DATA PROCESSING ADDENDUM

This Data Processing Addendum ("DPA") forms part of the Master Subscription Agreement (including Order Forms) between Customer and Salesloft or other written or electronic agreement between Salesloft and Customer for the purchase of online services from Salesloft (the "Agreement") to reflect the parties' agreement with regard to the Processing of Customer Data, including Personal Data, in accordance with the requirements of Data Protection Laws and Regulations. All capitalized terms not defined herein shall have the meaning set forth in the Agreement.

HOW THIS DPA APPLIES

If the Customer entity signing this DPA is a party to the Agreement, this DPA is an addendum to and forms part of the Agreement. In such case, the Salesloft entity that is party to the Agreement is party to this DPA.

If the Customer entity signing this DPA has executed an Order Form with Salesloft or its Affiliate pursuant to the Agreement, this DPA is an addendum to that Order Form and applicable renewal Order Forms, and the Salesloft entity that is party to such Order Form is party to this DPA.

If the Customer entity signing this DPA is neither a party to an Order Form nor the Agreement, this DPA is not valid and is not legally binding. Such entity should request that the Customer entity who is a party to the Agreement execute this DPA.

If the Customer entity signing the DPA is not a party to an Order Form nor a Master Subscription Agreement directly with Salesloft, but is instead a customer indirectly via an authorized reseller of Salesloft services, this DPA is not valid and is not legally binding. Such entity should contact the authorized reseller to discuss whether any amendment to its agreement with that reseller may be required.

This DPA shall not replace any comparable or additional rights relating to Processing of Customer Data contained in the Agreement (including any existing data processing addendum to the Agreement).

DATA PROCESSING TERMS

In the course of providing the Services to Customer pursuant to the Agreement, Salesloft may Process Personal Data on behalf of Customer and each party agrees to comply with the following provisions with respect to any Personal Data.

1. DEFINITIONS

"Customer" means the entity receiving services provided by Salesloft.

"Customer Data" means electronic data and information submitted, transferred, or uploaded by or to the Subscription Services and processed by Salesloft on Customer's behalf (including electronic data and information the Subscription Services may obtain from Third Party Applications such as salesforce.com).

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

“Data Processor” means the entity which Processes Personal Data on behalf of the Data Controller.

“Data Protection Laws and Regulations” means the data protection laws and regulations applicable to the Processing of Personal Data under the Agreement, including the laws and regulations of the United States and European Data Protection Laws.

“European Data Protection Laws” means the data protection laws and regulations of the European Union, the European Economic Area (“EEA”) and their member states, and of the United Kingdom to the extent that it is not a member state, including but not limited to Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (“GDPR”).

“Data Subject” means the individual to whom Personal Data relates.

“Personal Data” means any information relating to (i) an identified or identifiable person and, (ii) an identified or identifiable legal entity (where such information is protected similarly as personal data or personally identifiable information under applicable Data Protection Laws and Regulations), where such data is submitted to the Services as Customer Data.

“Personal Data Breach” means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed.

“Processing” means any operation or set of operations which is performed upon Personal Data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.

“Security, Privacy, and Architecture Documentation” means the security standards applicable to the specific Services purchased by Customer, as updated from time to time, as made reasonably available by Salesloft.

“Salesloft” means Salesloft, Inc., a company incorporated in Delaware.

“Standard Contractual Clauses” means the standard contractual clauses (controller to processor module) as adopted by the EU Commission Implementing Decision EU 2021/914 of June 4, 2021.

“Sub-processor” means any Data Processor engaged by Salesloft.

“Third Country” means a country outside the EEA not recognized by the European Commission as providing an adequate level of protection for personal data.

“UK Standard Contractual Clauses” means the Standard Contractual Clauses for data controller to data processor transfers approved by the European Commission in decision 2010/87/EU.

