



DATA PROCESSING ADDENDUM

In providing the Sprinklr Services to Customer, Sprinklr may Process Personal Data on behalf of Customer. This Data Processing Addendum ("DPA") reflects the Customer's instructions and the parties' agreement for the Processing of Personal Data, in accordance with Data Protection Legislation. This DPA, as amended from time to time, is incorporated by reference as part of the Master Services Agreement (or other agreement for the license and purchase of the Sprinklr Services, hereinafter collectively "Agreement") between Customer and Sprinklr. Capitalized terms not defined in this DPA are defined in the Agreement.

Only to the extent that Customer is a "Covered Entity" or a "Business Associate," as defined by the Health Insurance Portability and Accountability Act ("HIPAA"), and only to the extent that Customer instructs Sprinklr to process "Protected Health Information" on Customer's behalf, the terms of the Business Associate Agreement ("BAA") between Sprinklr and Customer shall govern with respect to the processing of Protected Health Information.

This DPA will terminate automatically upon termination of the Agreement, or when Sprinklr ceases to Process Personal Data on behalf of Customer.

This DPA consists of:

- A. Data Processing Terms
- B. Data Processing Details
- C. Technical and Organizational Measures
- D. 2021 EU SCCs
- E. UK IDT Addendum

A. DATA PROCESSING TERMS

1. DEFINITIONS

To the extent not defined in the applicable Agreement, the following definitions shall apply. In the event of any inconsistencies or conflict between the Agreement and the definitions set out below, the definitions in the Agreement shall prevail.

"Account Information" means any Content other than Customer Content and Inbound Content and Customer Care Data.

"Affiliate" means any entity which is directly or indirectly controlling, controlled by, or under common control with a party to this Agreement.

"Connected Services" means the various channels and integrations supported by the Platform that Customer desires to connect to through the Platform, including the social media services.

"Content" means Inbound Content, Customer Content and Account Information entered into the Sprinklr Account or Platform or any other data managed by the Customer via the Platform.

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

"Customer Care Data" means any material that is submitted to the Platform by a person other than a Customer User through the Connected Services that the Customer has integrated into the Sprinklr Platform for purposes of customer care and support (including, where applicable under the Order Form, voice data) and specifically the Sprinklr Service module.

"Customer Content" means any material that is (i) entered into the Sprinklr Account by Customer, an Agency or employee on behalf of or under the direction of Customer (ii) generated by Customer, an Agency or employee on behalf of or under the direction of Customer, through use of the Sprinklr Platform, or (iii) published through the Sprinklr Account to the Connected Services for which Sprinklr has Connected Services Authorization.

"Customer User" means an individual user who is authorized by Customer to use the Platform and to whom Customer supplied a user identification and password. Customer Users may include, for example, Customer's employees and contractors or any other individual authorized by Customer.

"Data Protection Legislation" means all privacy, data protection, and data security laws and regulations of any jurisdiction applicable to either party's Processing of Personal Data under the Agreement. For the avoidance of doubt, a law applicable to one party does not automatically apply to the other party by virtue of this DPA.



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

"EU-US Data Privacy Framework" means the approved mechanism as developed by the US Department of Commerce and the European Commission and the UK Government, to facilitate lawful transfers of data from the UK and EU to the US. Reference to the Data Privacy Framework is inclusive of the UK Extension to the Data Privacy Framework.

"Inbound Content" means any information received from any Connected Service, including any information published on any Connected Service, not created by a Customer User. Such information includes, but is not limited to, in whatever form and/or nature, text, data, graphics, photos, audio, video, electronic messages, trademarks and other identifiers. Where applicable to the Sprinklr Services being purchased, Inbound Content may include Customer Care Data.

"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 Processed by Sprinklr in connection with the Agreement; provided that, for purposes of this DPA, the foregoing shall not include "Protected Health Information," as defined by HIPAA, which to the extent applicable, shall be addressed separately in the BAA executed by the parties.

"Personal Data Breach" means a failure of Sprinklr's security controls 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.

"Platform" means Sprinklr's proprietary customer experience software service, accessed by Customer via the internet, as specified in an applicable Order Form. Platform includes Updates made during the Term.

