DATA PROCESSING AGREEMENT

This Data Processing Agreement (the "**DPA**") is entered into by and between MaintainX Inc. ("**MaintainX**") and Customer (as defined in Section 1 below). Customer and MaintainX may each be referred to as a "**Party**" or together as the "**Parties**". This DPA is incorporated into and forms part of the MaintainX Terms of Service Agreement or Master Services Agreement, or other or other written or electronic agreement, entered into between MaintainX and the Customer, and in each case, that includes a link or express reference incorporating this DPA into the terms of such agreement (hereinafter, the "**Agreement**"), and sets forth each Party's respective obligations with respect to the processing of Personal Data in connection with the Services provided pursuant to the Agreement. Capitalized terms not defined in this DPA shall have the meaning set forth in the Agreement.

1. Definitions. In addition to the terms defined elsewhere in this DPA, the following terms have the meanings set forth below:

1.1. "***Anonymous Data***" means Personal Data that has been Processed in such a manner that it can no longer be attributed to an identified or identifiable Data Subject and cannot be re-identified, including "aggregate consumer information," as such term is defined in the CPRA or other Applicable Data Laws.

1.2. "***Applicable Data Law***" means any state, federal, local and/or foreign data protection and privacy law, rule or regulation applicable to the Processing of Customer Personal Data under the Agreement and this DPA, including, but not limited to, (to the extent applicable): (a) EU Data Laws, and (b) the California Privacy Rights Act, together with any implementing regulations, as may be amended, superseded, or replaced from time to time (collectively, "**CPRA**").

1.3. "***Controller***" means the entity which determines the purposes and means of the Processing of Personal Data, including as applicable any "Business", as defined under the CPRA.

1.4. "***Customer Personal Data***" means Personal Data that MaintainX Processes on behalf of Customer in connection with the provision of the Services, as further described in Exhibit A to this DPA .

1.5. "***Data Subject***" means an identified or identifiable person to whom Customer Personal Data relates, including as applicable any "Consumer" as defined under the CPRA or other Applicable Data Laws.

1.6. "**Data Subject Request**" means a request by a Data Subject to exercise any of the Data Subject's rights provided for under Applicable Data Laws, including, but not limited to, the right of: access, rectification, restriction of Processing, erasure, data portability, restriction of or objection to Processing, withdrawal of consent to Processing, or objection to being subject to Processing that constitutes automated decision-making.

1.7. "***De-Identified Data***" has the meaning provided for under the relevant Applicable Data Law.

1.8. "***EU Data Laws***" means, individually and collectively, the GDPR, UK GDPR, the Swiss Federal Data Protection Act or any other applicable data protection laws, rules or regulations of Switzerland ("**Swiss Data Laws**"), and the EU e-Privacy Directive (Directive 2002/58/EC), each as applicable and as amended, repealed, consolidated or replaced from time to time.

1.9. "***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").

1.10. "***Instruction***" means a direction or instruction with respect to the Processing of Customer Personal Data, either in writing, in textual form (e.g., by e-mail) or by using a software or online tool, issued by or on behalf of Customer to MaintainX.

1.11. "***Personal Data***" means information defined as personal data, personal information, or a similar term by

Applicable Data Laws, and any other information that identifies, relates to, describes, or is capable of being associated with, directly or indirectly, an individual or household. Personal Data does not include Anonymous Data and/or De-Identified Data, as provided for under Applicable Data Law.

1.12. "***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.

1.13. "***Processor***" means a natural or legal person, public authority, agency or other body which processes Personal Data on behalf of the Controller, including, as applicable, any "service provider" as defined under the CPRA or other Applicable Data Laws.

1.14. "***Regulatory Authority***" means any governmental, regulatory, or supervisory authority, including, any U.S. State Attorney Generals, the U.S. Federal Trade Commission, or an independent public authority established by a member state of the European Economic Area or the United Kingdom, that has competent authority in its jurisdiction for overseeing, enforcing, or supervising the Applicable Data Laws of such jurisdiction.

