29 West 35th Street, 7th Floor
New York, NY 10001

Data Processing Addendum

In the course of providing its services to Customer, Sprinklr may Process Personal Data on behalf of Customer. This Data Processing Addendum ("DPA") reflects the parties' agreement with regard to the Processing of Personal Data, in accordance with the requirements of Data Protection Legislation. This Data Processing Addendum ("DPA") is incorporated by reference as part of the Master Services Agreement (or other agreement for the purchase of Sprinklr's services, hereinafter collectively "MSA") between Customer and Sprinklr

This DPA reflects the parties' agreement with regard to the Processing of Personal Data, in accordance with the requirements of Data Protection Legislation. This DPA shall not replace any additional rights relating to Processing of Personal Data previously negotiated by Customer in the MSA.

This DPA will terminate automatically upon termination of the MSA, or as earlier terminated pursuant to the terms of this DPA.

This DPA consists of two parts:

A. Data Processing Terms
B. Standard Contractual Clauses

A. DATA PROCESSING TERMS

1. DEFINITIONS

"Affiliate" means any entity that directly or indirectly controls, is controlled by, or is under common control with the subject entity. "Control," for purposes of this definition, means direct or indirect ownership or control of more than 50% of the voting interests of the subject entity.

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

"Data Protection Legislation" means all laws and regulations, including laws and regulations applicable to the Processing of Personal Data under the MSA.

"Data Subject" means the individual to whom the Personal Data pertains.

"Personal Data" means "personal data," "personal information" or an equivalent term, as defined by applicable Data Protection Legislation to the extent such data or information is accessed, collected, stored, transmitted, processed, hosted, used, handled, or disposed of by Sprinklr in connection with the Agreement.

"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 in Sprinklr's possession, custody or control, to the extent the breach materially compromises the confidentiality, security or integrity of the Personal Data.

"Processing" means any operation or set of operations which is performed by or on behalf of Sprinklr in connection with the Agreement 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.

"Processor" means the entity which Processes Personal Data on behalf of the Controller; where the entity Processes the Personal Data pursuant to the Controller's instructions and solely to provide the Services.

"Services" shall mean Sprinklr's customer experience and social media management platform, provided as SaaS, and any required, usual, appropriate or acceptable activities relating to the Services, including without limitation to (a) carry out the Services or the business of which the Services are a part, (b) carry out any benefits, rights and obligations relating to the Services, (c) maintain records relating to the Services, or (d) comply with any legal or self-regulatory obligations relating to the Services.

"Sub-processor" means any Processor engaged by Sprinklr or a Sprinklr Affiliate.

"Users" shall mean Customer', Customer's Affiliates' and Customer's contractors' employees, entitled to use the Services under the MSA.

2. DATA PROCESSING

2.1 The parties acknowledge and agree that with regard to the Processing of Personal Data, Customer is the Controller and Sprinklr is the Processor.

2.2 The parties shall each comply with their respective obligations under the Data Protection Legislation. Customer shall, in its use of the Services, Process Personal Data in accordance with the requirements of Data Protection Legislation.

2.3 Customer's instructions for the Processing of Personal Data shall comply with Data Protection Legislation. Sprinklr shall inform Customer immediately if, in Sprinklr's opinion, an instruction from Customer violates Data Protection Legislation.

2.4 Sprinklr shall only Process Personal Data on behalf of and in accordance with Customer's documented instructions for purposes of (i) Processing for business purposes, in accordance with the MSA; (ii) Processing initiated by Users in their use of the Services; and (iii) Processing to comply with other documented reasonable instructions provided by Customer, as further set out in Sprinklr's published privacy policies. Sprinklr agrees that it shall not sell any Personal Data.

2.5 Sprinklr shall take reasonable steps to instruct and train any of its and/or its Sub-processors' employees who have access to Personal Data to maintain the confidentiality and security of the Personal Data, and shall limit access to Personal Data on a need-to-know basis.

3. DATA SUBJECTS' RIGHTS REQUESTS

3.1 Sprinklr shall, to the extent legally permitted, promptly notify Customer if Sprinklr receives a request from a Data Subject to exercise the Data Subject's right of access, right to rectification, restriction of Processing, erasure ("right to be forgotten"), data portability, object to the Processing, or its right not to be subject to an automated individual decision making ("DSR Request").

