Servicemax Data Processing Addendum

(Version date: July 28, 2023)

This ServiceMax Data Processing Addendum ("**DPA**") is an addendum to the ServiceMax Hosted Services Terms ("**Agreement**") between ServiceMax, Inc. ("**ServiceMax**") and the entity that accepted the Agreement. This DPA is effective simultaneously with the Agreement ("**DPA Effective Date**") and applies to Customer's use of ServiceMax Services ("**Services**").

This DPA reflects the Parties' agreement regarding the Processing of Personal Data. By agreeing to the Agreement, Customer enters this DPA on behalf of itself and, to the extent required under Applicable Privacy Laws, in the name of and on behalf of its Authorized Affiliates, if and to the extent ServiceMax and its applicable Affiliates processes Personal Data for which such Authorized Affiliates qualify as the Controller. For the purposes of this DPA only, and except when indicated otherwise, the term "**Customer**" shall include Customer and its Authorized Affiliates. All capitalized terms not defined in this DPA have the meaning stated in the Agreement. In providing the Services to Customer pursuant to the Agreement, ServiceMax and its applicable Affiliates may Process Personal Data on behalf of Customer and the parties agree to comply with the following provisions with respect to any Personal Data, each acting reasonably and in good faith. The parties' liability under this DPA will be as stated in the Agreement.

1. Definitions

1.1. "**Affiliate**" has the meaning stated in the Agreement.

1.2. "**Applicable Privacy Law**" means applicable data privacy, data protection, and cybersecurity laws, rules and regulations to which ServiceMax is subject, including, but not limited to; (a) the California Consumer Privacy Act of 2018 ("**CCPA**"); (b) the EU General Data Protection Regulation 2016/679 ("**EU GDPR**") including the applicable implementing legislation of each member state; (c) the UK Data Protection Act 2018, and the UK General Data Protection Regulation ("**UK GDPR**", and together with the EU GDPR, the "**GDPR**"); (d) the Swiss Federal Act on Data Protection of 19 June 1992; (e) any other applicable law with respect to any Personal Data in respect of which Customer is subject to; and (f) any other data protection law and any guidance or statutory codes of practice issued by any relevant Privacy Authority, in each case, as amended from time to time and any successor legislation to the same.

1.3. "**Authorized Affiliate**" means any of Customer's Affiliates that: (a) are subject to Applicable Privacy Laws; and (b) are permitted to use the Services pursuant to the Agreement between Customer and ServiceMax but have not signed their own Sales Order with ServiceMax and are not a "Customer" as defined under the Agreement.

1.4. "**Controller**" means the entity which determines the purposes and means of the Processing of Personal Data.

1.5. "**Customer Data**" has the meaning stated in the Agreement.

1.6. "**Data Protection Plan Documentation**" means the ServiceMax Data Protection Plan applicable to the specific Services purchased by Customer, as updated by ServiceMax from time to time. The Data Protection Plan Documentation is available at https://www.servicemax.com/trust/security or a successor webpage/website that ServiceMax may publish.

1.7. "Data Breach" means an incident that has resulted in a compromise of the security, confidentiality, availability or integrity of Personal Data resulting in the unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer Data.

1.8. "**Data Subject**" means the identified or identifiable person to whom Personal Data relates.

1.9. "**Personal Data**" means: (a) Personal Data, personal information, personally identifiable information, or similar term as defined by Applicable Privacy law; or (b) if not defined by Applicable Privacy Law, any information that relates to a Data Subject, in each of (a) and (b), to the extent Processed by or on behalf of ServiceMax, in connection with ServiceMax's performance of the agreement into which this DPA is incorporated.

1.10. "**Privacy Authority**" means any competent supervisory authority, attorney general, or other regulator with responsibility for privacy or data protection matters in the jurisdiction of Customer.

1.11. "**Processing**" means any operation or set of operations which is performed upon Personal Data, whether by automatic means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction.

1.12. "**Processor**" means the entity which Processes Personal Data on behalf of the Controller.
1.13. "**Sales Order**" has the meaning stated in the Agreement.
1.14. "**ServiceMax Group**" means ServiceMax and its Affiliates, if any, engaged in the Processing of Personal Data.
1.15. "**Standard Contractual Clauses**" means (a) with respect to restricted transfers (as such term is defined under Applicable Privacy Law) which are subject to the GDPR and other Applicable Privacy Laws pursuant to which the same have been adopted, the Controller-to-Processor standard contractual clauses, as set out in the European Commission's Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of Personal Data to third countries pursuant to GDPR, as may be amended or replaced by the European Commission from time to time (the "**EU Clauses**"), and (b) with respect to restricted transfers subject to the UK GDPR, the International Data Transfer Addendum to the EU Commission Standard Contractual of 21 March 2022, as may be amended or replaced by the UK Information Commissioner's Office from time to time (the "**UK Clauses**").
1.16. "**Sub-processor"** means any Processor engaged by ServiceMax or a member of the ServiceMax Group.