1.15. "***Security Breach***" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to unencrypted Personal Data.

1.16. "***Services***" means the services provided by MaintainX in relation to the Processing of Customer Personal Data as described in the Agreement.

1.17. "***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 (available at https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj), as may be amended or replaced by the European Commission from time to time, and, where the UK GDPR applies, as amended by the UK Addendum, and subject to the operative provisions and additional terms attached hereto at Exhibit C.

1.18. "***UK Addendum***" means the template Addendum B.1.0 and the accompanying mandatory clauses as issued by the UK's Information Commissioner's Office and laid before Parliament in accordance with s119A of the Data Protection Act 2018 of the UK on 2 February 2022, and in force on 21 March 2022 (available at https://ico.org.uk/media/for-organisations/documents/4019539/international-data-transfer-addendum.pdf).

1.19. "***UK GDPR***" means the GDPR as implemented into the law of the United Kingdom by the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 and the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2020 and the Data Protection Act 2018.

2. Roles of the Parties. The parties acknowledge and confirm that with respect to the Processing of Customer Personal Data, Customer is the Controller or Processor, and MaintainX is the Processor.

3. Details of Processing. The subject matter, nature, purpose, and duration of Processing, as well as the types of Customer Personal Data and categories of Data Subjects that may be Processed by MaintainX, are described in Exhibit A hereto

4. Customer Obligations

4.1. Customer shall, in its use of the Services, at all times Process Customer Personal Data in compliance with the Applicable Data Laws. Customer shall ensure that its Instructions comply with all laws, rules and regulations applicable in relation to the Customer Personal Data, and that the Processing of Customer Personal Data in accordance with Customer's Instructions shall not cause MaintainX to be in breach of any

Applicable Data Laws. Customer is solely responsible for the accuracy, quality, and legality of (a) the Customer Personal Data provided to MaintainX by or on behalf of Customer, (b) the means by which Customer acquired any such Customer Personal Data, and (c) the Instructions it provides to MaintainX regarding the Processing of such Customer Personal Data. Customer shall not provide or make available to MaintainX any Customer Personal Data other than as specified in Exhibit A hereto, unless otherwise mutually agreed upon in writing by the parties.

4.2. To the extent required by Applicable Data Laws, Customer is responsible for ensuring that any necessary Data Subject consents to this Processing are obtained and for ensuring that a record of such consents is maintained. Should such a consent be revoked by the Data Subject, Customer shall promptly notify MaintainX of such revocation.

4.3. Where Customer is a Processor, Customer warrants that its Processing Instructions as set out in the Agreement and this DPA, including its authorizations to MaintainX for the appointment of Sub-Processors in accordance with this DPA, have been authorized by the relevant Controller. Customer shall be solely responsible for forwarding any notifications received from MaintainX to the relevant Controller where appropriate.

4.4. Where an Affiliate of Customer is the Controller over any Customer Personal Data processed by MaintainX under this DPA, Customer shall ensure that any relevant Affiliate complies with the obligations of Customer under the Applicable Data Laws and this DPA in respect of such Customer Personal Data. Customer shall remain responsible for its Affiliates' performance under this DPA.

5. Processing Requirements.

5.1. With respect to all Customer Personal Data that it Processes on behalf of Customer, MaintainX shall at all times, unless otherwise expressly permitted under the Agreement:

5.1.a. 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 each case, in accordance with the Instructions of Customer;

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

5.1.c. 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 and using Anonymous Data and/or De-Identified Data which is derived from the Customer Personal Data.