3.2 Taking into account the nature of the Processing, Sprinklr 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 DSR Request under Data Protection Legislation.

3.3 To the extent Customer, in its use of the Services, does not have the ability to address a DSR Request, Sprinklr shall, upon Customer's request, provide commercially reasonable efforts to assist Customer in responding to such a DSR Request, to the extent Sprinklr is legally permitted to do so and the response to such DSR Request is required under Data Protection Legislation. To the extent legally permitted, Customer shall be responsible for any costs arising from Sprinklr's provision of such assistance.

4. DATA PROTECTION IMPACT ASSESSMENTS

Sprinklr shall provide reasonable assistance to Customer with any data protection impact assessments, and prior consultations with a competent data protection supervisory authority, required under Data Protection Legislation, in each case solely in relation to Processing of Personal Data by, and taking into account the nature of the Processing and information available to, Sprinklr.

5. PERSONAL DATA BREACH NOTIFICATION

5.1 Sprinklr shall notify Customer without undue delay, and, in any event, within forty-eight (48) hours, after becoming aware of a Personal Data Breach. Sprinklr shall provide Customer with sufficient information to allow Customer to meet any obligations to notify regulators and/or affected individuals of the Personal Data Breach.

5.2 Sprinklr shall make reasonable efforts to identify the cause of a Personal Data Breach and take those steps as Sprinklr deems necessary and reasonable in order to remediate the cause of such a Personal Data Breach to the extent the remediation is within Sprinklr's reasonable control.

5.3 The obligations herein shall not apply to incidents that are caused by Customer.

6. SUB-PROCESSING

6.1 Customer hereby consents to Sprinklr's usage of Sub-processors, as described at www.sprinklr.com/legal.

6.2 Sprinklr has entered into a written agreement with each Sub-processor containing data protection obligations not less protective than those in this DPA with respect to the protection of Personal Data to the extent applicable to the nature of the Services provided by such Sub-processor.

6.3 Sprinklr shall be liable for the acts and omissions of its Sub-processors to the same extent Sprinklr 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 MSA

7. SECURITY AND OTHER SUPPLEMENTARY MEASURES

Sprinklr shall maintain technical and organizational measures designed to protect 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, Personal Data), confidentiality and integrity of Personal Data.

Where Personal Data is transferred to a country which does not ensure a level of protection essentially equivalent to that guaranteed within the European Union and where the EU standard of essential equivalence cannot be achieved through the measures set out in Appendix 2, the Parties shall adopt and implement supplementary measures as required for compliance with regulations of the European Data Protection Board (hereinafter "Supplementary Measures"). As part of such Supplementary Measures, Sprinklr agrees not to allow, unless required by law, regulations, order of a court or any regulatory, judicial, governmental or similar body or authorized by Customer, access to Customer Personal Data (excluding any publicly available data) by any administrative body, authority or agency. Customer acknowledges that Sprinklr may be required by law to allow such access to Customer Personal Data. Before Sprinklr discloses any such Customer Personal Data, Sprinklr shall (to the extent permitted by law) use commercially reasonable efforts to inform the Customer of the circumstances of the required disclosure and the Customer Personal Data that must be disclosed.

8. DELETION OR RETURN OF PERSONAL DATA

8.1 Sprinklr shall delete the Personal Data upon termination/expiry of the MSA as specified in the MSA or upon Customer's reasonable request at any time. Sprinklr may retain Personal Data to the extent required by applicable laws and only to the extent and for such period as required by the applicable laws and always provided that Sprinklr shall ensure the confidentiality of all such Personal Data and shall ensure that such Personal Data is only Processed as necessary for the purpose(s) specified in the applicable laws requiring its storage and for no other purpose.

8.2 Sprinklr shall return Personal Data to Customer in accordance with the procedure and timeframe specified in the MSA.

9. AUDITS AND INSPECTIONS

9.1 Sprinklr shall make available to Customer all information necessary to demonstrate compliance with this DPA and shall allow for and contribute to audits by Customer or a third-party auditor mandated by Customer in relation to the Processing of Personal Data. Upon Customer's written request, Sprinklr shall, not more than once per year, accurately complete a reasonable information security questionnaire provided by Customer regarding Sprinklr's data protection and information security practices and policies.