2. Processing of Personal Data

2.1. Roles of the Parties**.** The parties acknowledge and agree that, regarding the Processing of Personal Data, Customer is the Controller, ServiceMax is the Processor and that ServiceMax or members of the ServiceMax Group will engage Sub-processors pursuant to the requirements set forth in Section 5 (Sub-processors) below.
2.2. Customer's Processing of Personal Data**.** Customer shall, in its use of the Services, Process Personal Data in accordance with the requirements of Applicable Privacy Laws. All Customer instructions for the Processing of Personal Data must comply with Applicable Privacy Laws, and ServiceMax has no obligation to comply with any Customer instruction that does not comply with Applicable Privacy Laws. Customer is solely responsible for the accuracy, quality, and legality of Personal Data, how Customer acquired Personal Data, the provision of any required notices to, and consents from, Data Subjects relating to ServiceMax's processing of Personal Data on behalf of Customer, including ensuring any transfer of Personal Data to ServiceMax is in accordance with Applicable Privacy Law.
2.3. Additional Customer Obligations. To the extent ServiceMax's provision of the Services requires implementation of mapping technologies, Customer shall comply with the applicable requirements set forth in the terms of the applicable map provider, as indicated in the Sub-processor List in Annex 3.
2.4. Sensitive Personal Data. The Services are not intended to process Personal Data that is considered 'special category' or 'sensitive' Personal Data under Applicable Privacy Law (collectively "Sensitive Personal Data"). Customers are not permitted to input Sensitive Personal Data into the Services (including via any free form text fields). To the extent Customer does input Sensitive Personal Data into the Services, it does so at its own risk and ServiceMax is not responsible, and accepts no liability, for processing of Sensitive Personal Data over and above its general obligations as set forth in this DPA.
2.5. ServiceMax's Processing of Personal Data**.** ServiceMax will treat Personal Data as confidential and shall only Process Personal Data on behalf of and in accordance with Customer's documented instructions for the following purposes: (a) Processing in accordance with the Agreement and applicable Sales Order(s); (b) Processing initiated by Users in their use of the Services; and (c) Processing to comply with other documented reasonable instructions provided by Customer (e.g., via email) where such instructions are consistent with the terms of the Agreement.
2.6. Details of the Processing**.** The subject-matter of Processing of Personal Data by ServiceMax is the performance of the Services pursuant to the Agreement. The duration of the Processing, the nature and purpose of the Processing, the types of Personal Data and categories of Data Subjects Processed under this DPA are further specified in Annex 1 of Schedule 1 to this DPA.
2.7. CCPA. ServiceMax acknowledges that: (a) Customer discloses Personal Data to ServiceMax solely for the business purpose of Customer; and (b) ServiceMax has not and will not receive any monetary or other valuable consideration in exchange for its receipt of the Personal Data, and that any consideration paid by Customer to ServiceMax under the Agreement relates only to ServiceMax's provision of the Services. ServiceMax shall not collect, retain, use, disclose, or otherwise Process the Personal Data (i) for any purpose other than for the specific purpose of providing the Services to Customer, or (ii) outside of the direct business relationship between Customer and ServiceMax. In addition, ServiceMax shall not 'sell,' as defined under Applicable Privacy Law (including,

without limitation, CCPA), or otherwise disclose any Personal Data except to authorized Sub-processors needed to render the Services.

3. **Data Subject Requests.** ServiceMax shall, to the extent legally permitted, promptly notify Customer if ServiceMax receives a request from a Data Subject to exercise the Data Subject's right under Applicable Privacy Laws ("**Data Subject Request**"). Considering the nature of the Processing, ServiceMax shall assist Customer by appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of Customer's obligation to respond to a Data Subject Request under Applicable Privacy Laws. In addition, to the extent Customer, in its use of the Services, does not have the ability to address a Data Subject Request, ServiceMax shall upon Customer's request provide commercially reasonable efforts to assist Customer in responding to such Data Subject Request, to the extent ServiceMax is legally permitted to do so and the response to such Data Subject Request is required under Applicable Privacy Laws. To the extent legally permitted, Customer shall be responsible for any costs arising from ServiceMax's provision of such assistance.

4. **ServiceMax Personnel**

4.1. Confidentiality**.** ServiceMax shall ensure that its personnel engaged in the Processing of Personal Data are informed of the confidential nature of the Personal Data, have received appropriate training on their responsibilities and have executed written confidentiality agreements. ServiceMax shall ensure that such confidentiality obligations survive the termination of the personnel engagement.

4.2. Reliability**.** ServiceMax shall take commercially reasonable steps to ensure the reliability of any ServiceMax personnel engaged in the Processing of Personal Data.

4.3. Limitation of Access**.** ServiceMax shall ensure that ServiceMax personnel access to Personal Data is limited to those personnel performing Services in accordance with the Agreement.

5. **Sub-processors**

5.1 Appointment of Sub-processors**.** Customer acknowledges and agrees that: (a) ServiceMax's Affiliates may be retained as Sub-processors; and (b) ServiceMax and ServiceMax's Affiliates respectively may engage third-party Sub-processors in connection with the provision of the Services. ServiceMax or a ServiceMax Affiliate has entered or will enter into a written agreement with each Sub-processor containing data protection obligations not less protective than those in this Agreement with respect to the protection of Customer Data to the extent applicable to the nature of the Services provided by such Sub-processor.