5.2. To the extent MaintainX's Processing of Customer Personal Data is subject to the CPRA, MaintainX shall not: (1) retain, use, or disclose Customer Personal Data for any purpose (commercial or otherwise) other than the business purposes expressly stated in this DPA or outside the direct business relationship between Customer and MaintainX, unless expressly permitted in the CPRA; (2) "sell" or "share" Customer Personal Data, as such terms are defined under the CPRA; or (3) combine the Customer Personal Data received with Personal Data received from another business or that MaintainX collects itself (unless such combination is necessary for certain business purposes identified in the CPRA). In addition, MaintainX will (a) allow and cooperate with Customer's reasonable efforts to assess MaintainX's compliance with the CPRA, which shall be subject to and satisfied by the obligations set forth in Section 10 of this DPA, and (b) notify Customer if MaintainX cannot meet its obligations under CPRA and stop and remediate any unauthorized use of Customer Personal Data.

5.3. If MaintainX is unable to Process Customer Personal Data pursuant to the Instructions due to legal requirements under applicable laws, MaintainX will inform the Customer of that legal requirement before Processing (unless such notification is otherwise prohibited by applicable laws). MaintainX agrees to

promptly inform the Customer if, in its reasonable opinion, an Instruction infringes any Applicable Data Laws. In such case, MaintainX will cease all Processing of the affected Customer Personal Data (other than merely storing and maintaining the security of the affected Customer Personal Data) until such time as the Customer issues new Instructions with which MaintainX is able to comply, and MaintainX shall not be liable to Customer under the Agreement for failure to perform the Services until such time as Customer issues such Instructions.

5.4. MaintainX shall comply with Applicable Data Laws in its Processing of Customer Personal Data.

5.5. MaintainX shall, taking into account the nature of the Processing and the information available to MaintainX, provide Customer with reasonable cooperation and assistance where necessary for Customer to comply with Customer's obligations under Applicable Data Laws as it relates to the Processing of Customer Personal Data, including, but not limited to: (a) any requirements to conduct a data protection, privacy, or transfer impact assessment, provided that Customer does not otherwise have access to the relevant information, or (b) Customer's cooperation or prior consultation with any Regulatory Authority, where necessary or where required by the Applicable Data Laws.

5.6. 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 its Processing of Customer Personal Data for the purposes of providing the Services pursuant to this DPA and the Agreement and/or with any of its express obligations as Processor under any Applicable Data Law; provided, however, that Customer shall reimburse MaintainX for its reasonable costs associated with MaintainX's (a) performance of its obligations set forth in Section 5.5 above or Section 12 below, and/or (b) compliance with the directions or decisions of any Regulatory Authority to the extent such compliance obligations arise as a result of Customer's failure to comply with Applicable Data Law.

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

6. MaintainX Personnel. MaintainX shall:

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

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

6.3. 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 Data Law and the terms set forth herein.

7. Security of Customer Personal Data.

7.1. MaintainX shall maintain, during the term of the Agreement, appropriate industry standard technical and organizational security measures reasonably designed to protect the Customer Personal Data against accidental or un- lawful 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***").

7.2. Without prejudice to MaintainX's obligations under this DPA, and elsewhere in the Agreement, Customer is responsible for its secure use of the Services, including, without limitation: (a) protecting account authentication credentials; (b) protecting the security of Customer Personal Data using third party tools not operated or controlled by MaintainX when in transit to and from the Services; and (c) implementing measures to allow Customer to backup and archive appropriately in order to restore availability and access to Customer Personal Data in a timely manner in the event of a physical or technical incident.

8. Sub-Processors.

8.1. Subject to this Section 8, You expressly and specifically authorize MaintainX to engage another Processor to Process Customer Personal Data ("***Sub-Processor***"), and specifically consent to MaintainX's use of the Sub-Processors identified at: https://www.getmaintainx.com/maintainx-sub-processors as of the Effective Date.

8.2. Following the Effective Date, MaintainX will provide Customer's designated privacy contact specified on Exhibit A with reasonable prior notice via email, as required under Applicable Data Laws, before enabling any new Sub-Processor to Process any Customer Personal Data in connection with the provision of the Services. You shall have a period of 10 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 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. If You do not object to the engagement of a new Sub-Processor in accordance with this Section 8.2 within such 30 days period, You shall have deemed to accept and consent to the use of such Sub-Processor.

