Sprinklr Contracts FAQ:
Who is Sprinklr and What do we Do?

These Sprinklr Contracts FAQs intend to provide some background information on Sprinklr's products and services to give a better understanding of our offerings and to facilitate the review of our Master Services Agreement. While the folks in the front office know what we do, often, attorneys and contract professionals are sent contracts from Sprinklr to review, without having an understanding of who we are, what is being purchased and how we provide that product or service so we've outlined below many of the common questions around those products and services to help with that. This FAQ document does not form part of the agreement between you and Sprinklr.

➢ **What does Sprinklr Sell and What is being Purchased?**

Sprinklr offers the only unified Customer Experience Management Platform which includes a number of products and services (the "Platform"), and is purpose-built to help large enterprises make their customers happier. The Platform integrates with over 30 digital channels and uses Sprinklr's unique AI to create insights to provide their customers with deeper, real-time customer experiences. Sprinklr is a cloud based Software as a Service ("SaaS") application provided over the Internet, in a multi-tenant hosted environment. Being SaaS, all customers use the same version of the Platform. For more information, please visit www.sprinklr.com.

➢ **What kind of data is processed by the Sprinklr Platform?**

The data collected and processed by Sprinklr in the context of the provisioning of Sprinklr's services for our customers includes (i) customer and customer employee data that is needed to manage our customer relationships and enable access to Sprinklr's services ("**Account Information"**); (ii) any data that customer end users upload or stored in the Platform or that is published through Sprinklr to channels and integrations supported by the Platform and authorized by customers (**"Customer Content"**); (iii) any data that is submitted to the Platform through channels and integrations by individuals who are seeking customer care and support from Sprinklr's customers ("**Customer Care Data**"); and (iv) any other data received from a third party through any of the integrated services, such as social media channels (**"Inbound Content"**). Collectively, all these data types are referred to as **"Content"** throughout the Master Services Agreement. Sprinklr's customers authorize Sprinklr to connect to a number of digital channels including CRM systems, public media sources, and social media accounts and can unilaterally determine the scope of the data being consumed and the type of data processing. The data collected and processed by Sprinklr on behalf of its customers is primarily publicly accessible data, in particular social media messages and posts published by the users of the various social media networks, reviews, blog posts and other online content.

➢ **What is Sprinklr's approach to Data Protection?**

Data protection and compliance with data protection legislation is of paramount importance to Sprinklr. Sprinklr takes its data protection obligations very seriously and has a robust privacy programme. Sprinklr respects all laws applicable to Sprinklr and our internal legal team monitors and assesses new privacy laws to promote ongoing compliance. Where there are adjustments to the regulatory landscape that mean we need to make adjustments to our contracts, policies and product or service offering or website for example, we instigate internal processes to ensure compliance. We also have appointed an external and independent Data Protection Officer to support our compliance with applicable data privacy laws. You can learn more about Sprinklr's privacy program and get access to documentation and resources at www.sprinklr.com/trust.

Sprinklr processes personal data at our customer's instruction and in accordance with the limitations and instructions included in our Master Services Agreement and Data Protection Agreement (DPA). The DPA, which is available at www.sprinklr.com/legal, documents customer instructions on data processing and records the obligations imposed on Sprinklr in accordance with certain data protection legislation. Sprinklr leverages the 2021 EU Standard Contractual Clauses (SCCs) and the UK International Data Transfer Addendum to enable cross-border data transfer of personal information for transfers out of the EEA/UK, and SCCs will be entered into between the contracting parties. Sprinklr's DPA also lists the technical and organizational measures Sprinklr deploys as additional safeguards for those transfers of data.

Sprinklr is committed to transparency with regards to its data processing operations, including identifying all sub-processors used by Sprinklr. Sprinklr has several types of sub-processors, including affiliates and third party sub-processors. For a full list of sub-processors and to subscribe for updates, please visit www.sprinklr.com/legal. Sprinklr obligates its sub-processors to contractual obligations that are substantially similar to those imposed on Sprinklr under the DPA with our customers.

The Sprinklr platform establishes tooling to enable our customers to respond to data subject requests for access, rectification, objection, restriction, portability, and deletion (right to be forgotten) in an efficient way, directly via the user interface and/or via an API.

Sprinklr informs every employee of their data protection and confidentiality obligations. Every employee participates in mandatory data protection and information security training and is contractually or statutorily obliged to confidentiality. Sprinklr has a dedicated privacy team and also appointed a third party Data Protection Officer.

➢ **How does Sprinklr protect customer data?**

Sprinklr is a multi-tenant SaaS product which is hosted in a virtual private cloud (VPC). This means that your data shares the physical environment with other Sprinklr customers but is logically isolated for additional security. This hosting environment creates a high availability redundant enterprise grade installation with strong security. Sprinklr holds SOC 2 Type 2 and ISO 27001 certifications. Sprinklr encrypts data in transit and data at rest. In addition, Sprinklr has contracts or terms in place with all supported channel integrations, and these contracts impose obligations which Sprinklr must enforce to ensure that prohibited content is not allowed to be posted via the Sprinklr system.

