Data Protection Addendum

1. Introduction

The Parties agree that this AutoRek Data Protection Addendum (**"DPA"**) sets forth their obligations with respect to the processing and security of Client Personal Data in connection with the Services. This DPA is incorporated by reference into the Agreement.

2. Definitions

Capitalised terms used but not defined in this DPA shall have the meaning given to them in the Agreement and Order Form as applicable.

Agreement:	the legally binding terms and conditions agreed between AutoRek and the Client (in relation to the use by the Client of Software Subscription Service) comprising the Software as a Service Agreement and any ancillary documentation referred to therein including any Order Form, and any SOW.
Business Purpose:	the purpose described in Annex A.
CCPA	California Consumer Privacy Act 2018.
Client Personal Data:	Personal Data provided by or on behalf of the Client to AutoRek and processed by AutoRek on behalf of the Client pursuant to the Agreement.
Controller:	the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of Personal Data.
Data Protection Laws:	in each case to the extent applicable (a) the UK GDPR; (b) the Data Protection Act 2018 to the extent that it relates to processing of Client Personal Data and privacy; (c) any United States federal, state, or local laws governing the privacy, confidentiality, retention, security, or processing of Client Personal Data and any other applicable law or regulation related to the protection of Client Personal Data; (d) all Laws about the processing of Client Personal Data and privacy which are applicable to AutoRek's provision of the Services; and (e) (to the extent that it applies) the EU GDPR.
Data Protection Audit:	an audit carried out by or on behalf of the Client pursuant to paragraph 4 (Data Protection Terms) of this DPA.
Data Subjects:	shall have the meaning given to it in the Data Protection Laws.
EU GDPR:	General Data Protection Regulation 2016/679
Law:	any law, statute, subordinate legislation within the meaning of Section 21(1) of the Interpretation Act 1978, bye-law, right within the meaning of the European Union (Withdrawal) Act 2018 as amended

	by European Union (Withdrawal Agreement) Act 2020, regulation, order, regulatory policy, mandatory guidance or mandatory code of practice, judgment of a relevant court of law, or directives or mandatory requirements of any regulatory body with which AutoRek is bound to comply.
Personal Data:	shall have the meaning given to it in the Data Protection Laws, in each case to the extent applicable.
Personal Data Breach	shall have the meaning given to it in the Data Protection Laws, in each case to the extent applicable.
Processor:	shall have the meaning given to it in the Data Protection Laws, in each case to the extent applicable.
Regulator:	The European Data Protection Board, the UK's Information Commissioner's Office (in the case of the United Kingdom) and/or any other supervisory authority or data protection authority or any other regulator (including a financial regulator) or court, in each case to the extent applicable under Data Protection laws.
UK GDPR:	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 (United Kingdom General Data Protection Regulation), as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018, together with the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019.

3. General Terms

3.1 AutoRek will comply with all laws and regulations applicable to its providing the Services. However, AutoRek is not responsible for compliance with any laws or regulations applicable to the Client or the Client's industry that are not generally applicable to AutoRek or the Services. AutoRek does not determine whether the Client's data includes information subject to any specific law or regulation other than the Data Protection Laws.

3.2 The Client must comply with all laws and regulations applicable to its use of AutoRek products and services including laws related to Personal Data, confidentiality of communications, and requirements of data protection laws. The Client is responsible for determining whether the Services are appropriate for storage and processing of information subject to any specific law or regulation and for using the Services in a manner consistent with the Client's legal and regulatory obligations. The Client is responsible for responding to any request from a third party regarding the Client's use of AutoRek's Services.

4. Data Protection Terms

4.1 Parties

4.1.1 The Client and AutoRek agree and acknowledge that for the purpose of Data Protection Laws:

a. The Client is the Controller, Business (as defined under CCPA) or equivalent, and AutoRek is the Processor, Service Provider (as defined under CCPA) or equivalent;

b. The Client retains control of the Personal Data and remains responsible for its compliance obligations under the Data Protection Laws, including but not limited to, providing any required notices to and obtaining any required consents of Data Subjects, and for the written processing instructions it gives to AutoRek.