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

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

"Professional Services" means services other than the Platform that may be offered from time to time and that Customer elects to receive as described in an executed Statement of Work.

"SCCs" means a transfer mechanism enabling the lawful cross-border transfer of Personal Data under Data Protection Legislation, as applicable: (i) the Standard Contractual Clauses approved by the European Commission pursuant to Commission Implementing Decision (EU) 2021/914 of 4 June 2021, which are attached as Part D ("**2021 EU SCCs**"); (ii) the Addendum issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, which went into effect on 21 March 2022 and is attached as Part E ("**UK IDT Addendum**"); or (iii) Standard Contractual Clauses of any jurisdiction applicable to either party's Processing of Personal Data under the Agreement.

"Sprinklr Services" means the Platform and Professional Services.

"Subprocessor" means any Processor engaged by Sprinklr or a Sprinklr Affiliate to support with the provision of the Sprinklr Services to the Customer.

2. DATA PROCESSING DETAILS

- 2.1 The parties acknowledge and agree that with regard to the Processing of Personal Data, Sprinklr is the **Processor** and Customer and/or the Customer Affiliate determines the purposes and means of the Processing of Personal Data and is the **Controller**.
- 2.2 The parties shall each comply with their respective obligations under Data Protection Legislation. Customer shall, in its use of the Sprinklr Services, Process Personal Data in accordance with Data Protection Legislation, the Agreement, and Sprinklr's Acceptable Use Policy.
- 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 Customer warrants that it has an appropriate lawful basis under Data Protection Legislation to share Personal Data with Sprinklr in connection with the Sprinklr Services.
- 2.5 Unless required under applicable law, Sprinklr shall only Process Personal Data (i) in accordance with Customer's documented instructions as set out in this DPA or the Agreement, Order Form, Statement of Work or for the purposes of providing the Sprinklr Services; or (ii) to comply with other reasonable instructions provided by Customer.
- 2.6 Sprinklr shall take reasonable steps to (and instruct Subprocessors to) (i) train employees on applicable Data Protection Legislation and security requirements; (ii) instruct and train employees who have access to Personal Data on maintaining the confidentiality of the Personal Data; and (iii) limit access to Personal Data on a need-



to-know basis.

- 2.7** To the extent Sprinklr processes any de-identified data under the Agreement, Sprinklr shall (i) take reasonable measures to ensure such data cannot be associated with a natural person; and (ii) where required by Data Protection Legislation, publicly commit to maintain and use the data only in a de-identified fashion and not attempt to re-identify the data unless instructed by Customer or permitted by Data Protection Legislation.

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 Rights under Data Protection Legislation ("**DSR Request**").
- 3.2** Taking into account the nature of the Processing, Sprinklr shall assist Customer by offering appropriate technical and organizational measures, insofar as this is possible, to support Customers in their obligation to respond to a DSR Request under Data Protection Legislation.
- 3.3** To the extent Customer does not have the ability to address a DSR Request using the measures offered by Sprinklr in Section 3.2 and the response to such DSR Request is legally required, Customer may request commercially reasonable assistance in responding to such a DSR Request. Customer shall be responsible for any costs arising from Sprinklr's provision of assistance under this Section 3.3, which exceeds Sprinklr's legally required support of Customers in the fulfillment of their obligations in relation to DSR Requests.

4. DATA PROTECTION IMPACT ASSESSMENTS

As required under Data Protection Legislation and to the extent the information is known, available, and relates to the Processing of Personal Data under the Agreement, Sprinklr shall provide reasonable assistance to Customer with data protection impact assessments and consultations with a supervisory authority.

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. Where possible, and to the extent applicable, Sprinklr shall provide Customer with sufficient information to allow Customer to meet any legally required notification obligations. To the extent known to Sprinklr, the information provided shall include:
- (a) the nature of the Personal Data Breach including where applicable, the categories and approximate number of Data Subjects concerned, and the categories and approximate volume of Personal Data records concerned;
 - (b) the likely consequences and impact of the Personal Data Breach;
 - (c) the measures taken or proposed to be taken by Sprinklr to address the Personal Data Breach, including, where appropriate, measures to mitigate its possible adverse effects; and
 - (d) the name and contact details of the DPO (if relevant) or a point of contact from whom more information can be obtained.
- 5.2** Sprinklr shall make reasonable efforts to identify the cause of a Personal Data Breach and take the steps Sprinklr deems possible, necessary, and reasonable to remediate such cause to the extent the remediation is within Sprinklr's reasonable control.
- 5.3** The obligations with regards to remediation in 5.2 above shall not apply to Personal Data Breaches that are caused by Customer.