5.2 General Authorization**.** Customer authorizes ServiceMax to engage the Sub-processors specified in Annex 3 of Schedule 1.

5.3 Objection Right for New Sub-processors**.** Customer may object to ServiceMax's use of a new Sub-processor by notifying ServiceMax promptly in writing within 10 days after receipt of ServiceMax notifying Customer of a new Sub-processor. If Customer objects to a new Sub-processor, as permitted in the preceding sentence, ServiceMax will use reasonable efforts to make available to Customer a change in the Services or recommend a commercially reasonable change to Customer's configuration or use of the Services to avoid Processing of Personal Data by the objected-to new Sub-processor without unreasonably burdening Customer. If ServiceMax is unable to make available such change within a reasonable time, which shall not exceed 30 days, Customer may terminate the applicable Sales Order(s) with respect only to those Services which cannot be provided by ServiceMax without the use of the objected-to new Sub-processor by providing written notice to ServiceMax. ServiceMax will refund Customer any prepaid fees covering the remainder of the term of such Sales Order(s) following the effective date of termination with respect to the terminated Services, without imposing a penalty for such termination on Customer.

5.4 Liability**.** ServiceMax shall be liable for the acts and omissions of its Sub-processors to the same extent ServiceMax would be liable if performing the services of each Sub-processor directly under the terms of this DPA, except as otherwise set forth in the Agreement.

6. **Security**

6.1 Controls for the Protection of Customer Data**.** ServiceMax shall maintain appropriate technical and organizational measures for protection of the security (including protection against unauthorized or unlawful Processing and against accidental or unlawful destruction, loss or alteration or damage, unauthorized disclosure of,

or access to, Customer Data), confidentiality and integrity of Customer Data, as set forth in Annex II of Schedule 1 and the Data Protection Plan Documentation. ServiceMax regularly monitors compliance with these measures. ServiceMax will not materially decrease the overall security of the Services during a subscription term.

6.2 Third-Party Certifications and Audits**.** Third-party certifications and audits have been obtained for the Services. Upon Customer's written request at reasonable intervals, and subject to the confidentiality obligations set forth in the Agreement, ServiceMax shall make available to Customer (or Customer's independent, third-party auditor that is not a competitor of ServiceMax) a copy of ServiceMax's (or, as applicable, its Sub-processor's) then most recent third-party audits or certifications, as applicable. Customer may contact ServiceMax in accordance with the "Notices" Section of the Agreement to request an audit of the procedures relevant to the protection of Personal Data commencing on a mutually agreed date. Customer may request an audit no more frequently than once each calendar year. Customer shall reimburse ServiceMax for any time expended for any audit at the ServiceMax Group's then-current professional services rates, which shall be made available to Customer upon request. Before the commencement of any such audit, Customer and ServiceMax shall mutually agree upon the scope, timing, and duration of the audit in addition to the reimbursement rate for which Customer shall be responsible. Customer shall promptly provide to ServiceMax a copy of any reports by the auditors and ServiceMax may reasonably dispute any findings. In that event, Customer and ServiceMax will confer to resolve the concerns.

7. Notification of Data Breach

7.1 ServiceMax has implemented controls and policies designed to detect and promptly respond to incidents that may constitute a Data Breach. ServiceMax will promptly define escalation paths to investigate such incidents in order to confirm if a Data Breach has in fact occurred, and to take reasonable measures designed to identify the root cause(s) of the Data Breach, mitigate any possible adverse effects and prevent a recurrence. In the event of a Data Breach and taking into account the nature of Processing and the information available, ServiceMax shall cooperate with and assist Customer to comply with its obligations under Applicable Law.

7.2 In the event of a Data Breach, ServiceMax shall notify Customer without undue delay and in any event within 72 hours of ServiceMax becoming aware of the Data Breach. Where possible, such notification shall contain, at least:

(a) "What Happened," a description of the nature of the Data Breach, the date and time at which it was first identified, and its likely consequences to the extent known;

(b) "What Information Was Involved," where possible, the nature of the Personal Data affected, the categories and approximate number of Individuals and data records concerned where known;

(c) "What We Are Doing," the measures taken or proposed to be taken to address the Data Breach, including to mitigate its possible adverse effects;

(d) "What You Can Do" being measures that ServiceMax recommends Customer take to mitigate the effect of the Data Breach;

(e) "For More Information" the details of a contact point where more information concerning the Data Breach can be obtained.

7.3 Where, and insofar as, it is not possible to provide all this information at the same time, further information shall be provided, as it becomes available, without undue delay.

7.4 Unless required by Applicable Law, ServiceMax shall not notify any individual or any third party other than law enforcement, forensic investigators, insurance providers or legal counsel of Customer's name or identity in association with any Data Breach without first consulting with, and obtaining Customer's written consent, which shall not be unreasonably denied. To the extent the Data Breach impacts other customers of ServiceMax, a general public statement may be made as long as Customer's identity is not disclosed.