2. PROCESSING OF PERSONAL DATA

2.1 Roles of the Parties. The parties acknowledge and agree that with regard to the Processing of Personal Data, Customer is the Data Controller, Salesloft is a Data Processor and that Salesloft will engage Sub-processors pursuant to the requirements set forth in Section 5 “Sub-processors” (and Section 9, if applicable) 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 Data Protection Laws and Regulations. For the avoidance of doubt, Customer is responsible for ensuring that its instructions for the Processing of Personal Data comply with Data Protection Laws and Regulations. Customer shall have sole responsibility for the accuracy, quality, and legality of Personal Data and the means by which Customer acquired Personal Data.

2.3 Salesloft’s Processing of Personal Data. Unless required otherwise by law to which Salesloft is subject (in which case Salesloft shall inform Customer of that requirement before Processing, unless such law prohibits such information), Salesloft shall only Process Personal Data on behalf of and in accordance with Customer’s documented instructions and shall treat Personal Data as Confidential Information. Customer instructs Salesloft to Process Personal Data for the following purposes: (i) Processing in accordance with the Agreement and applicable Order Form(s); (ii) Processing initiated by Users in their use of the Services; and (iii) Processing to comply with other reasonable instructions provided by Customer (e.g., via email) where such instructions are consistent with the terms of the Agreement. Additional instructions outside the scope of the then current documented instructions shall require prior written agreement between the parties, including agreement on any additional fees payable by Customer to Salesloft for carrying out such instructions. To the extent required by Data Protection Laws and Regulations, Salesloft shall immediately inform Customer if Salesloft develops an opinion that Customer’s instructions infringe Data Protection Laws or Regulations, it being understood that Salesloft has no obligation to research or monitor Customer’s business or specific use of the Services in conjunction with Data Protection Laws or Regulations for the purposes of the foregoing obligation.

2.4 Scope, Purpose and Duration; Categories of Personal Data and Data Subjects. The subject-matter of Processing of Personal Data by Salesloft is the performance of the Services pursuant to the Agreement. The duration of such Processing is set forth in the Agreement. The nature and the purposes of the Processing of Personal Data by Salesloft, the types of Personal Data and categories of Data Subjects Processed under this DPA, are further specified in Schedule 1 (Details of the Processing) to this DPA.

3. RIGHTS OF DATA SUBJECTS

3.1 Correction, Blocking and Deletion. To the extent Customer, in its use of the Services, does not have the ability to locate, correct, amend, restrict, copy, block, or delete Personal Data, as may be required by Data Protection Laws and Regulations, Salesloft shall comply with any commercially reasonable request by Customer (including by appropriate technical and organizational measures) to assist such actions to the extent Salesloft is legally permitted to do so and required by Data Protection Laws and Regulations. To the extent legally permitted, Customer shall be responsible for any costs arising from Salesloft’s provision of such assistance.

3.2 Data Subject Requests. Salesloft shall, to the extent legally permitted, promptly notify Customer if it receives a request from a Data Subject to exercise his or her rights in respect of Personal Data. Salesloft shall not respond to any such Data Subject request without Customer's prior written consent except to confirm that the request relates to Customer. Salesloft shall provide Customer with commercially reasonable cooperation and assistance in relation to handling of a Data Subject's request for access to that person's Personal Data, to the extent legally permitted and to the extent Customer does not have access to such Personal Data through its use of the Services. If legally permitted, Customer shall be responsible for any costs arising from Salesloft's provision of such assistance.

4. SALESLOFT PERSONNEL

4.1 Confidentiality. Salesloft 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 or are under an appropriate statutory obligation of confidentiality. Salesloft shall ensure that such confidentiality obligations survive the termination of the personnel engagement.

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

4.3 Limitation of Access. Salesloft shall ensure that Salesloft's 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 expressly authorizes (a) Salesloft to engage Salesloft's Affiliates as Sub-processors; and (b) Salesloft and Salesloft's Affiliates respectively to engage third-party Sub-processors, in connection with the provision of the Services. Any such Sub-processors will be permitted to obtain Personal Data only to deliver the services Customer has retained Salesloft to provide, and they are prohibited from using Personal Data for any other purpose.

5.2 Liability. Salesloft shall be liable to Customer for the acts and omissions of its Sub-processors to the same extent Salesloft would be liable if performing the services of each Sub-processor directly under the terms of this DPA.