6. SECURITY AND OTHER SUPPLEMENTARY MEASURES

Sprinklr shall implement and maintain appropriate technical and organizational measures to protect Personal Data and Customer Content against a Personal Data Breach, as defined in the ***Enterprise Security Addendum*** located at www.sprinklr.com/legal.

7. THIRD PARTY DISCLOSURES

- 7.1** Sprinklr agrees not to allow, unless required by applicable law, regulations, order of a court or any regulatory, judicial, governmental, or similar body, or as authorized by Customer, access to Customer Content (including Personal Data but excluding any publicly available data) by any administrative body, authority or agency.
- 7.2** Customer acknowledges that Sprinklr may be required by law to allow such access to Customer Content. Where Sprinklr receives such a demand, Sprinklr shall, where legally permitted, seek to redirect the demand to Customer, and Customer agrees that Sprinklr may provide information as reasonably necessary to facilitate such a redirect. If Sprinklr is not able to redirect the demand to the Customer, then 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 Content that must be disclosed. For the avoidance of any doubt, this shall in no way prejudice Sprinklr's obligations arising out Clause 15.2 of the 2021 EU SCCs.

8. DELETION OR RETURN OF PERSONAL DATA

- 8.1** Sprinklr shall delete the Personal Data (a) upon termination/expiry of the Agreement, (b) in accordance with the selected retention package as specified in the Order Form and configured by the Customer; and/or (c) upon Customer's reasonable request at any time. Sprinklr may retain Personal Data to the extent legally required and only to the extent and for such period as legally required, and always provided that Sprinklr shall ensure the confidentiality of the Personal Data and that such Personal Data is only Processed as necessary for the legally required purpose(s).
- 8.2** Upon request, Sprinklr shall make available technical measures for the Customer to obtain certain Personal Data prior to termination of the Agreement.

9. AUDITS AND INSPECTIONS

- 9.1** Subject to the terms of this Section 9, Sprinklr shall make available to Customer reasonable information necessary to demonstrate compliance with the Agreement and shall allow for and contribute to an annual audit by Customer or a mutually agreed to third-party auditor ("Auditor") in relation to the Processing of Customer Content.
- 9.2** Customer or Auditor may, in accordance with applicable law, at Customer's expense and no more than annually perform an on-site audit of Sprinklr's data protection and information security practices with written notice provided reasonably, but at least thirty (30) business days, in advance. The audit shall take place over not more than one day, unless Sprinklr permits otherwise, during Sprinklr's normal business hours on a mutually agreed schedule that will minimize the audit's impact on Sprinklr's operations. Customer or Auditor shall comply with Sprinklr's security requirements related to the performance of the audit. Due to confidentiality and security requirements, such audit shall exclude on-site inspections of other Sprinklr customer environments or multi-tenant environments (such as IaaS data centers or other shared services used by Sprinklr). The limitations in this Section 9.2 apply to any type of assessment, review, questionnaire or audit.
- 9.3** Upon Customer's written request and no more than once per year, Sprinklr shall complete Customer's reasonable data protection and information security questionnaire. Sprinklr may refuse to provide answers to questions or information requests which, if broadly made available, could lead to (i) disclosure of sensitive Sprinklr intellectual property or trade secrets; (ii) disclosure of non-public information of other Sprinklr customers or Data Subjects or (iii) a material weakening of Sprinklr's security controls. If any assessment, questionnaire, or review conducted by the Customer or Auditor involves activities similar to those typically performed in an on-site audit (including but not limited to the submission of evidence, virtual or in-person meetings, and engagement of multiple Sprinklr personnel), such assessment shall be considered equivalent to an audit under the terms of this Agreement and shall count toward the one (1) audit allowed per calendar year and adhere to terms established in this section 9.
- 9.4** Audits performed via online video-sharing conferencing tools are considered on-site audits.
- 9.5** If the controls or measures to be assessed in the requested audit are addressed in a SOC 2 Type 2 report or similar and current qualified third-party audit report or certificate, Customer agrees to accept such report in lieu of requesting an audit.
- 9.6** All information provided to Customer or Auditor is considered Sprinklr Confidential Information. 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 or 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 to under the Agreement. 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 Agreement and all DPAs together. In particular, it shall not be understood to apply individually and severally to Customer and/or to any of Customer's Affiliates.
- 10.2** The mandatory statutory provisions in Data Protection Legislation, apply in the event of compensation or liability claims from a Data Subject. The parties' liability towards each other remains subject to the limitation of liability section in the Agreement.
- 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. SUBPROCESSORS