8. **Data Protection Impact Assessments**. To the extent required under Applicable Privacy Law and upon Customer's request, ServiceMax shall provide Customer with reasonable cooperation and assistance needed to fulfil Customer's obligation under Applicable Privacy laws to carry out a data protection impact assessment related to Customer's use of the Services, to the extent Customer does not otherwise have access to the relevant information, and to the extent such information is available to ServiceMax. ServiceMax shall provide reasonable assistance to Customer in the cooperation or prior consultation with a Privacy Authority, to the extent required under Applicable Privacy Laws.

9. **Return and Deletion of Customer Data.** ServiceMax deletes Customer Data within 30 days after a Customer terminates its agreement with ServiceMax, consistent with the Salesforce timeframe.

10. Authorized Affiliates

10.1. Contractual Relationship**.** The parties acknowledge and agree that, by executing the Agreement, the Customer enters the DPA on behalf of itself and, as applicable, in the name and on behalf of its Authorized Affiliates, thereby establishing a separate DPA between ServiceMax and each such Authorized Affiliate subject to the provisions of the Agreement and this Section 10 and Section 11 below. Each Authorized Affiliate agrees to be bound by the obligations under this DPA and, to the extent applicable, the Agreement. For clarity, an Authorized Affiliate is not and does not become a party to the Agreement unless it separately executes a Sales Order and is only a party to the DPA. All access to and use of the Services by Authorized Affiliates must comply with the terms and conditions of the Agreement and any violation of the terms and conditions of the Agreement by an Authorized Affiliate shall be deemed a violation by Customer.

10.2. Communication**.** The Customer that is the contracting party to the Agreement shall remain responsible for coordinating all communication with ServiceMax under this DPA and be entitled to make and receive any communication in relation to this DPA on behalf of its Authorized Affiliates.

10.3. Rights of Authorized Affiliates**.** When an Authorized Affiliate becomes a party to the DPA with ServiceMax, it shall to the extent required under Applicable Privacy Laws be entitled to exercise the rights and seek remedies under this DPA, subject to the following:

10.3.1. Except when Applicable Privacy Laws require the Authorized Affiliate to exercise a right or seek any remedy under this DPA against ServiceMax directly by itself, the parties agree that: (a) solely the Customer that is the contracting party to the Agreement shall exercise any such right or seek any such remedy on behalf of the Authorized Affiliate; and (b) the Customer that is the contracting party to the Agreement shall exercise any such rights under this DPA not separately for each Authorized Affiliate individually but in a combined manner for all of its Authorized Affiliates together (as set forth, for example, in Section 10.3.2, below).

10.3.2. The parties agree that the Customer that is the contracting party to the Agreement shall, when carrying out an audit of the procedures relevant to the protection of Personal Data, take all reasonable measures to limit any impact on ServiceMax and its Sub-Processors by combining, to the extent reasonably possible, several audit requests carried out on behalf of different Authorized Affiliates in one single audit. If there are multiple audits, each audit will be subject to the audit terms stated in this DPA.

11. European and United Kingdom Specific Provisions

11.1 GDPR**.** ServiceMax will Process Personal Data in accordance with GDPR requirements directly applicable to ServiceMax's provision of its Services.

11.2 Transfer Impact Assessment. In accordance with obligations under GDPR, ServiceMax has completed a Transfer Impact Assessment, which is incorporated herein as Schedule 2.

12. Transfer Mechanisms for Data Transfers

12.1. Standard Contract Clauses**.** The Parties acknowledge and agree that, to the extent a transfer of Personal Data under this DPA is considered a restricted transfer with respect to which the Standard Contractual Clauses constitute a valid transfer mechanism, the Parties shall undertake such transfer pursuant to the applicable Standard Contractual Clauses, the terms of which are hereby incorporated into this DPA by reference.

12.2. Transfers out of the EEA. If Customer transfers Personal Data out of the EEA to ServiceMax in a country not deemed by the European Commission to have adequate data protection, such transfer will be governed by the EU Clauses, the terms of which are hereby incorporated into this DPA. In furtherance of the foregoing, the Parties agree that:

- Customer will act as the data exporter, and ServiceMax will act as the data importer under the EU Clauses;
- For purposes of Annex I to the EU Clauses, the categories of data subjects, data, special categories of data (if appropriate), and the Processing operations shall be as set out in Annex 1 of this DPA;
- For purposes of Annex II to the EU Clauses, the technical and organizational measures shall be as set out in Annex 2 of this DPA;
- The optional docking clause in Clause 7 of the EU Clauses shall be included;
- The audits described in Clause 8.9 of the EU Clauses shall be performed in accordance with Section 6.2 (Third-Party Certifications and Audits) of this DPA;
- Section 5 (Sub-processors) of this DPA shall constitute the procedures with regard to authorization for Sub-processors under Clause 9(a)(Option 2) of the EU Clauses;
- The optional language in Section 11(a) of the EU Clauses shall not be included;
- For Clause 13, the supervisory authority shall be the authority identified in Annex 1 of this DPA;
- Option 1 of Clause 17 shall apply, and the EU Clauses will be governed by the law of Ireland; and
- Any dispute arising from the EU Clauses shall be resolved by the courts of Ireland