9.2 To the extent applicable Data Protection Legislation requires Sprinklr to submit to such an audit, Customer or a third-party auditor mandated by Customer may, at Customer's expense and not more than once per year, perform an on-site inspection of Sprinklr's data protection and information security practices and policies with written notice reasonably, at least ten business days, in advance. The inspection shall take place over not more than one day during Sprinklr's normal business hours on a mutually agreed schedule that will minimize the audit's impact on Sprinklr's operations. Customer or a third-party auditor mandated by Customer shall comply with Sprinklr's security requirements related to the performance of the inspection. Due to confidentiality and security requirements, such inspections shall exclude on-site inspections of multi-tenant environments (such as IaaS data centres used by Sprinklr). On-site examinations of such environments can be substituted by detailed documentation regarding the respective data protection and security measures taken and specific certifications issued by reputable third-party auditors, provided by Sprinklr upon Customer's request.

9.3 Notwithstanding Sprinklr's obligations under Section 9.2., if the controls or measures to be assessed in the requested audit are addressed in a SOC 2 Type 2, ISO, NIST or similar audit report performed by a qualified third party auditor within twelve (12) months of Customer's audit request and Sprinklr has certified in writing that there are no known material changes in the controls audited, Customer agrees to accept such report in lieu of requesting an audit – as set out in Section 9.2 -- of such controls or measures

9.4 Customer shall promptly notify Sprinklr of any non-compliance discovered during such an audit/inspection.

10. LIABILITY

10.1 Each party's liability arising out of or related to this DPA and all DPAs between Customer's Affiliates and Sprinklr, whether in contract, tort or under any other theory of liability, is subject to the limitation of liability section agreed under the MSA, and any reference in such section to the liability of a party means the aggregate liability of that party and all of its affiliates under the MSA and all DPAs together.

10.2 For the avoidance of doubt, Sprinklr's total liability for all claims from the Customer and all of Customer's Affiliates arising out of or related to the MSA and each DPA shall apply in the aggregate for all claims under both the MSA and all DPAs established under this Agreement, including by Customer and all Customer's Affiliates, and, in particular, shall not be understood to apply individually and severally to Customer and/or to any of Customer's Affiliate that is a contractual party to any such DPA.

10.3 Where a Data Subject asserts any claims against a party to this DPA in accordance with applicable Data Protection Legislation, the other party shall support in defending against such claims, where possible.

11. INTERNATIONAL PERSONAL DATA TRANSFERS

11.1 Sprinklr Processes Personal Data in various jurisdictions, including the United States.

11.2 The attached Standard Contractual Clauses shall apply to any transfers of Personal Data under this DPA from the

European Economic Area and/or their member states, Switzerland and the United Kingdom to countries which do not ensure an adequate level of data protection within the meaning of Data Protection Legislation of the foregoing territories, to the extent such transfers are subject to such Data Protection Legislation.

11.3 In the event of any conflict or inconsistency between these Data Processing Terms and the Standard Contractual Clauses, the Standard Contractual Clauses shall prevail.

11.4 Further, Sprinklr currently remains certified under the EU-U.S Privacy Shield. Sprinklr continues to comply with its ongoing obligations with respect to transfers made under the EU-U.S Privacy Shield framework.

B. STANDARD CONTRACTUAL CLAUSES

Commission Decision C(2010)593 for the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection

Data exporting organisation	
Name:	
Address:	
Tel./fax/e-mail:	
Customer enters into these Standard Contractual Clauses on behalf of itself and in the name and on behalf of its Affiliates	
hereinafter the “data exporter”	

Data importing organisation	
Name:	Sprinklr, Inc. (including its Affiliates)
Address:	29 West 35th Street, New York, NY 10001, USA
Tel./fax/e-mail:	+1-917-933-7800; fax: n/a; e-mail: privacy@sprinklr.com
hereinafter the “data importer”	

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

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

Clause 1: Definitions

For the purposes of the Clauses:

(a) *'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject'* and *'supervisory authority'* shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;

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

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

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

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

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

Clause 2: Details of the transfer

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

Clause 3: Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.
2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.
3. The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.
4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4: Obligations of the data exporter

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b) that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

(g) to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

(j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5: Obligations of the data importer

The data importer agrees and warrants:

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;

(d) that it will promptly notify the data exporter about:

  (i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,

  (ii) any accidental or unauthorised access, and

  (iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(h) that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing services by the subprocessor will be carried out in accordance with Clause 11;

(j) to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter.