4.2 **Client's Obligations**

4.2.1 The Client:

a. warrants that it has and will maintain all necessary appropriate consents and notices to enable the lawful transfer of Personal Data to AutoRek and shall only transfer Personal Data to AutoRek to the extent required to fulfil the purpose defined in Annex A;

b. agrees that it is solely responsible for the accuracy, quality, and legality of (i) the Personal Data provided to AutoRek by or on behalf of Client, (ii) the means by which Client acquired any such Personal Data, including providing notice and obtaining all consents and rights necessary for AutoRek to process Personal Data pursuant to the Agreement and this DPA, and (iii) the instructions it provides to AutoRek regarding the Processing of such Personal Data. Client shall not provide or make available to AutoRek any Personal Data in violation of Data Protection Laws or the Agreement or otherwise inappropriate for the nature of the Services, and shall indemnify AutoRek from all claims and losses in connection therewith

c. shall at all times comply with data protection and privacy laws applicable to it insofar as they relate to the Agreement or the receipt of the Services;

d. shall not instruct AutoRek in such a way that shall or is likely to breach the Data Protection Laws. In particular, Client shall ensure that its instructions comply with all Data Protection Laws, and that the processing of Personal Data in accordance with Client's instructions will not cause AutoRek to be in breach of the Data Protection Laws.

4.3 **AutoRek's Obligations**

4.3.1 AutoRek shall:

a. only process the Client Personal Data to the extent, and in such a manner, as is necessary for the Business Purposes in accordance with the Client's written instructions and this DPA shall constitute such documented initial instructions. AutoRek will not process the Client Personal Data for any other purpose or in a way that does not comply with this DPA or the applicable Data Protection Laws. AutoRek shall promptly notify the Client if, in its opinion, the Client's instructions do not comply with the Data Protection Laws;

b. notify Client if a Client instruction, in AutoRek's opinion, infringes the Data Protection Laws.

c. take commercially reasonable measures designed to maintain the confidentiality of the Client Personal Data and ensure that persons authorized to process the Client Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality. AutoRek will not disclose the Client Personal Data to third-parties unless the Client or the Agreement specifically authorizes the disclosure, or as required by Data Protection Laws, court or regulator. If Data Protection Laws, court or Regulator requires AutoRek to process or disclose the Client Personal Data to a third-party, AutoRek shall first inform the Client of such legal or regulatory requirement and give the Client an opportunity to object or challenge the requirement, unless the Data Protection Law prohibits the giving of such notice;taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, implement appropriate technical and organisational measures against accidental,

unauthorized or unlawful processing, access, copying, modification, reproduction, display or distribution of the Client Personal Data, and against accidental or unlawful loss, destruction, alteration, disclosure or damage of Personal Data including, but not necessarily limited to, the security measures set out in the AutoRek Security Addendum (**"Technical and Organizational Measures"**). Individual security measures may be replaced by new measures that serve the same purpose without diminishing the security level protecting the Personal Data;

d. Without prejudice to AutoRek's obligations in paragraph c above, the Client is responsible for reviewing the information made available by AutoRek relating to data security and making an independent determination as to whether the AutoRek Services meet Client's requirements and legal obligations under Data Protection Laws. Client acknowledges that the Technical and Organizational Measures are subject to technical progress and development and that AutoRek may update or modify the Technical and Organizational Measures from time to time. Client agrees that except as provided by this DPA, Client is responsible for its secure use of the Services, including securing its account authentication credentials, protecting the security of Personal Data when in transit to and from the AutoRek services, and taking any appropriate steps to securely encrypt or backup any Personal Data uploaded to such services.

e. This Section 4.3(e) shall apply if and only to the extent that any Personal Data is subject to the CCPA. As used in this Section, the terms "Sell," "Share," "Business Purpose," and "Commercial Purpose" shall have the meanings given to them in the CCPA. AutoRek will not: (a) Sell or Share any Personal Data; (b) retain, use, or disclose any Personal Data (i) for any purpose other than for the Business Purposes specified in the Agreement, namely for AutoRek to provide recurring billing and payments management and such other services for Client's use, (ii) unless otherwise permitted by the CCPA, for any Commercial Purpose other than the Business Purposes specified in the Agreement, or (iii) unless otherwise permitted by the CCPA, outside of the direct business relationship between Client and AutoRek. AutoRek will comply with applicable obligations under the CCPA and provide the same level of privacy protection to Personal Data as is required by Client under the CCPA. Either party will notify the other party if it makes a determination that the party can no longer meet its obligations under the CCPA. If and only to the extent that AutoRek notifies Client of unauthorized use of Personal Data, Client will have the right to take reasonable and appropriate steps to stop and remediate such unauthorized use. Nothing in this Section 4.3(h) shall limit AutoRek's right to use Personal Data as permitted for Processors under Data Protection Laws.

