauses are attached hereto as Exhibit C hereto.

12.2. Where Customer Personal Data originating in the United Kingdom is Processed by MaintainX outside the United Kingdom, in a territory that has not been designated by the Information Commissioner’s Office as ensuring an adequate level of protection pursuant to Applicable Privacy Law, MaintainX and Customer agree that the transfer will be subject to the Transfer Contract Clauses which shall be deemed to apply in respect of such Processing. The Transfer Contract Clauses are attached hereto as Exhibit D hereto.

13. Indemnity. MaintainX shall indemnify Customer (and each of its respective officers, employees and agents), against all Losses arising out of or in connection with any material breach by MaintainX (and by any Sub-Processor) of the provisions of this DPA or the negligence or willful misconduct of MaintainX, its employees or agent. Customer shall promptly notify MaintainX, in writing, of any such alleged breach and Customer shall not incur any costs or liabilities with respect to the same and with respect to which it would be indemnified by MaintainX hereunder, without the prior written consent of MaintainX, such consent not to be unreasonably delayed or withheld.

14. Term. This DPA shall commence on the Effective Date and shall continue in full force and effect until the later of (a) the termination or expiration of the Agreement, or (b) completion of the last of the Services to be performed pursuant to the Agreement.

15. Governing Law. This DPA shall be governed by and construed in accordance with the laws of the _____.

16. Order of Precedence. The Parties agree that this DPA is part of the Agreement and is governed by its terms and conditions, unless otherwise required by applicable law. In case of conflict, the order of precedence in respect of the Processing of Customer’s Personal Data shall be: Exhibits to this DPA, this DPA and then the Agreement.

17. Amendments. If an amendment to this DPA, including its Exhibits, is required in order to comply with applicable law, the Customer shall provide an amendment to this DPA with the required changes to MaintainX. Both Parties shall work together in good faith to promptly execute a mutually agreeable amendment to this DPA. In case MaintainX is not able to accommodate the requested changes having been given a reasonable opportunity to do so, Customer may terminate all or part of the Agreements and this DPA with thirty (30) days’ written notice.

18. Counterparts. This DPA may be executed in any number of counterparts, each of which shall be deemed an original, but all of which together shall constitute one and the same instrument.

MAINTAINX INC.

CUSTOMER

By: _____

By: _____

Printed Name: _____

Printed Name: _____

Title: _____

Title: _____

Date: _____

Date: _____

Exhibit A

Summary of Processing

1. **Subject Matter:** The context for the Processing of Customer Personal Data is MaintainX's provision of the Services under the Agreement(s).
2. **Duration of Processing:** MaintainX will Process Customer Personal Data until expiration or termination of the Agreement(s).
3. **Nature and Purpose of Processing:** MaintainX will Process Personal Data for the purpose of providing Services in accordance with the Agreement(s).
4. **Categories of Data Subjects:** MaintainX will Process Personal Data that relates to any and all data subjects about whom Customer transfers Personal Data to MaintainX to provide services under the Agreement(s).

5. Types of Personal Data Processed:

X **Contact Information** (e.g., name, email address, phone number, username, password)

- o **Name, email address and phone number**

X **Location Data** (e.g., postal address, IP address, etc.)

- o **IP addresses are kept on log in tokens for security purposes**

X **Preference Data** (e.g., profile/account settings such as languages, etc.)

- o **User preferences regarding display and language for using service**

X **Other** (e.g., online identifiers, payroll data, system access data, compensation data, etc.) - if applicable, please de-scribe:

- o **System access data for user support purposes**

6. Contact Details of MaintainX's Privacy Contact:

For questions related to security and privacy please email security@getmaintainx.com, or privacy@getmaintainx.com,

Exhibit B

Security Measures

Operational Security

MaintainX's Security Team is responsible for operational security. This includes network and data security, as well as the patching and monitoring of MaintainX's computing resources.

Physical Security

MaintainX utilizes best in breed cloud hosting facilities, these facilities are certified in various levels of ISO, PCI, and SOC compliance. Specific certifications are available on request. Access to infrastructure is tightly controlled as per SAS 70 requirements and guidelines.

Network Security

MaintainX follows industry standard best practices regarding the hardening of servers, and communication protocols against attacks and exploits and are audited on an ongoing basis. All production systems are built from standard system images that are closely audited and tested. MaintainX allows only specific traffic from known services to communicate with its applications and servers; extraneous services are disabled and required ports are whitelisted. Applications are run with restricted privileges, and passwords are rotated.

MaintainX leverages on and off-host network access control lists (ACLs) to actively protect against application layer attacks. These systems are configured to pass only HTTPS (TLS) traffic and other limited ports required for proper application operation.

Access control policies are enforced based on server roles and kept in a known state. MaintainX's in-house security team audits the currently enforced policies on a regular basis to maintain effective security controls.

Access to network administration controls are restricted to audited roles. These roles, network tools, protocols, and configuration are reviewed and evaluated at least monthly.