8.3. Each Sub-Processor shall be bound by a written agreement which subjects the Sub-Processor to obligations regarding the Processing of Customer Personal Data that are no less protective than those to which MaintainX is subject under this DPA and to the extent applicable to the nature of the services provided by the Sub-Processors. MaintainX shall remain responsible and liable for its Sub-Processors' performance under, and compliance with, this DPA.

9. Breach Notification.

9.1. Unless otherwise prohibited by applicable law, MaintainX shall notify Customer's privacy contact identified in Exhibit A via email, as soon as is reasonably possible under the circumstances but in any event no later than within 48 hours after becoming aware, of any actual or suspected Security Breach involving Customer Personal Data ("***Customer Security Incident***"). Such notification shall include, to the extent available, (a) a detailed description of the Customer Security Incident, (b) the type of data that was the subject of the Customer Security Incident and (c) the identity of each affected person (or, where not feasible to provide the identity, 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 Customer Security Incident; (iii) a description of the measures taken or proposed to be taken by MaintainX to address the Customer Security Incident, 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 Customer Security Incident or that MaintainX is required to provide to Customer pursuant to this Section 9.1.

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

10. **Audit Rights.** During the Term, upon prior written request by Customer (not less than 30 days), MaintainX shall within a reasonable time provide Customer with: (a) a summary of the audit reports available to MaintainX that demonstrate MaintainX's material compliance with its obligations under Applicable Data Laws and this DPA with

respect to Customer Personal Data, after redacting any confidential and commercially sensitive information; and (b) confirmation that such audit has not revealed any material vulnerability in MaintainX's systems, or to the extent that any such vulnerability was revealed, that MaintainX has taken steps to remediate such vulnerability (collectively, the "***Audit Report***"). If the above measures are insufficient to confirm MaintainX's material compliance with Applicable Data Laws or this DPA with respect to Customer Personal Data, then subject to MaintainX's reasonable confidentiality and security procedures, MaintainX will permit Customer, or an independent third party auditor that is mutually agreed upon by the parties, at Customer's sole cost and expense, to audit MaintainX's data protection compliance program ("***Customer Audit***"). Any Customer Audit must be conducted during MaintainX's normal business hours, and the parties must mutually agree upon the scope, timing, and duration of a Customer Audit in advance of a Customer Audit. In addition, Customer acknowledges that MaintainX operates a multi-tenant cloud environment. Accordingly, MaintainX shall have the right to reasonably adapt the scope of any Customer Audit to avoid or mitigate risks with respect to, and including, service levels, availability, and confidentiality of MaintainX's other customers' information.

The Audit Reports and results of any Customer Audit, which may include the results of any written reports in connection with a Customer Audit, shall be deemed MaintainX's Confidential Information. Customer may only request an Audit Report (and any related Customer Audit) once per consecutive 12 month period; provided that, in the event of a Customer Security Incident, Customer may request a supplementary Audit Report and a Customer Audit subject to and in accordance with this Section.

11. Deletion of Customer Personal Data. MaintainX shall, promptly or within no more than 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.

12. Data Subject and Legal Disclosure Requests.

12.1. As between the parties, Customer is responsible for handling and responding to all Data Subject Requests relating to Customer Personal Data under Applicable Data Laws, including, but not limited to, communicating with the Data Subject who is the subject of the applicable Data Subject Request. If MaintainX receives a Data Subject Request in relation to Customer Personal Data, MaintainX will (a) promptly notify Customer of the request and provide a copy of the request to Customer; and (b) advise the Data Subject to submit their request to Customer. MaintainX will use commercially reasonable efforts to assist Customer with responding to any such request upon Customer's written request for assistance; provided that, (i) Customer is itself unable to respond without MaintainX's assistance and (ii) MaintainX is able to do so in accordance with all applicable laws, rules, and regulations, including, Applicable Data Laws.