4.4 **Personal Data Breach**

4.4.1 AutoRek shall notify the Client without undue delay after becoming aware of a Personal Data Breach.

4.4.2 Such notification shall at least:

a. describe the nature of the Personal Data Breach including where possible, the categories and approximate number of Data Subjects concerned and the categories and approximate number of Client Data records concerned;

b. communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;

c. describe the measures taken or proposed to be taken by AutoRek to address the Personal Data Breach, including, where appropriate, measures to mitigate its possible adverse effects.

4.5 **Cross-Border Transfers of Personal Data**

4.5.1 To the extent a transfer of data would be deemed a restricted transfer within the meaning of Data Protection Law, AutoRek shall not transfer or otherwise process Client Personal Data outside the UK to any country that has not received an adequacy decision unless AutoRek participates in a valid cross-border transfer mechanism under the Data Protection Laws and AutoRek has informed the Client and given the Client reasonable details regarding the basis of the transfer and a reasonable opportunity to object to the transfer. The Client understands and agrees that the Hosting Services are provided by the Hosting Provider. Where there is an obligation on the Hosting Provider to do or omit to do anything, AutoRek shall procure such obligation from the Hosting Provider. AutoRek has no authority to bind the Hosting Provider pursuant to this DPA or the Agreement. Where Microsoft is the Hosting Provider, Client Personal Data is transferred outside of the UK. In such event, all transfers of Client Personal Data out of the European Union, European Economic Area, United Kingdom, and Switzerland to provide the Hosting Services shall be governed by the 2021 Standard Contractual Clauses implemented by the Hosting Provider. In addition, transfers from the United Kingdom shall be governed by the IDTA implemented by the Hosting Provider. For purposes of this DPA, the "IDTA" means the International data transfer addendum to the European Commission's standard contractual clauses for international data transfers issued by the UK Information Commissioner's Office under S119A(1) of the UK Data Protection Act 2018. The Hosting Provider will abide by the requirements of European Economic Area, United Kingdom, and Swiss data protection law regarding the collection, use, transfer, retention, and other processing of Personal Data from the European Economic Area, United Kingdom, and Switzerland. All transfers of Personal Data to a third country or an international organization will be subject to appropriate safeguards as described in Article 46 of the GDPR and such transfers and safeguards will be documented according to Article 30(2) of the GDPR. In addition, the Hosting Provider is certified to the EU-U.S. and Swiss-U.S. Data Privacy Frameworks and the commitments they entail.

4.5.2 Where such notification has been provided in accordance with paragraph 4.5.1, AutoRek or any sub-processor appointed by AutoRek may only process Client Personal Data outside the UK under the following conditions:

a. AutoRek is processing the Client Personal Data in a territory which is subject to adequacy regulations under the Data Protection Laws that the territory provides adequate protection for the privacy rights of individuals; or

b. AutoRek participates in a valid cross-border transfer mechanism under the Data Protection Laws, so that AutoRek (and, where appropriate, the Client) can ensure that appropriate safeguards are in place to ensure an adequate level of protection with respect to the privacy rights of individuals as required by Article 46 of the UK GDPR and EU GDPR.

4.6 Sub-processors

4.6.1 AutoRek may only authorize a third-party (Sub-processor) to process the Client Personal Data if:

a. the Client provides written consent prior to the appointment of each subcontractor or is provided with an opportunity to object to the appointment of each sub-processor within 10 Business Days after AutoRek supplies the Client with full details in writing regarding such Sub-processor;

b. AutoRek enters into a written contract with the Sub-processor that contains terms as referred to in Article 28(3) of the UK GDPR, in particular, in relation to requiring appropriate technical and organisational data security measures, and, upon the Client's written request, provides the Client with copies of the relevant excerpts from such contracts;

4.6.2 Those Sub-processors approved as at the commencement of this DPA are as set out in Annex A.

4.7 Data Subject Requests and Third-Party Rights

4.7.1 AutoRek shall, take such technical and organisational measures as may be appropriate taking into account the nature of processing and the information available to AutoRek, and promptly provide such information to the Client as the Client may reasonably require in respect of the Client Personal Data, to assists the Client in complying with:

a. the rights of Data Subjects under the Data Protection Laws, including where applicable subject access rights, the rights to rectify, port and erase personal data, object to the processing and automated processing of Personal Data, and restrict the processing of Personal Data; and

b. information or assessment notices served on the Client by the Commissioner or other relevant regulator under the Data Protection Laws.