6. SECURITY

Salesloft shall maintain administrative, physical, and technical safeguards for protection of the security, confidentiality, and integrity of Customer Data, including Personal Data, as set forth in the Security, Privacy, and Architecture Documentation. Salesloft regularly monitors compliance with these safeguards. Salesloft will not materially decrease the overall security of the Services during a subscription term.

7. PERSONAL DATA BREACH MANAGEMENT AND NOTIFICATION

Salesloft maintains security incident management policies and procedures and shall, to the extent permitted by law, without undue delay notify Customer of any actual or reasonably suspected Personal Data Breach of Customer Data, by Salesloft or its Sub-processors of which Salesloft becomes aware. Salesloft shall, taking into account the nature of the Processing and information available to it, to the extent required by Data Protection Laws and Regulations, assist Customer with its obligations to notify or communicate any Personal Data Breach to a data protection supervisory authority or to a Data Subject. To the extent such Personal Data Breach is caused by a violation of the requirements of this DPA by Salesloft, Salesloft shall make reasonable efforts to identify and remediate the cause of such Personal Data Breach.

8. RETURN AND DELETION OF CUSTOMER DATA

Customer hereby directs Salesloft to return Customer Data to Customer and delete Customer Data upon request and in accordance with the procedures and timeframes specified in the Security, Privacy, and Architecture Documentation, unless applicable law or regulation requires continued storage of all or part of the Customer Data.

9. JURISDICTION SPECIFIC TERMS

9.1. EEA and UK. To the extent Personal Data is subject to European Data Protection Laws, the following additional terms shall apply:

9.1.1 Sub-processors:

(a) **List of Current Sub-processors/Notification of New Sub-processors.** For the purpose of the authorization in Section 5.1 of this DPA, Salesloft shall make available to Customer a current list of Sub-processors for the respective Services (“Sub-processor List”). Salesloft shall provide Customer with a mechanism to subscribe to updates to the relevant Sub-processor List, to which Customer shall subscribe, and Salesloft shall provide such updates at least thirty (30) days before any new Sub-processor(s) Process Personal Data in connection with the provision of the Services.

(b) **Objection Right for New Sub-processors.** If Customer has a reasonable basis to object to Salesloft’s use of a new Sub-processor, Customer shall notify Salesloft in writing within ten (10) business days after receipt of Salesloft’s notice of a new Sub-processor(s). In the event Customer objects to a new Sub-processor(s) and that objection is not unreasonable, Salesloft will use reasonable efforts to make available to Customer a change in the affected Services or recommend a commercially reasonable change to Customer’s configuration or use of the affected Services to avoid Processing of Personal Data by the objected-to new Sub-processor without unreasonably burdening Customer. If Salesloft is unable to make available such change within a reasonable period of time, which shall not exceed ninety (90) days, Customer may terminate the applicable Order Form(s) in respect only to those Services which cannot be provided by Salesloft without the use of the objected-to new Sub-processor, by providing written notice to Salesloft. If no objection is received during the applicable timeframe, Salesloft will deem Customer to have authorized the new Sub-processor.

(c) **Sub-processor Obligations.** To the extent required by European Data Protection Laws, Salesloft shall enter into a written agreement with each Sub-processor imposing substantively similar data protection obligations as set out in this DPA. Where Salesloft's engagement of a Sub-processor involves a transfer of Personal Data to a Third Country, Salesloft will ensure a valid transfer mechanism is in place with each Sub-processor as may be required by European Data Protection Laws.

9.1.2 Cross Boarder Transfers of Personal Data. Customer agrees that Salesloft may transfer and process Personal Data outside of the EEA or UK where Salesloft, its Affiliates, or its Sub-processors maintain data processing operations, including in the United States. This Section 9.1.2, and the Standard Contractual Clauses or the UK Standard Contractual Clauses, (collectively, the "Clauses"), as applicable, shall apply only to Personal Data that is transferred in circumstances such that, absent the protections afforded by the Clauses, such transfer and/or subsequent processing would contravene European Data Protection Laws, including with respect to transfers of Personal Data to a Third Country. The Clauses will not apply where Salesloft has adopted Binding Corporate Rules with its processors or otherwise adopts an alternative and compliant transfer mechanism.