12.3. Transfers out of the UK. If Customer transfers Personal Data out of the UK to ServiceMax in a country not deemed by the UK Government to have adequate data protection, such transfer will be governed by the UK Clauses, the terms of which are hereby incorporated into this DPA. In furtherance of the foregoing, the Parties agree that Tables 1 through 4 of the UK Clauses shall be satisfied by the following information

- Table 1: Reference to Table 1 shall be satisfied by the information in the signature block of this DPA;
- Table 2: For Table 2, the version of the Approved EU SCCs shall be the EU Clauses, Controller to Processor module;
- Table 3: Reference to Table 3 shall be satisfied by the information in Annexes 1, 2, and 3; and
- Table 4: For Table 4, the Exporter and Importer shall have the rights outlined in Section 19 of the UK Clauses.

List of Schedules and Annexes

Schedule 1: Annexes to Standard Contractual Clauses

- Annex 1 – Details of ServiceMax Processing
- Annex 2 – ServiceMax Security Controls
- Annex 3 – List of Sub-processors

Schedule 2: Transfer Impact Assessment

SCHEDULE 1
STANDARD CONTRACTUAL CLAUSES

ANNEX 1 TO STANDARD CONTRACTUAL CLAUSES
DETAILS OF SERVICEMAX PROCESSING

This Schedule 1 and its associated Annexes are an attachment to the ServiceMax Data Protection Addendum (DPA). If there are any conflicts between this Schedule 1 and the DPA, this Schedule 1 and its Annexes will control.

Data exporter. The Data Exporter is (please briefly specify your activities relevant to the transfer):

The Data Exporter is: (i) the Customer legal entity that has executed the Standard Contractual Clauses as a Data Exporter; and (ii) all Affiliates (as defined in the Agreement) of Customer established within jurisdictions from which the transfer is considered a restricted transfer under Applicable Privacy Laws, to the extent the same have purchased the Services based on one or more Order Form(s).

Data importer. The Data Importer is (please briefly specify your activities relevant to the transfer):

The Data Importer performs Services on behalf of the Data Exporter. The Data Importer will have access to Personal Data solely for the purposes of performing the services and may transfer Personal Data globally in accordance with the terms of the Agreement, applicable Order Form(s), the Data Exporter's instructions, and the provisions of the Standard Contractual Clauses.

Data subjects. The Personal Data transferred concern the following categories of data subjects (please specify):

Name and business contact information of employees/contractors of the Data Exporter and Data Exporter's customers

Categories of Personal Data. The Personal Data transferred concern the following categories of data (please specify):

The Data Exporter determines what data is input into the Service. The Data Exporter inputs data provided or made available to the Data Exporter in connection with its business operations (including the Data Exporter's provision of services to its customers) and Processed by the Data Importer while providing the Services. The Personal Data transferred could include the following categories of data:

(a) personal identification data (name, surname, address, email address, date and other identifying information that Customer inputs into its Salesforce instance);
(b) professional identification data (professional status, education, awards, job description, hierarchical positioning, performance levels);
(c) system log data;
(d) geolocation data; and
(e) other Personal Data that may be contained in business related communications and interactions, internal systems, and log data.

However, the data categories specified below represent the most typical data set that may be input into the Service by the Data Exporter. However, as described further below, in most cases, directly identifiable Personal Data is neither required nor processed by Data Importer to provide the relevant Services and Data Exporter agrees to minimize the amount of Personal Data provided to the Data Importer or Sub-processors.

- Business contact details (of Data Exporter employees/contractors and Data Exporter's employees)
- Details of service/support request raised by Data Exporter personnel

Special categories of data (if appropriate)**.** The Personal Data transferred concern the following special categories of data (please specify):

Not applicable

The frequency of the transfer

On a continuous basis during the term of the Agreement between Data Importer and Data Exporter

Nature of the processing; Purpose of the data transfer and further processing. The Personal Data transferred will be subject to the following basic processing activities (please specify):

The Data Importer may process Personal Data for the following purposes:

- managing and responding to Data Exporter requests for service and support;
- addressing Data Exporter service events and issue escalations;
- providing remote services and troubleshooting certain devices and equipment;
- providing technical support for relevant systems and databases;
- managing off-site repair, refurbishment and disposal of malfunctioning components and devices;
- providing various enhanced or add-on services to which the Data Exporter has subscribed (for example data analytics and trending); and
- otherwise supporting the Data Exporter's use of the Data Importer(s) products and services

The Data Exporter's Personal Data may be Processed by the Data Importer: (a) directly by those limited, authorized personnel engaged in service and engineering functions with responsibility for the diagnosis, management and resolution of support issues raised by the Data Exporter's personnel; and (b) potentially indirectly by those limited IT or support personnel by virtue of their role in supporting the systems/technology platforms/components in which the relevant information is maintained.