- 11.1** Sprinklr has Customer's general authorization to use the Subprocessors listed at



www.sprinklr.com/subprocessors, provided that Sprinklr shall (i) carry out adequate diligence prior to engaging the Subprocessor to select Subprocessors that are capable of maintaining the privacy, confidentiality, security, integrity, and availability of Personal Data consistent with the requirements of this DPA; and (ii) ensure that the arrangement between Sprinklr and Subprocessor is governed by a binding contract that includes terms which offer a substantially similar level of protection for Personal Data as those set forth in this DPA and which meet the requirements of Data Protection Legislation.

- 11.2** If Subprocessors are replaced or added during the term of the Agreement, Sprinklr shall give customer notice of such changes 30 days prior, provided Customer has subscribed to receive email notifications of such changes at www.sprinklr.com/subprocessors. Customer shall have 15 days from receipt of that notice to raise a material objection to the change and Sprinklr and Customer shall work together in good faith to cure any material objection. If no material objection is raised within the objection period, the proposed Subprocessor will be deemed agreed and authorized to Process Personal Data.
- 11.3** Sprinklr will remain liable to the Customer for the acts and omissions of Sprinklr's Subprocessors to the extent they relate to the provision of the Sprinklr Services to the Customer, subject always to the limitations of liability in the Agreement.

12. CCPA

- 12.1** This section shall only apply where the California Consumer Privacy Act of 2018, as amended by the California Privacy Rights Act of 2020 ("**CCPA**") is applicable to either party's Processing of Personal Information under the Agreement. For purposes of this Section 12, the terms "**Commercial Purpose**," "**Sell**," "**Service Provider**," and "**Share**" shall have the respective meanings given thereto in the CCPA, and "**Personal Information**" shall mean Personal Data that constitutes Personal Information governed by the CCPA.
- 12.2** It is the Parties' intent that with respect to any Personal Information, Sprinklr is the Service Provider. Sprinklr (i) acknowledges that Personal Information is disclosed by Customer only for limited and specified purposes described in the Agreement; (ii) shall comply with applicable obligations under the CCPA, and shall provide the same level of privacy protection to Personal Information as is required by the CCPA; (iii) agrees that Customer has the right to take reasonable and appropriate steps under Section 9 of the DPA to help ensure that Sprinklr's use of Personal Information is consistent with Customer's obligations under the CCPA; (iv) shall notify Customer in writing of any determination made by Sprinklr that it can no longer meet its obligations under the CCPA; and (v) agrees that Customer has the right, upon notice, including pursuant to the preceding clause, to take reasonable and appropriate steps to stop and remediate use of Personal Information.
- 12.3** Sprinklr, shall not (i) Sell or Share any Personal Information; (ii) retain, use, or disclose any Personal Information for any purpose other than for the specific Business Purpose of providing the Sprinklr Services under and in accordance with this Agreement, including retaining, using, or disclosing Personal Information for a Commercial Purpose other than the Business Purpose of providing the Sprinklr Services or as otherwise permitted by the Agreement or applicable law; (iii) retain, use, or disclose the Personal Information outside of the direct business relationship between Customer and Sprinklr; or (iv) combine Personal Information received pursuant to the Agreement with Personal Information (a) received from or behalf of another person or (b) or collected from Sprinklr's own interaction with any Consumer to whom such Personal Information pertains, except as otherwise permitted under the Agreement or Applicable Law.
- 12.4** Customer agrees that Sprinklr notifying Customer of Subprocessor engagements in accordance with Section 11 of this DPA shall satisfy Sprinklr's obligation under the CCPA to give notice of such engagements.
- 12.5** The Parties acknowledge that Sprinklr's retention, use, and disclosure of Personal Information authorized by Customer's instructions documented in the DPA are integral to the provision of the Sprinklr Services and the business relationship between the Parties.