(a) **Transfers Outside of the EEA.** Where the foregoing conditions are met and the transfer includes Personal Data of EEA Data Subjects, each party agrees to abide by and process Customer Personal Data in compliance with the Standard Contractual Clauses, which are attached hereto as Exhibit A and form part of this DPA. The Standard Contractual Clauses apply to (i) the 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 the European Economic Area and Switzerland which have signed Order Forms for the Services. For the purpose of the Standard Contractual Clauses and this Section 9, the aforementioned entities shall be deemed "data exporters", and Salesloft shall be deemed a "data importer". Notwithstanding the forgoing, Customer recognizes and agrees that, to the extent standard contractual clauses are required to enable a lawful transfer of Personal Data to a Sub-processor, Salesloft may transfer Personal Data to a Sub-processor outside of the EEA pursuant to the standard contractual clauses approved by the European Commission in decision 2010/87/EU, so long as use of such transfer mechanism is in compliance with European Data Protection Laws. To the extent any Sub-processors have not executed Standard Contractual Clauses (as adopted by the EU Commission by means of the Implementing Decision EU 2021/914 of June 4, 2021) as of the effective date of this DPA, Salesloft will use reasonable efforts to execute such Standard Contractual Clauses with such Sub-processors as soon as possible, but in any event no later than December 27, 2022.

(b) **Transfers outside of the UK.** Where the foregoing conditions are met and the transfer includes Personal Data of UK Data Subjects (as such term is defined by UK data protection laws and regulations) the parties agree to abide by and process Personal Data in compliance with the UK Standard Contractual Clauses, which are hereby incorporated by reference and completed as follows: (1) the governing law in Clause 9 and Clause 11.3 is the law of England; (2) the description of in scope data subjects, categories of personal data, processing applications, and the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) are as identified in Schedule 1 and Schedule 2 (Annexes I and II) to this DPA. In addition, the following changes apply: (i) references to data protection law are replaced with references to applicable UK data protection law, (ii) references to the EU or Member States are replaced with references to the UK, and (iii) references to EU authorities are replaced with references to the competent UK authority.

9.1.3 Data Impact Assessment/Consultation. Salesloft shall, taking into account the nature of the Processing and information available to it, reasonably assist Customer with its obligations to conduct a data protection impact assessment and consult with data protection supervisory authorities, at Customer's sole cost.

9.1.4 Data Protection Officer. Salesloft has appointed a data protection officer where such appointment is required by European Data Protection Laws. The appointed person may be reached at security@Salesloft.com.

9.1.5 Copies of Sub-processor Agreements. The parties agree that the copies of the Sub-processor agreements that must be sent by Salesloft to Customer pursuant to the Clauses (a) shall be treated as the Confidential Information of Salesloft in accordance with the Agreement, (b) may have all commercial information, or clauses/provisions unrelated to the Clauses or their equivalent, removed by Salesloft beforehand, and (c) will be provided by Salesloft only upon reasonable request by Customer.

9.1.6 Correction of Personal Data. Taking into account the nature of the processing, Customer agrees that it is unlikely that Salesloft would become aware that Customer Data is inaccurate or outdated, and that Customer is primarily responsible for ensuring that Personal Data is accurate and current. However, if Salesloft becomes aware that Customer Data is inaccurate or outdated, it will inform Customer without undue delay. Upon request, Salesloft will reasonably assist Customer in rectifying inaccurate or outdated Personal Data transferred under the Clauses (at Customer's expense only if complying with such request will require significant resource (including significant time allocation) from Salesloft), to the extent Customer is unable to carry out such functions without Salesloft's assistance.