Only in very limited cases (typically only for the most complex cases requiring the highest service level escalation) may identifiable data be accessed, and then only with Customer's express permission and limitations prescribed by Customer. In addition, where the Data Exporter requests certain additional enhanced or add-on services, the Data Importer may also host and/or incidentally access Personal Data in performing support for those services on the Data Exporter's behalf to deliver that enhanced or add-on service.

Retention of Personal Data

Subject to Section 9 of the DPA, ServiceMax will Process Personal Data for the duration of the Agreement, unless otherwise agreed upon in writing.

Transfers to (Sub-) processors

As described in the Agreement between Data Importer and Data Exported and as described in Annex 3.

Competent Supervisory Authority

The competent supervisory authority shall be the supervisory authority that has jurisdiction over the Data Exporter.

ANNEX 2 TO STANDARD CONTRACTUAL CLAUSES
SERVICEMAX SECURITY CONTROLS

Technical and Organizational Measures. Data Importer implements and maintains industry standard technical and organizational measures to protect the security of Personal Data that it Processes in connection with its Services, which include the following measures:

i. **Organization of Information Security**

1) **Security Ownership**. The Data Importer has appointed a security leader responsible for coordinating and monitoring the security rules and procedures.
2) **Security Roles and Responsibilities**. The Data Importer personnel with access to Personal Data are subject to confidentiality obligations.
3) **Risk Management Program**. The Data Importer conducts periodic risk assessments.

ii. **Asset Management**

1) **Asset Inventory**. The Data Importer maintains an up-to-date inventory of IT managed assets on which Personal Data is stored.
2) **Asset Handling**. The Data Importer provides guidance to Data Importer businesses on: (a) classifying information generated or used by the applicable Data Importer business; and (b) recommended ways to label, store, transmit, and dispose of such information, depending on its classification. This includes paper documents, electronic reports and presentations, as well as transmitted or stored data such as email and Data Exporter transactions.

iii. **Human Resources Security**

1) **Security Training**
   A. The Data Importer informs and trains its personnel about relevant policies and their respective roles. The Data Importer also informs its personnel of possible consequences of breaching the policies.
   B. Data Importer personnel sign an annual commitment to act in accordance with Data Importer's policies.
   C. The Data Importer will only use anonymous data in training.

iv. **Physical and Environmental Security**

1) **Physical Access to Facilities.** The Data Importer limits access to its facilities where information systems that process Personal Data are located, to identified authorized individuals. Such measures implemented to limit access shall correspond with the nature of information being Processed and may include access control, CCTV, and intrusion detection systems; implementing visitor entry control procedures; securing offices, rooms, and facilities; protecting against external and environmental threats; and controlling all access points including delivery and loading areas.
2) **Protection from Disruptions**. The Data Importer uses a variety of industry standard measures to protect Personal Data against physical and environmental threats to limit interruption to the Data Importer's processing activities and potential loss of data. These measures may include, for example, equipment citing, physically securing power and telecommunications cabling, ensuring equipment is properly maintained and protected from power failures.
3) **Component Disposal**. The Data Importer uses industry standard processes to securely delete data to prevent its subsequent retrieval or destroy media/components containing Personal Data when these are no longer needed. These processes may include industry standard secure wipe tools (e.g., those compliant with NIST Special Publication 800-88 Revision 2) or physical destruction (e.g., shredding/degaussing).

v. **Communications and Operations Management**

1) **Operational Policy**. The Data Importer maintains security documents describing its security measures and the relevant procedures and responsibilities of its personnel who have access to Personal Data.
2) **Malicious Software**. The Data Importer has anti-malware controls to help avoid malicious software gaining unauthorized access to Personal Data, including malicious software originating from public networks. These controls

include updating of relevant software, firmware and firewalls used on the Data Importer's information systems, and use of up-to-date anti-virus software, in line with industry best practice to mitigate against potential vulnerabilities.

3) **Data in transit**. The Data Importer restricts access to Personal Data leaving the Data Importer's network (e.g., through encryption).

4) **Event Logging**. When access to Personal Data is granted by the Data Exporter to the Data Importer, access and actions to data can be limited (restricted), as well as audited and traceable by the Data Exporter. In addition, per response to malicious software compliance, ServiceMax-managed assets as well as traffic on ServiceMax networks are monitored by ServiceMax IT, providing further auditing and traceability.

vi. **Access Control**

1) **Access Policy.** The Data Importer maintains a record of individuals having access to Data Importer or Data Exporter systems.

2) **Access Authorization**

A. The Data Importer maintains and updates a record of personnel authorized to remotely access the Data Exporter systems that contain Personal Data.

B. The Data Importer deactivates authentication credentials to remote access the Data Importer systems that have not been used for a period not to exceed six months and of any terminated employees as soon as reasonably practical and, in any event, within 24 hours.

C. The Data Importer identifies those personnel who may grant, alter or cancel authorized access to data and resources.

D. The Data Importer ensures that where more than one individual has access to the Data Exporter's systems containing Personal Data, the individuals have separate identifiers/logins.