13. INTERNATIONAL PERSONAL DATA TRANSFERS

- 13.1** Customer acknowledges and accepts that Sprinklr's provision of Sprinklr Services under the Agreement may involve the transfer of Personal Data to, or the Processing of Personal Data in, locations outside of the originating region, including to any country in which Sprinklr, Sprinklr Affiliates, or Sprinklr Subprocessors Process Personal Data in the performance of their services. Customer agrees that such transfers are permitted, provided that they comply with Data Protection Legislation and are consistent with the safeguards included in this Section 13, to the extent applicable.
- 13.2** Sprinklr, Inc. is an active participant in the EU-US Data Privacy Framework and the UK and Swiss Extensions and agrees to maintain its participation in this framework. If Customer chooses to rely on the EU-US Data Privacy Framework and its Extensions as an adequate method of transferring Personal Data to Sprinklr it shall be referenced in Part D of the DPA. To the extent the Data Privacy Framework may be invalidated, or another transfer mechanism is required or relied on, such as Standard Contractual Clauses, it shall be referenced in



part D of this DPA.

13.3 In the event of any conflict or inconsistency between this DPA and the relevant SCCs the relevant SCCs shall prevail.

14. CHANGE IN LAWS

Either party may, on notice, amend this DPA upon agreement with the other party, to the extent reasonably necessary to address the requirements of Data Protection Legislation including by replacing the relevant SCCs with (i) any new form of the relevant SCCs or any replacement thereof prepared and populated accordingly, or (ii) another transfer mechanism, other than the SCCs.

15. TERMINATION

Any termination rights arising from a breach of a provision in this DPA shall be in accordance with the termination provisions set forth in the Agreement.

B. PARTIES AND DATA PROCESSING DETAILS

LIST OF PARTIES

Data exporter(s): Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union.

Name	[...}
Address	[...}
Contact Person's name, position, and contact details	[...}
Activities Relevant to the data transferred under these Clauses:	The data exporter is a licensee and user of the Sprinklr platform.
Role (controller/processor):	Controller

Data importer(s): Identity and contact details of the data importer(s) and, where applicable, of its/their data protection officer and/or representative in the European Union.

Name	Sprinklr, Inc.
Address	441 9th Avenue, 12th Floor, New York, NY 10001
Contact Person's name, position, and contact details	privacy@sprinklr.com - DPO
Activities Relevant to the data transferred under these Clauses:	The data importer provides the Sprinklr Platform (SaaS), a customer experience and social media management platform.
Role (controller/processor):	Processor