12.2. Unless prohibited by applicable law, in the event that any Customer Personal Data in MaintainX's possession or control is required to be disclosed by law, court order, warrant, subpoena, or other legal judicial process ("***Legal Request***"), MaintainX shall notify Customer promptly and shall provide, at Customer's expense, reasonable assistance requested by Customer in connection with any action taken by Customer to respond or object to, or challenge, any such demands, requests, inquiries or complaints.

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

13.1. Customer acknowledges and accepts that the provision of the Services may involve the transfer of Customer Personal Data to, and Processing of Customer Personal Data in, locations outside of the European Economic Area and/or United Kingdom from time to time, including processing in the United States and any country in which MaintainX, its affiliates and Sub-Processors perform the Services.

13.2. Where Customer Personal Data subject to EU Data Laws (for purposes of this Section 13, "***EU Personal Data***") is transferred to, or Processed by MaintainX in, countries (or territories or sectors within a country) or international organizations which do not benefit from an adequacy decision under EU Data Laws, MaintainX and Customer agree that the transfer will be subject to the Transfer Contract Clauses which shall be

deemed to apply in respect of the Processing of EU Personal Data.

13.3. For the avoidance of doubt, data transfers where Customer is established in Switzerland or falls within the territorial scope of application of Swiss Data Laws, the Transfer Contractual Clauses also apply to the transfer of information relating to an identified or identifiable legal entity where such information is protected similarly as Personal Data under Swiss Data Laws until such laws are amended to no longer apply to a legal entity. In such circumstances, general and specific references in the Transfer Contractual Clauses to GDPR or other applicable EU Data Laws shall have the same meaning as the equivalent reference in Swiss Data Laws.

13.4. The Transfer Contractual Clauses are subject to this DPA and the additional safeguards set out hereunder. The rights and obligations afforded by the Transfer Contractual Clauses will be exercised in accordance with this DPA, unless stated otherwise. In the event of any conflict or inconsistency between the body of this DPA and the Transfer Contract Clauses, the Transfer Contract Clauses shall prevail with respect to EU Personal Data.

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 governing law and jurisdiction provisions in the Agreement; except where otherwise expressly stated in this DPA or as otherwise required by Applicable Data Laws.

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. For the avoidance of doubt, each Party's liability and remedies under this DPA are subject to the aggregate liability limitations and damages exclusions set forth in the Agreement.

17. **Amendments.** Notwithstanding any provisions to the contrary in this DPA, if any change in Applicable Data Laws may require or result in any variation to this DPA, MaintainX shall modify this DPA as necessary to incorporate such change(s) and provide a copy of the modified DPA to Customer. Customer shall notify MaintainX of any objection to such modifications of the DPA within 30 days of MaintainX's delivery of such modified DPA to Customer. If MaintainX does not receive any objection from Customer within this 30 day period, Customer shall be deemed to have accepted such modifications and such modifications shall become binding and enforceable as part of this DPA. Should Customer submit objections to MaintainX within the above-referenced 30 days, Customer and MaintainX agree to discuss and negotiate in good faith any such necessary modifications to this DPA to address the changes with a view to agreeing and implementing modifications as mutually agreeable to both Customer and MaintainX as soon as is reasonably practicable but no later than 30 days following MaintainX's receipt of Customer's objections. If Customer and MaintainX are unable to reach agreement on modifications to this DPA within such 30 day time period and do not mutually agree in writing to extend the negotiation period prior to expiration of such 30 day period, either party may terminate the Agreement upon written notice to the other party, and MaintainX will issue a pro rata refund for any Fees paid and unused under any then-current Statement(s) of Work corresponding to the time period between the effective date of termination and the expiration of the Agreement. Except as stated above or as otherwise expressly set forth in this DPA, this DPA may be modified or amended only in writing signed by both MaintainX and Customer.