4.7.2 AutoRek shall notify the Client if it receives a request from a Data Subject for access to their Client Personal Data or to exercise any of their other rights under the Data Protection Laws.

4.7.3 AutoRek will give the Client all reasonable co-operation and assistance in responding to any complaint, notice, communication or Data Subject request.

4.8 Data Return and Destruction

4.8.1 On termination of the Agreement for any reason or expiry of its term, AutoRek will, subject to its reasonable and customary data retention and business continuity practices, securely delete or destroy or, if directed in writing by the Client, return and not retain, all or any of the Personal Data related to this DPA in its possession or control.

4.8.2 If any law, regulation, or government or regulatory body requires AutoRek to retain any documents or materials or Client Personal Data that the AutoRek would otherwise be required to return or destroy, it will notify the Client in writing of that retention requirement, giving details of the documents, materials or Client Personal Data that it must retain, unless AutoRek is prohibited from doing so by law or regulation.

4.9 Records

4.9.1 AutoRek will keep detailed, accurate and up-to-date written records regarding any processing of the Client Personal Data, including but not limited to, the access, control and security of the Client Personal Data, the processing purposes, categories of processing, any transfers of personal data to a third country and related safeguards, and a general description of the technical and organisational security measures in place in respect of the Client Personal Data (**"Records"**).

4.9.2 Upon written request from the Client, AutoRek shall make available to the Client all information necessary to demonstrate compliance with AutoRek's obligations in this DPA.

4.10 Audit

4.10.1 To the extent the Client's audit requirements under the Data Protection Laws cannot reasonably be satisfied through audit reports, documentation or compliance information AutoRek makes available to the Client, AutoRek will promptly respond to the Client's additional audit instructions. Before the commencement of an audit, the Client and AutoRek will mutually agree upon the scope, timing, duration, control and evidence requirements, provided that this requirement to agree will not permit AutoRek to unreasonably delay performance of the audit. All audits shall be conducted during AutoRek's ordinary business hours and in a non-disruptive manner.

4.10.2 To the extent needed to perform the audit, AutoRek will make the processing systems, facilities and supporting documentation relevant to the processing of Client Personal Data by AutoRek available. Such an audit will be conducted by an independent, accredited third-party audit firm, during regular business hours, subject to reasonable confidentiality procedures.

4.10.3 Neither the Client nor the auditor shall have access to any data from AutoRek's other clients or to AutoRek systems or facilities not involved in providing the applicable Services. Each Party shall bear their own costs related to such audit. If the audit report generated as a result of the Client's audit includes any finding of material non-compliance with this DPA, the Client shall share such audit report with AutoRek and AutoRek shall promptly cure any confirmed material non-compliance.

4.10.4 The Client shall conduct no more than one (1) Data Protection Audit in any twelve (12) month period and shall provide at least thirty (30) days' notice (or such lesser notice prescribed by Data Protection Law) of its intention to conduct a Data Protection Audit unless such Data Protection Audit is conducted: by or upon the request of a Data Protection Regulator, in which case the Client shall give AutoRek such notice as is reasonably practicable and to the extent notice is permitted by the Data Protection Regulator or Data Protection Laws), and in no such case shall such Data Protection Audits count toward the maximum of one (1) audit in any twelve (12) month period.

4.11 Warranties

4.11.1 AutoRek warrants that:

a. AutoRek employees, subcontractors, agents and any other person or persons accessing the Client Personal Data on its behalf have received the required training on the Data Protection Laws;

b. Subject to Section 4.2, AutoRek has no reason to believe that the Data Protection Laws prevent it from providing any of the contracted Services; and

4.11.2 The Client warrants and represents that AutoRek's processing of the Client Personal Data for the Business Purpose and as specifically instructed by the Client will comply with the Data Protection Laws.