9.2 California/United States. To the extent "personal information" of "consumers" (as such terms are defined by the California Consumer Privacy Act of 2018 ("CCPA")) contained within Customer Data and processed by Salesloft is subject to the CCPA ("CCPA Data"), the parties agree that Customer is a business and that it appoints Salesloft as its service provider to process CCPA Data as permitted under the Agreement and this DPA. Salesloft agrees that: (a) it will process CCPA Data in accordance with the Agreement, and will not use or disclose CCPA Data for any other purpose other than for providing the Services or in connection with its rights and obligations under the Agreement, and (b) it shall not "sell" (as such term is defined by the CCPA) CCPA Data. If SalesLoft receives a request from a consumer to exercise a right such consumer has under the CCPA in relation to information relating to such consumer contained in and identified as Customer CCPA Data, Salesloft will provide a copy of the request to Customer. For the avoidance of doubt, Customer will be responsible for handling and communicating with consumers in relation to such requests.

10. AUDITS

10.1 Audits and Certifications. The parties agree that Customer's right to audit Processing of Customer Data by Salesloft (including for purposes of the audits described in GDPR Art. 28(3)(h) and Clause 8.9 of the Standard Contractual Clauses) shall be carried out in accordance with the following specifications:

Upon Customer's request, and subject to the confidentiality obligations set forth in the Agreement, Salesloft shall make available to Customer that is not a competitor of Salesloft (or Customer's independent, third-party auditor that is not a competitor of Salesloft) information regarding Salesloft's compliance with the obligations set forth in this DPA in the form of the third-party certifications and audits set forth in the Security, Privacy, and Architecture Documentation to the extent Salesloft makes them generally available to its customers. Customer may contact Salesloft in accordance with the "Notices" Section of the Agreement to request an on-site audit of the procedures relevant to the protection of Personal Data. Customer shall reimburse Salesloft for any time expended for any such on-site audit at Salesloft's then-current professional services rates, which shall be made available to Customer upon request. Before the commencement of any such on-site audit, Customer and Salesloft shall mutually agree upon the scope, timing, and duration of the audit in addition to the reimbursement rate for which Customer shall be responsible. All reimbursement rates shall be reasonable, taking into account the resources expended by Salesloft. Customer shall promptly notify Salesloft with information regarding any non-compliance discovered during the course of an audit.

10.2 Demonstration of Compliance. Salesloft shall make available to Customer upon reasonable demand any other information necessary to demonstrate compliance with this DPA, provided that such information (a) shall be treated as the Confidential Information of Salesloft and in accordance with the Agreement, and (b) may have all commercial information, or information unrelated to compliance with this DPA, removed by Salesloft beforehand. Such information will be provided by Salesloft only upon reasonable request by Customer.

11. LIMITATION OF LIABILITY

Each party’s and its Affiliates’ liability arising out of or related to this DPA, including the Clauses, (whether in contract, tort, or under any other theory of liability) is subject to the section ‘Limitation of Liability’ of the Agreement, and any reference in such section to the liability of a party means that party and its Affiliates in the aggregate.

12. CONFLICT

Notwithstanding any language in the Agreement to the contrary, in the event of any conflict or inconsistency (i) between the Agreement and this DPA, the latter shall prevail; (ii) between this DPA and the Standard Contractual Clauses in Schedule 2 or the UK Standard Contractual Clauses, as applicable, the latter shall prevail.

List of Schedules

Schedule 1: Details of Processing

Schedule 2: Standard Contractual Clauses

The parties' authorized signatories have duly executed this Agreement:

CUSTOMER

Signature: ______________________________

Customer Legal Name: ______________________________

Print Name: ______________________________

Title: ______________________________

Date: ______________________________

SALESLOFT, INC.