DETAILS OF PROCESSING AND DESCRIPTION OF TRANSFER

Categories of Data Subjects:	<ol style="list-style-type: none">1. Customer's employees, agents and subcontractors who are operating the Sprinklr Platform, as well as individuals collaborating and communicating with Customer's customers, followers, fans, and other Internet users who use social networks and websites.2. Any data subjects whose information is uploaded or stored by Customer into the Sprinklr Platform, including commercial contacts, prospects, or marketing contacts.3. Customer's customers, followers, fans, and other Internet users who use social media networks and websites, blogs, forums, review sites, mainstream news sources, or any other website, including websites owned by Customer where Sprinklr provides social and content management functionality on Customer's behalf, or which Customer has integrated into the Sprinklr Platform.
Categories of Personal Data	<ol style="list-style-type: none">1. Account Information, which includes Personal Data such as identification data (name, login), contact information (business email address), work related information (job title or role, social information (social contact handling data), and usage information (performance data, device data, and location data).2. Inbound Content, which includes any Personal Data published or sent by third parties, (e.g., social media users) via the Connected Services, including Customer's social media profiles which are integrated into the Sprinklr Platform, as well as publicly accessible data from the social media networks or other websites used for social and content management and research capabilities. Inbound Content may include user IDs, social network profile names and information, social network communications (both public and private messages to Customer), information shared across social media networks and other websites, such as comments, reviews, reactions, and engagement and associated metadata.3. Customer Care Data, which includes any Personal Data submitted by Customer's customers, followers, fans, and other individuals to Customer for purposes of customer care and support (including, where applicable under the relevant Order Form, voice data).4. Customer Content, which includes any other category of Personal Data Customer provides as part of the Customer Content.
Special Categories of Data, Sensitive Data, and Safeguards	<p>Sprinklr does not require special categories of data to provide its services, but such data may be processed if:</p> <ol style="list-style-type: none">1. Customer enables certain optional Platform features which require the processing of special categories of data.2. Customer Content contains special categories of data, depending on what kind of data Customer uploads/stores into the Sprinklr Platform.3. Inbound Content or Customer Care Data contains special categories of data, depending on what information individuals choose to provide through social networks, public internet sources, or as part of customer care and support inquiries. <p>Sprinklr applies a consistent protection framework for all Personal Data, including special categories of data, and such controls include (i) address physical and logical access limitation based on a need-to-know principle; (ii) usage exclusively for providing the Sprinklr Services, as instructed by the Customer; (iii) adequate training for all operational staff with access to highly sensitive data; (iv) comprehensive logging; (v) encryption of data where technically feasible; and (vi) data destruction using industry standard destruction procedures.</p>
Frequency of Transfer	Continuous.



Nature of Processing	Sprinklr processes, stores, collects, records, discloses by transmission, and erases Personal Data as a data Processor to provide the Sprinklr Platform and Sprinklr Services as contracted in the Agreement, in accordance with and only on Customer's instructions.
Purpose of Processing	Personal Data is Processed for the following purposes: (1) Account Information is processed to operate the Sprinklr Platform and provide the Sprinklr Services (authentication, login, and audit trail) (2) Inbound Content, Customer Care Data, and Customer Content is processed for purposes of providing the Sprinklr Services, including social media management, social media listening and analytics, customer care and support, marketing analytics, and marketing management.
Duration of Processing/Retention Period	Sprinklr shall delete Personal Data (a) upon termination/expiry of the Agreement (b) in accordance with the selected retention package as specified in the Order Form and configured by the Customer, and/or (c) upon Customer's reasonable request at any time. Sprinklr may retain Personal Data to the extent legally required and only to the extent and for such period as legally required, provided that Sprinklr shall ensure the confidentiality of all such Personal Data and that such Personal Data is only Processed as necessary for the legally required purpose(s).

C. TECHNICAL AND ORGANIZATIONAL MEASURES

As set out in the Enterprise Security Addendum ("ESA"), available at www.sprinklr.com/legal.

D. 2021 EU STANDARD CONTRACTUAL CLAUSES

Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council.

1. SIGNATURE OF THE EU SCCs

- 1.1** Where applicable and in accordance with Section 13 of this DPA, each of the Parties is hereby deemed to have signed the EU SCCs at the relevant signature block in Annex I to the Appendix to the EU SCCs and the EU SCCs are entered into by and between the Parties with effect from (a) the DPA effective date, or (b) the date of the first EU International Transfer to which they apply, in accordance with Section 13 of this DPA, whichever is later.
- 1.2** In respect to any given International Transfer, on request from Customer, Sprinklr shall promptly, and in any event within ten (10) business days, execute full-form versions of the EU SCCs, which shall be amended and populated in accordance with this Part D.

2. MODULES

- 2.1** Taking into account the Parties to this DPA and the nature of the data flows, the following modules of the EU SCCs apply in the following manner:
- (a) where Customer is the Controller, Sprinklr is the processor, and Module 2 (Transfer controller to processor) applies.
 - (b) Where Customer Affiliate is the Controller, Customer is the Processor, Sprinklr is the Sub-Processor, and Module 3 (Transfer processor to processor) applies.

3. POPULATION OF THE BODY OF THE EU SCCs

- 3.1** Clause 7, the optional docking clause, applies.