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

Exhibit A
Summary of Processing

1. List of Parties

Data exporter

The data exporter is (please specify briefly your activities relevant to the transfer): The Data Exporter is the Customer, as identified in the Agreement.

Address: As identified in the Agreement.

Contact Person's Name, Position, and Contact Details: As identified in the Agreement.

Activities: The activities relevant to the data transferred under this DPA is the transferring and otherwise Processing of the Customer Personal Data identified and described in this Exhibit A related to receipt of the Services described in the Agreement.

Role (controller/processor):

For purposes of Module 2 of the Transfer Contract Clauses, Data Exporter is the Data Controller.

For purposes of Module 3 of the Standard Contractual Clauses, Data Exporter is a Data Processor

Data importer

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

Address: 382 NE 191st Street PMB 98008, Miami, Florida, 33179-3899, United States

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 Agreement.

Role (controller/processor): processor

2. Description of Transfer

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).

Types of Personal Data Processed:

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

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

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

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

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

- **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 describe:*

- **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 Agreement.**

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.**

Exhibit B
Security Measures

1. 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.

2. Physical Security

MaintainX utilizes best in class 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.

3. 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 only the required ports are allowed. Applications are executed with restricted privileges, and passwords and keys are rotated on a quarterly basis.

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.

4. 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.

5. 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.

6. Infrastructure Monitoring

MaintainX's Security team utilizes best in class & 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.

7. Software & Release Engineering

7.1. 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 login attempts and invalidates the temporary credentials after they have either been used, or too many requests on the same account are attempted.

7.2. 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.

8. Data Retention & Backup

8.1. 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.

8.2. 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.

9. 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 and remediated according to their severity.

10. 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
Transfer Contract Clauses - Operative Provisions and Additional Terms

1. STANDARD CONTRACTUAL CLAUSES:

Operative Clauses & Additional Terms

Operative Clauses & Additional Terms	***Module 2****:* Applies where Customer is the Controller	***Module 3****:* Applies where Customer is a Processor
Docking *(Clause 7)*	Disapplied	
Instructions and Notifications *(Clause 8.1(a))*	For the purposes of Clauses 8.1(a), the processing instructions by Customer are set out in Section 4.1 of this DPA and include onward transfers to a third party located outside Europe for the purpose of the performance of the Services.	
		In addition, where Module 3 applies, for the purposes of Clauses 8.1(a), Customer hereby informs MaintainX that it acts as Processor under the instructions of the relevant Controller in respect of Personal Data. Customer shall be solely responsible for forwarding any notifications received from MaintainX to the relevant Controller where appropriate.
Certification and Deletion *(Clauses 8.5 and 16(d))*	For the purposes of Clauses 8.5 and 16(d), the parties agree that MaintainX will provide the certification of deletion to Customer only upon Customer's written request	
Security of Processing (*Clause 8.6(c) and (d))*)	For the purposes of Clause 8.6(c), personal data breaches will be handled in accordance with Section 7 of this DPA.	
		In addition, where Module 3 applies, for the purposes of Clause 8.6(c) and (d), MaintainX shall provide notification of a personal data breach concerning Customer Personal Data Processed by MaintainX to Customer, and not to the relevant Controller.
Documentation and Compliance *(Clause 8.9) – Module 3 Only*		For the purposes of Clause 8.9, all enquiries from the relevant Controller shall be provided to MaintainX by Customer. If MaintainX receives an enquiry directly from a Controller, it shall forward the enquiry to Customer and Customer shall be solely responsible for responding to any such enquiry from the relevant Controller where appropriate.
Audits *(Clause 8.9)*	The parties agree that the audits described in Clause 8.9 shall be carried out in accordance with Section 10 of this DPA.	
Subprocessors *(Clause 9)*	Option 2 will apply and the time period for prior notice of subprocessor change shall be as set forth in Section 8.2 of this DPA. *List of Sub processors*: See Exhibit D of the DPA. The parties agree that: (i) the authorizations in Section 8.1 of this DPA shall constitute Customer's prior written consent to MaintainX's subcontracting the Processing of Customer Personal Data if such	