3) **Least Privilege**

A. Technical support personnel who may have access to Personal Data are trained on the appropriate handling of Personal Data and two factor authentication is used when accessing such data.

B. The Data Importer restricts access to Personal Data to only those individuals who require such access to perform their job function on a need-to-know basis.

C. The Data Importer operates a role based access infrastructure, modelled on region, role, and product.

4) **Integrity and Confidentiality**

A. The Data Importer instructs its personnel to disable administrative sessions when computers or remote Data Exporter sessions are left unattended and has implemented automated inactivity timeouts of 15 minutes or less on all Data Importers computing devices.

B. Mobile devices issued to Data Importer employees are protected with industry standard encryption and remote wipe capabilities.

5) **Authentication**

A. The Data Importer uses industry standard practices to identify and authenticate users who attempt to access information systems.

B. Where authentication mechanisms are based on passwords, the Data Importer requires that the passwords are renewed regularly.

C. Where authentication mechanisms are based on passwords, the Data Importer requires the password to meet prevailing industry standards for strength and complexity and include a minimum password length of at least eight characters with password composition to include upper and lower case letters and numbers or special characters.

D. The Data Importer ensures that de-activated or expired identifiers are not granted to other individuals.

E. The Data Importer maintains records of all activity logs to its information systems and is therefore able to monitor if remote access has been performed on a system and relevant activity which may include activity description (including whether and by whom Personal Data have been entered, modified, and deleted).

F. The Data Importer uses industry standard password protection practices including practices designed to maintain the confidentiality and integrity of passwords when they are assigned and distributed, and during storage (including, for instance, hashing and encryption systems).

6) **Network Design**

A. The Data Importer uses network segmentation to reduce risk of unauthorized access to Personal Data, for instance through the implementation of firewalls and intrusion prevention and detection systems.

B. The Data Importer utilizes industry standard controls to prevent unauthorized interception or infiltration of Personal Data in transit (e.g., through encryption).

vii. **Information Security Incident Management**

1) **Incident Response Process**. The Data Importer maintains an incident response process to appropriately identify potential privacy and information security incidents, engage appropriate stakeholders, and conduct the necessary remediation, including notification to Data Exporters and/or regulators where required.

viii. **Business Continuity Management**

1) The Data Importer maintains emergency and contingency plans for the facilities in which its information systems that process Personal Data are located.

2) The Data Importer's redundant storage and its procedures for recovering data where required are designed to facilitate the reconstruction of Personal Data held in the Data Importer facilities, to its original state from before the time it was lost or destroyed.

ANNEX 3 TO STANDARD CONTRACTUAL CLAUSES
LIST OF SUB-PROCESSORS

Sub-processing authorization

The Data Exporter hereby authorizes the Data Importer to partially sub-contract the data Processing activities described herein solely for the purpose of enabling the Data Importer and its Affiliates to provide to the Data Exporter the relevant Services and the following. Customers can subscribe to updates to the Sub-processor list at https://www.servicemax.com/trust/updates

NOTICE: Some countries place conditions and restrictions on use of map technology. Customers are solely responsible for using map technology that is permitted where the Customer intends to operate and for providing all necessary notices to, and obtaining any necessary consents from, the individuals whose personal information (including, without limitation, geolocation) is included in, or processed in connection with, map technology.

A. Google

ServiceMax enables Google Maps in the following ServiceMax products:

Core
Dispatch Module
Engage
Field Service Application mobile application
Service Optimization (aka Optimax)
Service Board
Go mobile application

Google Terms. ServiceMax has developed a Google Maps API implementation. The Google Terms of Service at *https://cloud.google.com/terms/* and the Google Maps Additional Terms of Service at *https://maps.google.com/help/terms_maps/* apply to Customers' use of Google Maps.

If ServiceMax has enabled customers to utilize their own license for Google Maps, then customers are responsible to comply with the terms that they have with Google for use of Google Maps in connection with ServiceMax products.

Customers using Google Maps must notify their users, via the Customer's privacy notice, that the Google Maps API(s) may be used in connection with certain products, and incorporate by reference Google's then current Privacy Policy found at http://www.google.com/policies/privacy). The Customer's privacy notice must notify users of the collection of geo location data.

B. Graphhopper

Schedule Optimization default map provider is Graphhopper. Graphhopper's Terms of Use at https://www.graphhopper.com/terms/ apply to Customers' use of Graphhopper products. Customers may provide their own license key to use Graphhopper, and in that case, Customers are fully responsible for complying with their applicable Graphhopper terms.

C. MapBox

Service Board default map provider is MapBox. MapBox's Terms of Use at https://www.mapbox.com/legal/tos apply to Customers' use of MapBox products. Customers may provide their own license key to use MapBox, and in that case, Customers are fully responsible for complying with their applicable MapBox terms.