- 3.2** Under Clause 9 (Use of Sub-Processors), the Parties select Option 2 (General Written Authorization). The current list of Sub-processors is set forth in Section 11, above. Sprinklr shall provide written notice at least thirty (30) days prior to any intended additions or replacements of Sub-Processors.
- 3.3** Under Clause 11 (Redress), the optional requirement that the data subjects be permitted to lodge a complaint with an independent dispute resolution body does not apply.
- 3.4** Under Clause 17 (Governing Law), the Parties choose Option 1 (the law of an EU Member State that allows for third-party beneficiary rights). The Parties select the law of Germany.
- 3.5** Under Clause 18 (Choice of Forum and Jurisdiction), the Parties select the courts of Germany.

4. POPULATION OF THE ANNEXES IN THE EU SCC APPENDICES

- 4.1** The entirety of Annex I to the EU SCCs is populated with the corresponding information detailed in Part B (*Data Processing Details*) to this DPA, with (a) Customer being Data Exporter and (b) Sprinklr being Data Importer is populated with the corresponding information detailed in Part B (*Data Processing Details*) to this DPA.
- 4.2** Annex II to the EU SCCs is populated with the security measures set forth in Part C (*Technical and Organizational Measures*) to this DPA.
- 4.3** Annex III to the EU SCCs is populated with Sprinklr's current List of Subprocessors can be accessed at www.sprinklr.com/legal, and Sprinklr has Customer's general authorization for use of these Subprocessors. Sprinklr will inform the Customer via electronic means of any changes to that list in the event Subprocessors are added or replaced during the term of the Agreement in accordance with Clause 9(a), Option 2 and the process set out in Section 11 of the DPA.

E. UK International Data Transfer Addendum to the EU Commission Standard Contractual Clauses

The Addendum issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, which went into effect on 21 March 2022.

This Addendum has been issued by the Information Commissioner for Parties making Restricted Transfers. The Information Commissioner considers that it provides Appropriate Safeguards for Restricted Transfers when it is entered into as a legally binding contract.

Part 1: Tables

Table 1: Parties

Start Date	as per Agreement	
The Parties	Exporter (Who sends the Restricted Transfer)	Importer (who receives the Restricted Transfer)
Parties Details	As set out in Part B (<i>List of Parties and Data Processing Details</i>).	As set out in Part B (<i>List of Parties and Data Processing Details</i>).
Contact Person's name, position, and contact details	As set out in Part B (<i>List of Parties and Data Processing Details</i>).	As set out in Part B (<i>List of Parties and Data Processing Details</i>).

Table 2: Selected SCCs, Modules and Selected Clauses

Addendum to EU SCCs	The Approved EU SCCs, including the Appendix Information and with only the following modules, clauses or optional provisions of the Approved EU SCCs brought into effect for the purposes of this Addendum:
----------------------------	---



Module	Module in Operation	Clause 7 (Docking Clause)	Clause 11 (Option)	Clause 9(a) (Prior Authorization or General Authorization)	Clause 9(a) (Time Period)	Is personal data received from the importer combined with Personal Data Collected by Exporter
1						
2	X	Yes	No	General Authorization	30 days	
3	X	Yes	No	General Authorization	30 days	
4						

Table 3: Appendix Information

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

Annex 1A: List of Parties: see Annex I(A) of the 2021 EU SCCs, above

Annex 1B: Description of Transfer: see Annex I(B) of the 2021 EU SCCs, above

Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data: see Annex II of the 2021 EU SCCs, above

Annex III: List of Sub processors (Modules 2 and 3 only): see Annex III of the 2021 EU SCCs, above

Table 4: Ending this Addendum when the Approved Addendum Changes

Ending this Addendum when the Approved Addendum Changes	Which Parties may end this addendum as set out in Section 19: {X} Importer (X) Exporter () neither party
--	--

Part 2: Mandatory Clauses

Mandatory Clauses	Part 2: Mandatory Clauses of the Approved Addendum, being the template Addendum B.1.0 issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act on 2 February 2022, as it is revised under 18 of those Mandatory Clauses.
--------------------------	--