	consent is required under the Standard Contractual Clauses; and (ii) the parties agree that the copies of the agreements with Sub-Processors that must be provided by MaintainX to Customer pursuant to Clause 9(c) may have commercial information, or information unrelated to the Standard Contractual Clauses or their equivalent, removed by MaintainX beforehand, and that such copies will be provided by MaintainX only upon request by Customer.	
Data Subject Requests *(Clause 10) - Module 3 only*		For the purposes of Clause 10, and subject to Section 12.1 of this DPA, MaintainX shall notify Customer about any request it has received directly from a Data Subject without obligation to handle it (unless otherwise agreed), but shall not notify the relevant Controller. Customer shall be solely responsible for cooperating with the relevant Controller in fulfilling the relevant obligations to respond to any such request.
Complaints – Redress *(Clause 11)*	For the purposes of Clause 11, and subject to Section 12.1 of this DPA, MaintainX shall inform data subjects on its website of a contact point authorized to handle complaints. The optional language in Clause 11(a) shall not apply.	
Government Requests *(Clause (15(1)(a))*	For the purposes of Clause 15(1)(a), MaintainX shall notify Customer (only) and not the Data Subject(s) in case of government access requests and Customer shall be solely responsible for promptly notifying the affected Data Subjects as necessary.	
Liability *(Clause 12(b))*	MaintainX's liability under Clause 12(b) shall be limited to any damage caused by its Processing where MaintainX has not complied with its obligations under the GDPR specifically directed to Processors, or where it has acted outside of or contrary to lawful instructions of Customer, as specified in Article 82 GDPR.	
Governing Law *(Clause 17)*	Option 1 will apply, and the member state will be the Republic of Ireland.	
Choice of Forum/Jurisdiction *(Clause 18(b))*	The member state will be the Republic of Ireland.	

Appendix Information

Annex 1	*List of Parties*: As set forth in Section A (List of Parties) of Exhibit A of this DPA. By signing the Agreement or this DPA, the data exporter and data importer will be deemed to have signed Annex I.	*Description of Transfer*: The required information is set out in Exhibit A to the DPA.	*Competent Supervisory Authority*: The Irish Data Protection Commissioner.
Annex 2	The required information is set out in Exhibit B of this DPA.		

2. UK ADDENDUM

Table 1: Parties: As set forth in Section A (List of Parties) of Exhibit A of this DPA. By signing the Agreement or this DPA, the data exporter and data importer will be deemed to have signed Annex I.

Table 2: Selected SCCs, Modules and Selected Clauses:

Addendum EU SCCs	☐ The version of the Approved EU SCCs which this Addendum is appended to, detailed below, including the Appendix Information: Date: Reference (if any): Other identifier (if any): Or ☒ the Approved EU SCCs, including the Appendix Information and with only the modules, clauses or optional provisions of the Approved EU SCCs brought into effect for the purposes of this Addendum set forth in Section 1 above.

Table 3: Appendix Information

"**Appendix Information**" means the information which must be provided for the selected modules as set out in the Appendix of the Approved EU SCCs (other than the Parties), and which for this Addendum is set out in:

Annex 1A: List of Parties: *See Exhibit A of the DPA*
Annex 1B: Description of Transfer: *See Exhibit A of the DPA*
Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data: *See Exhibit B of the DPA*
Annex III: List of Sub processors (Modules 2 and 3 only): See *Exhibit D of the DPA.*

Table 4: Ending this Addendum when the Approved Addendum Changes

Ending this Addendum when the Approved Addendum changes	Which Parties may end this Addendum as set out in Section 19: ☐ Importer ☐ Exporter ☒ neither Party

Exhibit D
List of Sub-processors

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