Data Security

Personal data is always transferred over TLS connections, using at minimum TLS version 1.2. Data is stored in encrypted form at rest using the AES-256 cipher. Encryption key integrity and safety is managed by AWS KMS.

Role based controls restrict access to personal data. Roles are centrally managed by MaintainX's Security team and access rights are actively maintained. MaintainX's Security team performs quarterly reviews of all privileges within our systems to ensure that entitlements align with the roles defined in our organization. Requests for changes to a user's entitlements are tracked via a Case Management system, which logs the requestor, approver and executor. Cases are stored indefinitely.

Changes to user entitlements are logged with the date, roles added/revoked, and the username of the user administering the change. Logs are retained for one year.

MaintainX undergoes a SOC2 Type II audit every year, and follows strict security protocols enforced by MaintainX's Security team and by the CTO.

Patching

Vulnerabilities and patches are reviewed and evaluated on a regular basis, and as required by MaintainX's Security team. Patches and operating system changes are validated in a staging environment that matches production before applying them to production. The production environment gets updated in a rolling deployment to ensure testing and compatibility.

Infrastructure Monitoring

MaintainX's Security team utilizes best of breed & industry standard utilities to monitor all systems and network-level activities. MaintainX uses host-based Intrusion Detection Systems that are integrated with our monitoring and alerting system.

Error logs are maintained in storage for 6 months and transferred via an encrypted protocol. Server logs are maintained in storage for 12 months and are transferred via encrypted protocols.

Software & Release Engineering

Software Development Process

MaintainX utilizes technologies that are designed to address the OWASP Top 10 vulnerabilities. MaintainX provides systematic security training to every hire. Code reviews are performed on 100% of the code change requests to identify potential security-related flaws.

Data is validated both on the client and on the server side before it gets used in the MaintainX ecosystem. Data input and output routines are architected to prevent both XSS (Cross-site scripting) and SQL injection as well as other forms of data corruption.

MaintainX uses one-time credentials that are generated on a logon attempt, to confirm user identity. The MaintainX software locks an account after several failed logon attempts and invalidates the temporary credentials after they have either been used, or too many requests on the same account are attempted.

Release Management

System updates are done on a continuous basis, to ensure bug fixes are in production without delay.

All production builds are produced on a controlled build system that pulls code directly from our source code repository and all code changes are tagged by developers and traceable back to individual engineers. Changes to production systems are verified in a staging environment that is a clone of production. Only builds that have been marked as tested by QA are eligible to be deployed to production.

The release management team reviews tested builds to assess timing and risk of production releases. Access controls ensure that only authorized individuals can initiate changes that will impact the production environment, via MaintainX's managed deployment system.

Data Retention & Backup

Data Retention Policy

Retailer-provided sales and returns data is retained for the period defined in MaintainX's contract with the retailer.

User registration data is retained indefinitely. Once a user has been inactive for a period of 3 years, that user's data is anonymized.

Backup Policy

Data backups are performed nightly and stored encrypted at rest in our hosting provider's cloud storage solution. Backups are kept for 30 days.

Restore tests of backups are run biannually. Test plans as well as result summaries are kept for 12 months.

Threat Management Practices

Non-critical threats and vulnerabilities are managed through monthly internal audits and yearly third-party audits.

Critical internal alerts and public CVE reports are triaged and assessed immediately and remediated as appropriate.

Third Party Audits

MaintainX works with independent security vendors to regularly perform independent testing of our service and infrastructure to assess vulnerabilities.

For additional information, please contact security@getmaintainx.com

Exhibit C

Processor Model Clauses EEA

Module Two – EEA Controller to U.S. Processor

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) for the transfer of 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 Appendix 1 (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 Appendix 1 (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 Appendix 1.
- (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 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 Appendix 1.

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, 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 Exhibit B 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 Appendix 1. 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 Exhibit B. 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) 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 specific restrictions and/or additional safeguards.

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 () (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;
- (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) **GENERAL WRITTEN AUTHORISATION.** The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list in Exhibit E. The data importer shall specifically inform the data exporter in writing of any intended changes to that list

through the addition or replacement of sub-processors at least fourteen (14) in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

- (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. () 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 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 Exhibit B 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.
- (b) 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.
- (c) 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.
- (d) 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.
- (e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.
- (f) 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 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 ();

- (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).
- (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 the _____ (*specify Member State*).

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 the _____ (*specify Member State*).
- (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.

Exhibit D
Processor Model Clauses UK
Standard Contractual Clauses (processors)

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection

Name of the data exporting organisation:

Address:

Tel.: _____ ; fax: _____ ; e-mail: _____

Other information needed to identify the organisation:

And
(the data **exporter**)

Name of the data importing organisation: **MaintainX Inc.**

Address: **244 Biscayne Blvd, #290, Miami, FL, 33139 USA**

.....
(the data **importer**)

each a “party”; together “the parties”,

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

For the purposes of the Clauses:

Clause 1

Definitions

(a) *'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject' and 'supervisory authority'* shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individ-

1

uals with regard to the processing of personal data and on the free movement of such data ;

(b) *'the data exporter'* means the controller who transfers the personal data;

(c) *'the data importer'* means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

(d) *'the subprocessor'* means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

(e) *'the applicable data protection law'* means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

(f) *'technical and organisational security measures'* means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2

Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

Clause 3

Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

3. The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insol-

vent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

- (a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;
- (b) that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;
- (c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;
- (d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;
- (e) that it will ensure compliance with the security measures;
- (f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;
- (g) to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;
- (h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;
- (i) that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and
- (j) that it will ensure compliance with Clause 4(a) to (i).