4.12 **Liability**

The total liability of each of Client and AutoRek (and their respective employees, directors, officers, affiliates, successors, and assigns), arising out of or related to this DPA, whether in contract, tort, or other theory of liability, shall not, when taken together in the aggregate, exceed the limitation of liability set forth in the Agreement. Client **further** agrees that any regulatory penalties or fines incurred by AutoRek in relation to the Personal Data that arise as a result of, or in connection with, Client's failure to comply with its obligations under this DPA or any applicable Data Protection Laws shall be subject to Client's indemnification obligations under the Agreement.

5. Contact Details

If you have a query in respect of this DPA, please contact:

dpo@autorek.com

cc: legal@autorek.com
Data Protection Office
API Software Limited
10 Montrose Street
Glasgow G1 1RE
United Kingdom
Tel: 0141 229 5300

Annex A

Scope	This DPA only apply to the processing of Client Personal Data in environments controlled by AutoRek and if applicable, AutoRek sub-processors.
Nature and Purpose of Processing	AutoRek will process Client Personal Data only as described and subject to the limitations below (a) to provide the Client with the Services in accordance with the Client's documented instructions and (b) for business operations incidental to providing the Services to the Client. As between the parties, the Client retains all right, title and interest in and to the Client Personal Data. For the purposes of this DPA, to "provide" the Services consists of: • delivering the functional capabilities of the Software Subscription Service; • delivering Professional Services • providing Support Services • keeping the Software Subscription Services up to date including by maintaining security; • trouble shooting (preventing, detecting, investigating, mitigating and repairing problems) For the purposes of this DPA, to "provide" business operations ancillary to the Services consists of: • to create aggregated statistical, non-personal data from data containing pseudonymized identifiers (such as usage logs) • To calculate statistics related to Client Personal Data; • Account Management; • Financial Reporting
Duration of Processing	The duration of the processing shall be in accordance with Client instructions and the terms of this DPA.
Categories of Data Processing	The types of Personal Data processed by AutoRek when providing the Services pursuant to the Agreement including: [Personal Data the Client elects to include in the Client Personal Data and Personal Data that AutoRek requires to provide the Services and business operations which are ancillary to providing the Services including: • Client Staff and Client customers names • Client Staff Contact Details (telephone numbers, email address, address, contact preferences) • Client Customers financial data ((transaction data, date and time of transaction, amount, description, debit/credit (excluding card numbers unless expressly agreed otherwise between AutoRek and the Client in writing), account numbers, and account names, institutions, assets, values etc); • technical data related to IP, location, system access/usage of Client staff;

<table>
<tr><td>Data Subjects</td><td colspan="4">The categories of data subjects are the Client’s representatives and end users such as existing or prospective staff, the Client’s existing or prospective customers and may include any other categories of data subject as identified in records maintained by the Client acting as Controller pursuant to Article 30 of the GDPR.</td></tr>
<tr><td rowspan="6">Approved Sub-Processors</td><td colspan="4">The Client Order Form confirms the Hosting Provider applicable to the Client.
In the case of: API Software Limited</td></tr>
<tr><td>Legal Entity</td><td>Address</td><td>Location of Processing</td><td>Processing Activity</td></tr>
<tr><td>Microsoft Ireland Operations Limited</td><td>70 SIR JOHN ROGERSON'S QUAY, DUBLIN 2, DUBLIN, D02R296</td><td>UK</td><td>Provision of Data Centres, network and Platforms;
Configuration, support, and network & systems administration of Platforms, Data Centres and related Cloud Infrastructure.</td></tr>
<tr><td colspan="4">In the case of: API Software Inc.</td></tr>
<tr><td>Legal Entity</td><td>Address</td><td>Location of Processing</td><td>Processing Activity</td></tr>
<tr><td>Microsoft Ireland Operations Limited</td><td>70 SIR JOHN ROGERSON'S QUAY, DUBLIN 2, DUBLIN, D02R296</td><td>USA</td><td>Provision of Data Centres, network and Platforms;
Configuration, support, and network & systems administration of Platforms, Data Centres and related Cloud Infrastructure.</td></tr>
</table>