Entity Name	Entity Type	Service Type	Entity Country
Salesforce	Third-party provider of cloud platform and application hosting	The ServiceMax Asset 360, Core, and FieldFX services are hosted on Salesforce software.	Varies by where Customer sets up its Salesforce instance
Amazon Web Services (AWS)	Third-party provider of global cloud infrastructure	ServiceMax uses AWS infrastructure to host the following: • Service Board • Sync Gateway • ServiceMax configuration and data replication engines • Zinc real-time communication engine • Optimization engine • Error, access and usage logging	United States, Ireland
AnyNines	Third party service provider.	AnyNines manages the ServiceMax AWS environment and applications on AWS.	Germany
Twilio	Third party provider of cloud-based communication APIs and services	Twillio is used to provide Zinc voice and video calling features within the ServiceMax products	United States
Google Maps	Third party map technology provider	Google map technology is available for use with ServiceMax Core, Dispatch Module, Engage, FSA, Service Board, Service Optimization, and ServiceMax Go.	United States
Graphhopper	Third party map technology provider	Graphopper map technology is available for use with ServiceMax Schedule Optimization.	United States
MapBox	Third party map technology provider	MapBox map technology is available for use with ServiceMax Service Board.	United States

SCHEDULE 2 – TRANSFER IMPACT ASSESSMENT

TRANSFER IMPACT ASSESSMENT FOR TRANSFERS OF PERSONAL DATA OUTSIDE THE EEA

	Questions	Relevant Information About ServiceMax Processing
1.	**What does ServiceMax do?**	ServiceMax is a provider of field service management software and services which support companies across industries to manage work orders, plan and schedule work assignments, provide mobile technician enablement, and enable crew management and shift planning.
2.	**Where is ServiceMax located?**	ServiceMax has operations in various countries around the world, with our headquarters located in the United States.
3.	**What types of Personal Data does ServiceMax process, and what does it do with it?**	Business contact information and other limited Personal Data relating to employees and contractors of ServiceMax customers. ServiceMax does not process special category data. ServiceMax does not use the customers' data for any purpose other than to perform our Services on behalf of our customers. ServiceMax may act as a processor for our customers' Personal Data under the EU General Data Protection Regulation and the UK General Data Protection Regulation (collectively, the "GDPR").
4.	**What measures does ServiceMax implement to protect the security of Personal Data it processes?**	ServiceMax uses industry standard technical and organizational measures to protect the security of Personal Data we process, as set forth in Annex 2 of Schedule 1 above. To the extent ServiceMax engages Sub-processors in connection with its performance of the Services, ServiceMax executes DPAs to ensure such Sub-processors comply with terms that are consistent with those we agree with our customers via our DPA.
5.	**Is Personal Data transferred outside of the EEA?**	Personal data may be transferred to, and processed in, the United States for the Zinc product. Personal data may be transferred outside the EEA in connection with the provision of technical support and professional services for all ServiceMax products.
6.	**What is the mechanism relied upon by ServiceMax for international transfers of Personal Data to third countries?**	For transfers of Personal Data which are subject to GDPR, to third countries outside the European Economic Area, ServiceMax relies on the Standard Contractual Clauses (Controller to Processor module)[1], together with the additional safeguards referenced in Section 4 above.

[1] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32021D0914&from=EN

	Questions	Relevant Information About ServiceMax Processing
7.	**Is ServiceMax subject to US government surveillance laws or other laws requiring it to disclose Personal Data to US national security agencies? If yes, are any legal remedies afforded to impacted individuals in the EU?**	Given the broad definition of *electronic communications service provider*, we, like most US companies, may theoretically be subject to US government surveillance laws, such as Section 702 of the Foreign Intelligence Surveillance Act ("FISA 702"), and National Security Letter requests issued by the FBI under Executive Order 12333 ("EO 12333" and together with FISA 702, "US Government Surveillance Laws"). However, given the limited nature of the Personal Data we process, it is unlikely that we will be subject to demands under such US Government Surveillance Laws. US government commitments and policies restrict intelligence collection to what is required for foreign intelligence purposes and expressly prohibit the collection of information for other purposes, including commercial advantage. As such, we have no reason to believe that our data transfers present risks under US Government Surveillance Laws. In addition, we do not voluntarily allow US government access to Personal Data transferred to us, for example in response to requests made under EO1233. To the extent we are ever subject to such an order, we expect government bodies and law enforcement agencies to follow applicable laws and regulations, in addition to ensuring due process for all data requests.
8.	**Does ServiceMax believe that US Government Surveillance Laws prevent it from complying with the Standard Contractual Clauses in its capacity as a Data Importer?**	No. Considering the nature of the Personal Data we process on behalf of our customers, it is unlikely that we will be subject to demands under US Government Surveillance Laws and, to date and to our knowledge, we have not received any such demands or requests. In the unlikely event we do receive such a request or demand, we will provide data only when legally bound by an order or subpoena issued by a court or legal body with proper jurisdiction. If such demand for data from a government body is received, we will attempt to redirect the government body to request that data directly from the applicable Data Exporter. If compelled to disclose data to a government body, we will give the applicable Data Exporter reasonable notice of the demand so that they can seek a protective order or other appropriate remedy, unless legally prohibited from doing so. In addition, and as discussed above, we have implemented and maintained additional safeguards in relation to our processing activities, such as processing the minimum amount of data necessary and encryption of data in transit and at rest.