Signature: ______________________________

Print Name: ______________________________

Title: ______________________________

Date: ______________________________

SCHEDULE 1 - DETAILS OF THE PROCESSING

Nature and Purpose of Processing

Sales Engagement Software as a Service

Categories of Data Subjects

Customer may submit and users may submit on behalf of Customer Personal Data to the Services, the extent of which is determined and controlled by Customer in its sole discretion, and which may include, but is not limited to Personal Data relating to the following categories of data subjects:

- Prospects, customers, business partners, and vendors of Customer (who are natural persons)
- Employees or contact persons of Customer’s prospects, customers, business partners, and vendors
- Employees, agents, advisors, freelancers of Customer (who are natural persons)
- Customer’s Users authorized by Customer to use the Services

Categories of Personal Data

Customer may submit Personal Data to the Services, the extent of which is determined and controlled by Customer in its sole discretion, and which may include, but is not limited to the following categories of Personal Data:

- First and last name
- Title
- Position
- Employer
- Contact information (company, email, phone, physical business address)
- ID data
- Professional life data
- Personal life data
- Connection data
- Localisation data

SCHEDULE 2 - STANDARD CONTRACTUAL CLAUSES

(MODULE TWO – CONTROLLER TO PROCESSOR)

SECTION I

Clause 1
Purpose and scope

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

(b) The Parties:

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

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

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

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

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

Clause 2
Effect and invariability of the Clauses

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

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

Clause 3
Third-party beneficiaries

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

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;
(ii) Clause 8.1(b), 8.9(a), (c), (d) and (e);
(iii) Clause 9(a), (c), (d) and (e);
(iv) Clause 12(a), (d) and (f);
(v) Clause 13;
(vi) Clause 15.1(c), (d) and (e);
(vii) Clause 16(e);
(viii) Clause 18(a) and (b).

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

Clause 4
Interpretation

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

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

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

Clause 5
Hierarchy

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

Clause 6
Description of the transfer(s)

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

Clause 7
Docking clause

Not applicable

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8
Data protection safeguards

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

8.1 Instructions

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

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

8.2 Purpose limitation

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

8.3 Transparency

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

8.4 Accuracy

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

8.5 Duration of processing and erasure or return of data

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

8.6 Security of processing

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

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

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

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

8.7 Sensitive data

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

8.8 Onward transfers

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

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

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

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

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

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

8.9 Documentation and compliance

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

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

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

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

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

Clause 9
Use of sub-processors

(a) The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least thirty (30) days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

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

(c) The data importer shall provide, at the data exporter’s request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

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

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

Clause 10
Data subject rights

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

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

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

Clause 11
Redress

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

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion.

The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

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

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

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

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

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

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

Clause 12
Liability

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

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

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

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

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

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

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

Clause 13
Supervision

(a) [Where the data exporter is established in an EU Member State:] The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679:] The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679:] The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

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

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

Clause 14
Local laws and practices affecting compliance with the Clauses

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

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

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

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

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

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

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

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

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

Clause 15
Obligations of the data importer in case of access by public authorities

15.1 Notification

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

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

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

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

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

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

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

15.2 Review of legality and data minimisation

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(c).

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

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

SECTION IV – FINAL PROVISIONS

Clause 16
Non-compliance with the Clauses and termination

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

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

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

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

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

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

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

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

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

Clause 17
Governing law

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

Clause 18
Choice of forum and jurisdiction

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

(b) The Parties agree that those shall be the courts of Ireland.

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

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

Annex 1 to Schedule 2

A. LIST OF PARTIES

Data exporter(s):

Name: Data Exporter is (i) the 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 the European Economic Area (EEA) and Switzerland that have purchased Services on the basis of one or more Order Form(s).

Address:

Contact person's name, position and contact details:

Activities relevant to the data transferred under these Clauses: Data Exporter's receipt and use of the Services.

Signature and Date:

Role (controller/processor): controller

Data importer(s):

Name: Salesloft, Inc.

Address: 1180 West Peachtree St. NW, Suite 600, Atlanta, GA 30309

Contact person's name, position and contact details: support@salesloft.com

Activities relevant to the data transferred under these Clauses: Salesloft is a provider of enterprise cloud computing solutions which processes personal data upon the instruction of the data exporter in accordance with the terms of the Agreement.