Clause 6: Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or subprocessor is entitled to receive compensation from the data exporter for the damage suffered.

2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity. The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.

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

contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the subprocessor shall be limited to its own processing operations under the Clauses.

Clause 7: Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:
   (a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;
   (b) to refer the dispute to the courts in the Member State in which the data exporter is established.
2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8: Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.
2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.
3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

Clause 9: Governing Law

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

Clause 10: Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11: Subprocessing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses. Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.
2. The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.
3. The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.
4. The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12: Obligation after the termination of personal data processing services

1. The parties agree that on the termination of the provision of data processing services, the data importer and the subprocessor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.
2. The data importer and the subprocessor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

Appendix 1 to the Standard Contractual Clauses

Data exporter

The data exporter is a licensee and user of Sprinklr's customer experience and social media management platform.

Data importer

The data importer provides the Sprinklr Platform (SaaS).

Data subjects

The personal data transferred concern the following categories of data subjects:

1. Data Subjects include individuals collaborating and communicating with the Data Exporter's customers, followers, fans and other Internet users who use social networks and websites and Data Exporter's employees, Data Exporter's agents and Data Exporter's subcontractors' employees operating the Sprinklr Platform ("Account Information").
2. The personal data transferred may also concern the Data Exporter's customers, prospects, marketing addressees etc. uploaded/imported by Data Exporter into the Sprinklr Platform ("Customer Content").
3. The personal data transferred may also concern the Data Exporter's customers, followers, fans and other Internet users who use social media networks and websites, blogs & blog comments, mainstream news sources and forums, and websites owned by the Data Exporter where the Data Importer provides social and content management functionality on the Data Exporter's behalf ("Social Data").

Categories of data

The personal data transferred concern the following categories of data:

1. Account Information transferred includes identification data (name, login), contact information (business email address) and work related information (usage/performance data, social contact handling data).
2. Customer Content transferred includes any category of Personal Data the Data Exporter uploads/stores into the Sprinklr Platform.
3. Social Data transferred includes content published or sent by social media users via customer's social media profiles (e.g. Customer's Facebook page), connected to the Sprinklr Platform (both public and private messages to Customer) and publicly accessible data from the social media networks and websites based on certain search queries (e.g. #customer), defined by the Customer. Social Data includes user/add IDs, social network profile names and information, social network communications and all types of information shared across social media networks and websites.

Special categories of data (if appropriate)

The personal data transferred may include the following special categories of data:

1. Customer Content transferred may contain special categories of data, depending on what kind of data the Data Exporter uploads/stores into the Sprinklr Platform.
2. Social Data transferred may concern special categories of personal data, depending on Data Exporter's usage of the Sprinklr Platform (e.g. definition of specific search queries for collection of publicly accessible personal data on the social media networks).

Processing operations

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

1. Account Information that is transferred will be processed solely for the purpose of operating the Sprinklr Platform (authentication, login and audit trail)
2. Customer Content and Social Data that is transferred will be processed for purposes of social media management, including social media listening and analytics, customer care and support, marketing analytics and marketing management.

Instructions

The DPA and the MSA are Data Exporter's complete instructions at the time of signature of the DPA to Sprinklr for the Processing of Personal Data. Any additional or alternate instructions must be agreed upon separately. For the purposes of Clause 5(a) of the Standard Contractual Clauses, the following is deemed an instruction by the Customer to process Personal Data: (i) Processing in accordance with the MSA; (ii) Processing initiated by Users in their use of the Services; and (iii) Processing to comply with other documented reasonable instructions provided by Customer.

Sub-Processing

Sub-processors used by the Data Importer (Sprinklr) to provide its contractual services as of the effective date of the DPA, including their role and scope of sub-processing and the geographical area of sub-processing are published in Sprinklr's List of Sub-processors, accessible at **www.sprinklr.com/legal**.

Such Sub-processors shall be agreed and consented to by Data Exporter (Customer), also according to Clauses 5(h) and 11 of the Standard Contractual Clauses.