Obligations of the data importer

The data importer agrees and warrants:

- (a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;
- (b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;
- (c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;
- (d) that it will promptly notify the data exporter about:
 - (i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,
 - (ii) any accidental or unauthorised access, and
 - (iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;
- (e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;
- (f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in MSA with the supervisory authority;
- (g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;
- (h) that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;
- (i) that the processing services by the subprocessor will be carried out in accordance with Clause 11;
- (j) to send promptly a copy of any subprocessor MSA it concludes under the Clauses to the data exporter.

Clause 6

Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or subprocessor is entitled to receive compensation from the data exporter for the damage suffered.
2. If a data subject is not able to bring a claim for compensation in accordance with para-

graph 1 against the data exporter, arising out of a breach by the data importer or his subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, in which case the data subject can enforce its rights against such entity.

The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the subprocessor agrees that the data subject may issue a claim against the data subprocessor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the subprocessor shall be limited to its own processing operations under the Clauses.

Clause 7

Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

(a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

(b) to refer the dispute to the courts in the Member State in which the data exporter is established.

2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8

Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

Clause 9

Governing Law

The Clauses shall be governed by the law of the Member State in which the data exporter is established.

Clause 10

Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding

clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11

Subprocessing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written MSA with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the

3

Clauses . Where the subprocessor fails to fulfil its data protection obligations under such written MSA the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such MSA.

2. The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

3. The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.

4. The data exporter shall keep a list of subprocessing MSAs concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12

Obligation after the termination of personal data processing services

1. The parties agree that on the termination of the provision of data processing services, the data importer and the subprocessor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

2. The data importer and the subprocessor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

On behalf of the data exporter:

Name (written out in full):

Position:

Address:

Other information necessary in order for the contract to be binding (if any):

Signature.....

(stamp of organisation)

On behalf of the data importer:

Name (written out in full):

Position:

Address:

Other information necessary in order for the contract to be binding (if any):

Signature.....

(stamp of organisation)

APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES (ATTACHMENT A)

This Appendix forms part of the Clauses and must be completed and signed by the parties.

The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix.

A. List of Parties

Data exporter

The data exporter is (please specify briefly your activities relevant to the transfer):

Address:

Contact Person's Name, Position, and Contact Details:

The activities relevant to the data transferred under these Clauses are the performance of the Services pursuant to the MSA.

Data importer

The data importer is (please specify briefly activities relevant to the transfer):

MaintainX is a US based company delivering maintenance and operational management digitization services to customers all over the world.

Address: 244 Biscayne Blvd, #290, Miami, FL, 33139 USA

Contact Person's Name, Position, and Contact Details: For questions related to security and privacy please email security@getmaintainx.com, or privacy@getmaintainx.com.

The activities relevant to the data transferred under these Clauses are the performance of the Services pursuant to the MSA.

Data subjects

The personal data transferred concern the following categories of data subjects (please specify):

Data subjects within the context of this Model Clauses are any natural person that is an employee or contractor of a customer of MaintainX.

B. Description of Transfer

Categories of data

The personal data transferred concern the following categories of data (please specify):

Name, email address, phone number; IP addresses (on log in tokens for security purposes); user preferences (for display and language for using the Services); and system access data (for user support purposes).

Special categories of data (if appropriate)

The personal data transferred concern the following special categories of data (please specify):

Not applicable.

Processing operations

The personal data transferred will be subject to the following basic processing activities (please specify):

The objective of Processing of Personal Data by data importer is the performance of the Services pursuant to the MSA.

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis): Continuous.

Nature and Purpose of the processing: MaintainX will Process Personal Data for the purpose of providing Services in accordance with the Agreement(s).

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period: MaintainX will Process Customer Personal Data until expiration or termination of the Agreement(s).

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing: Continuous.

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies:

DATA EXPORTER

Name:

Authorised Signature

DATA IMPORTER

Name: MaintainX

Authorised Signature

APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed by the parties.

Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached):

Data importer (MaintainX) will maintain technical and organizational security measures for protection of the security, confidentiality and integrity of Personal Data Processed in the context of the provision of the Services as described in Exhibit B to the Data Processing Agreement which is hereby incorporated by reference in its entirety.

DATA EXPORTER

Name:

Authorised Signature

DATA IMPORTER

Name:.....

Authorised Signature

Exhibit E

LIST OF SUB-PROCESSORS

The controller has authorised the use the sub-processors set forth at: <https://www.getmaintainx.com/maintainx-sub-processors/>