Signature and Date:

Role (controller/processor): processor

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

Data exporter may submit Personal Data to the Services, the extent of which is determined and controlled by the data exporter in its sole discretion, and which may include, but is not limited to Personal Data relating to the following categories of data subjects:

- Prospects, customers, business partners and vendors of data exporter (who are natural persons)
- Employees or contact persons of data exporter's prospects, customers, business partners and vendors
- Employees, agents, advisors, freelancers of data exporter (who are natural persons)
- Data exporter's Users authorized by data exporter to use the Services

Categories of personal data transferred

Data exporter may submit Personal Data to the Services, the extent of which is determined and controlled by the data exporter in its sole discretion, and which may include, but is not limited to the following categories of Personal Data:

- First and last name
- Title
- Position
- Employer
- Contact information (company, email, phone, physical business address)
- ID data
- Professional life data
- Personal life data
- Connection data
- Localization data

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

The parties do not intend for any sensitive data, including special categories data to be processed under the Agreement.

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

Personal data will be transferred to importer on a continuous basis throughout the duration of the Agreement.

Nature of the processing

Processing of Personal Data (that exporter elects, in its discretion, to send to importer) in connection with its use of importer's sales engagement Software-as-a-Service to provide the Services purchased by exporter and as otherwise permitted by the Agreement.

Purpose(s) of the data transfer and further processing

The operation, support, use, or provisioning of importer's Sales Engagement Software-as-a-Service product.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period.

The period of retention is as set out in the Agreement.

3. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with Clause 13 The supervisory authority of the #### shall act as competent supervisory authority.

The data exporter's competent supervisory authority will be determined in accordance with the GDPR.

DATA EXPORTER

Name: ____

Authorised Signature: ____

DATA IMPORTER (Salesloft, Inc.)

Name: ____

Authorised Signature: ____

Annex II to Schedule 2

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

Salesloft maintains the technical and organization measures outlined in this Annex, as further described in the Security, Privacy and Architecture Documentation applicable to the specific Services purchased by data exporter, and accessible via https://salesloft.com or otherwise made reasonably available by data importer. Data Importer will not materially decrease the overall security of the Services during a subscription term.

Measures of encryption of personal data/measures for protection of data during transmission and storage:

Data processed in the Salesloft platform is encrypted at rest and in transit using commonly accepted algorithms and protocols.

Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services.

Salesloft maintains an information security management system ("ISMS") in keeping with ISO 27001 designed to ensure ongoing confidentiality, integrity, availability, and resilience of processing systems and services.

Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident:

Salesloft performs daily backups of data, tests backups on an annual basis, and deploys infrastructure in a highly redundant fashion to support availability of data in the event of an incident.

Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing

Salesloft undergoes internal and external audits as well as risk assessments on an annual basis to regularly test, assess, and evaluate the effectiveness of its controls.

Measures for user identification and authorisation

Access to systems must be commensurate with job responsibilities or an approved business case, and strong authentication (e.g., multi-factor authentication) is enforced on all systems.

Measures for ensuring physical security of locations at which personal data are processed

Third party data center providers maintain industry leading physical security controls in alignment with standards such as ISO 27001, SOC 2 Type 2, etc.

Measures for ensuring events logging

Salesloft uses audit logging to detect suspicious activity and perform forensic analysis.

Measures for ensuring system configuration, including default configuration Measures for internal IT and IT security governance and management Measures for certification/assurance of processes and products

Salesloft scans relevant processing system configurations for deviations from established benchmarks.

Salesloft's IT systems are governed by the ISMS. IT control domains include but are not limited to endpoint management/protection, identity/access management, and security awareness training.

Salesloft maintains certifications and attestations against relevant standards (e.g., ISO 27001, SOC 2 Type 2).

Measures for ensuring accountability

Salesloft maintains clear lines of reporting and accountability, including dedicated team members responsible for data privacy and security.

Measures for allowing data portability and ensuring erasure

Salesloft supports the right to data erasure and portability in the event a data subject request is received by the customer.

For transfers to (sub-) processors, also describe the specific technical and organisational measures to be taken by the (sub-) processor to be able to provide assistance to the controller and, for transfers from a processor to a sub-processor, to the data exporter

Data protection commitments to Salesloft by its Sub-processors are substantively similar to those agreed to in the data protection agreement between Salesloft and the data exporter. Salesloft reviews vendor security and privacy posture prior to exporting data, and annually thereafter.