Data Importer (Sprinklr) may remove or appoint suitable and reliable other Sub-processors as follows

- Data Importer (Sprinklr) will inform Data Exporter (Customer) by electronic means at least 30 days in advance of granting access to Data Exporter's (Customer's) personal data to Sub-processor (except for Emergency Replacements as defined below) of any changes to the List of Sub-processors.
- If Data Exporter (Customer) has a legitimate, material reason to object to Data Importer's (Sprinklr's) use of a Sub-processor, Data Exporter (Customer) shall notify Data Importer (Sprinklr) thereof in writing within fifteen (15) days after receipt of Data Importer's (Sprinklr's) notice.
- If Data Exporter (Customer) does not object during such time-period, the new Sub-processor(s) shall be agreed and consented to by Data Exporter (Customer) in writing, also according to Clauses 5(h) and 11 of the Standard Contractual Clauses.
- If Data Exporter (Customer) objects to the use of the Sub-processor concerned, Data Importer (Sprinklr) shall have the right to cure the objection through one of the following options: (i) Data Importer (Sprinklr) will abort its plans to use the Sub-processor with regard to Data Exporter's (Customer's) personal data; or (ii) Data Importer (Sprinklr) will take the corrective steps requested by Data Exporter (Customer) in its objection (which remove Data Exporter's (Customer's) objection) and proceed to use the Sub-processor with regard to Data Exporter's (Customer's) personal data; or (iii) Data Importer (Sprinklr) may cease to provide or Data Exporter (Customer) may agree not to use (temporarily or permanently) the particular aspect of the service that would involve use of the Sub-processor with regard to Data Exporter's (Customer's) personal data.
- If none of the above options are reasonably available and the objection has not been cured within fifteen (15) days after Data Importer's (Sprinklr's) receipt of Data Exporter's (Customer's) objection, either party may terminate the affected service with reasonable prior written notice.

"Emergency Replacement" refers to a sudden replacement of a Sub-processor where such change is outside of Data Importer's (Sprinklr's) reasonable control (such as if the subprocessor ceases business, abruptly discontinues services to Data Importer (Sprinklr), or breaches its contractual duties owed to Data Importer (Sprinklr)). In such case, Data Importer (Sprinklr) will inform Data Exporter (Customer) of the replacing Sub-processor as soon as possible and the process to formally appoint such Sub-processor defined above shall be triggered.

Copies of the Sub-processor agreements that must be provided pursuant to Clause 5(j) of the Standard Contractual Clauses may have all commercial information, or clauses unrelated to the Standard Contractual Clauses or their equivalent, removed by Sprinklr beforehand; and, that such copies will be provided by Sprinklr, in a manner to be determined in its discretion, only upon request by Customer.

Audits and Inspections

The audits described in Clause 5(f) and Clause 12(2) of the Standard Contractual Clauses shall be carried out in accordance with Section 9 of the DPA.

Certification of Deletion

The certification of deletion of Personal Data that is described in Clause 12(1) of the Standard Contractual Clauses shall be provided by Sprinklr to Customer only upon Customer's request.

Appendix 2 to the Standard Contractual Clauses

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

1. Data Storage & Network Security.

(a) Data Storage.

Infrastructure. The Data Importer maintains Amazon Web Service (AWS) and/or Microsoft Azure for its data storage. The Data Importer stores all production data through these secure services. An overview of Web Services Security Processes is available at:

- http://d0.awsstatic.com/whitepapers/Security/AWS_Security_Whitepaper.pdf and
- https://azure.microsoft.com/en-us/services/security-center/

(b) Network Security.

Disaster Recovery Objectives. In case of a major disaster, all processes and personnel should be in place to fully restore the service within 24 hours. That is RTO (Recovery Time Objective) is 24 hours and RPO (Recovery Point Objective) is 24 hours.

High Availability. The Sprinklr application consists of more than 25 independent services. Each service component has at least two instances running at all times in two different zones (data centers) located in the U.S.A. Zones are located at distinct locations and are engineered to be isolated from failures in other Zones.

Disaster Recovery Process. Automation processes are in place to restore the service from the backup data and code in the secondary location. Using automation the entire service will be restored well within the defined RPO and RTO objectives.

Redundancy. Infrastructure systems have been designed to eliminate single points of failure and minimize the impact of anticipated environmental risks. The Services are designed to allow the Data Importer to perform certain types of preventative and corrective maintenance without interruption.

Server Operating Systems. The Data Importer servers use a Linux based implementation customized for the application environment. The Data Importer employs a code review process to increase the security of the code used to provide the Services and enhance the security in the production environments.

Businesses Continuity. The Data Importer replicates data over multiple systems to help to reduce the possibility of unintended destruction or loss of data. The Data Importer has designed and regularly tests its business continuity planning/disaster recovery programs.

(c) Networks & Transmission.

Incident Response. The Data Importer monitors a variety of communication channels for security incidents, and The Data Importer's security personnel will react promptly to detected incidents.

Encryption Technologies. The Data Importer requires HTTPS encryption (also referred to as SSL or TLS) for all connections. Web sessions are encrypted using HTTPS to provide secure data communication with the Sprinklr application. Backend server access (for support) is over SSH, SFTP and RDP.

2. Access and Site Controls.

Control Activities and Processes. Control activities provide reasonable assurance that logical access to relevant applications, data and system resources is restricted to properly authorized individuals and programs. Sprinklr Tech Operations team is responsible for configuration and administration of the firewall and security groups to control security and access to the Sprinklr platform.

Backend infrastructure requires two level access mechanisms. For Linux servers, public key based SSH authentication is used to access the Access Server. From Access Server, LDAP authentication is used to access other servers. LDAP authentication is based on User ID and Password. For Windows servers, RDP over SSL is used for both legs.

Access to applications is achieved via HTTPS, providing secure encrypted transport sessions to the application. Sprinklr utilizes user access using a role-based access control (RBAC) approach, where role is used to determine user access to only required features and functions.

As part of Sprinklr's Supplementary Measures, all sensitive data used by the system is stored encrypted conforming to industry standard practices, and direct access privilege to data store instances is given to database administrators only. There is no direct end-user access to the data store. End-user access is available only via the application.

The completion of the SOC 1 Type I and II and SOC 2 Type I and II examination typifies Sprinklr's continued commitment to create and maintain the most stringent controls needed to ensure the highest quality and security of service provided to its Customers.

The system is deployed on Linux and Windows server instances via Amazon Elastic Compute Cloud (EC2) managed service, which provides reliable and flexible server deployment including OS level patches.

Firewalls and host-based intrusion detection systems are deployed on the system. All security monitoring systems including, but not limited to, firewalls and host intrusion detection systems are deployed and enabled.

All infrastructure platforms and services (operating systems, web servers, database servers, firewalls, etc.) are configured according to industry best practices. Sprinklr IT Operations team is responsible for configuration and administration of the firewall using security groups to control security and access to “internal” network infrastructure.

The Data Importer has, and maintains, a security policy for its personnel, and requires security training as part of the training package for its personnel. The Data Importer’s infrastructure security personnel are responsible for the ongoing monitoring of the Data Importer’s security infrastructure, the review of the Services, and for responding to security incidents.

Access Control and Privilege Management. The Data Exporter’s administrators and end users must authenticate themselves via a central authentication system or via a single sign on system in order to use the Services. Each application checks credentials in order to allow the display of data to an authorized User or authorized administrator.

3. Data

Data Storage, Isolation, Authentication, Backup and Restoration. A full snapshot of the production environment database is performed on a daily basis. Database backups (DB) are taken using tools provided by the Sprinklr cloud vendor(s) and database snapshots (DB Snapshots) are taken on on-demand (during critical releases). The automated backup enables point-in-time recovery of your DB Instance. Sprinklr performs a full daily snapshot of the data and captures transaction logs (as updates to DB Instance are made). When a point-in-time recovery is initiated, transaction logs are applied to the most appropriate daily backup in order to restore the DB Instance to the specific time that is required.

4. Personnel Security.

The Data Importer personnel are required to conduct themselves in a manner consistent with the company’s guidelines regarding confidentiality, business ethics, appropriate usage and professional standards. The Data Importer conducts reasonably appropriate background checks to the extent legally permissible and in accordance with applicable local labor law and statutory regulations.

Personnel are required to execute a confidentiality agreement and must acknowledge receipt of, and compliance with, the Data Importer’s confidentiality and privacy policies. Personnel are provided with security training. Personnel handling customer data are required to complete additional requirements appropriate to their role (e.g., certifications). The Data Importer’s personnel will not process customer data without authorization.

5. Sub-processor Security.

Prior to onboarding Sub-processors, the Data Importer conducts an audit of the security and privacy practices of Sub-processors to ensure Sub-processors provide a level of security and privacy appropriate to their access to data and the scope of the services they are engaged to provide. Once the Data Importer has assessed the risks presented by the Sub-processor, the Sub-processor is required to enter into appropriate security, confidentiality and privacy contract terms.