Since Sprinklr is a multi-tenant system, we must protect the confidentiality of other customers sharing the environment. This places restrictions on the access we provide to our customers and the ability to audit and inspect our security environment.

Customers may, upon request, audit, inspect and approve SOW subcontractors who are working under a specific SOW which mentions that subcontractor by name. Multi-tenant subcontractors such as hosting or data providers, are not available for audit, inspection or approval to any customer in the multi-tenant environment. This policy is designed to ensure that all Sprinklr customers' data is protected. More information about Sprinklr's security program and the measures to protect our customers' data is provided in the Enterprise Security Addendum, attached to the MSA, as well as Sprinklr's Trust Portal, available at www.sprinklr.com/trust.

➢ **Does Sprinklr Access Protected Health Information?**

Sprinklr does not require access to Protected Health Information (PHI) to provide its services, but for those customers who are subject to the Health Insurance Portability and Accountability Act (HIPAA) and who will be providing Sprinklr with access to PHI, as defined by HIPAA, Sprinklr requires customer to: (1) inform Sprinklr that there will be such access; (2) execute an applicable Order Form, SOW, and a Business Associate Agreement. Customers wishing to process PHI with Sprinklr can only do so using HIPAA Eligible Sprinklr Services.

➢ **What happens to my Data on Termination or Expiration of the Agreement?**

Data is retained in accordance with the Active Data Retention packages as stated in the Service Level Agreement (SLA). The selected retention package is specified on the Order Form. For those customers who do not provide PHI to Sprinklr, upon request within thirty (30) days after the effective date of termination or expiration of the Agreement, Sprinklr will delete customer's available content from the Platform or extract such data and provide a copy to customer if customer requests a copy, at Customer's expense. Data is retained in accordance with the Active Data Retention packages as stated in the Service Level Agreement (SLA). The selected retention package is specified on the Order Form. For those customers who provide PHI to Sprinklr, such retention and destruction requirements will be governed by the applicable Business Associate Agreement executed by the parties.

➢ **What is Sprinklr's Service Level Agreement ("SLA")?**

Sprinklr's SLA can be found at www.sprinklr.com/legal. All customers of Sprinklr are on the same version of the Platform. We cannot modify this SLA on a customer by customer basis, as we would not be able to scale our operations without uniformity across our entire customer base.

➢ **What is Sprinklr's Acceptable Use Policy ("AUP")?**

Sprinklr's AUP can be found at www.sprinklr.com/legal. We have created this policy to make it very clear what can and cannot be done with the Sprinklr Platform. Much of this is required by the channels and integrations that our Platform interacts with. As a result, this is required to be accepted by our customers without any amendments.

➢ **What are Sprinklr's Standard Payment Terms?**

Sprinklr invoices for all fees upon execution of an order form and/or statement of work. Payment terms are thirty (30) days from the date of the invoice.

➢ **Does Sprinklr offer Termination for Convenience?**

Sprinklr does not allow termination of an agreement, order form or statement of work for convenience. Sprinklr sets its prices based on a committed term as set forth in an order form and any right to terminate without cause impacts our ability to book the contract or to recognize revenue on the contract upon signature. It is fundamental to Sprinklr's business that each party is committed to a term upon execution of an agreement, order form or statement of work, other than a termination due to breach.

➢ **Does Sprinklr allow Acceptance Testing of the Platform?**

SaaS models are fundamentally different than other methods of software delivery. Sprinklr operates a SaaS, multi-tenant environment that runs the Platform for all customers on a "single code line". The Platform that you license is the Platform readily available to, and already used by over 1,500 customers of Sprinklr, and is simply enabled for your use. The concept of acceptance of this Platform does not exist in Sprinklr's SaaS business model. Sprinklr's standard MSA provides warranties, support and SLA's in case the Platform is not operating in accordance with the terms of the agreement.

➢ **Does Sprinklr Provide an Indemnification?**

Pursuant to Section 6.1 of the MSA, if a third party claims that you have infringed on their IP rights as a result of using the Sprinklr Platform in accordance with the terms of the MSA, we stand behind our Platform and we will indemnify you for any such claims. Sprinklr also requires an indemnity from our customers for any third party claims resulting from a customer's breach of Sprinklr's AUP.

➢ **Does Sprinklr Provide Unlimited Liability?**

Sprinklr understands the importance of each party's liability and we agree to have caps that are fair for both Sprinklr and customers. Sprinklr, in line with industry standard, believes that the liability of each party should correlate directly to the value of the agreement between the parties. To achieve this goal, Sprinklr excludes indirect damages for both parties in all circumstances. In addition, Sprinklr's mutual limitation of liability for direct damages in a contract is the fees paid by a customer in the twelve (12) months prior to the event giving rise to the liability. There are three exceptions to the direct damages limitation, these are (i) either party's gross negligence or willful misconduct, (ii) each party's standard indemnification obligations as stated in our MSA, and (iii) a customer reverse engineering, or misappropriating Sprinklr's Intellectual Property. Sprinklr does not agree to, nor do we ask for, any other liabilities to be accepted on an unlimited basis. Our Platform and Intellectual Property is what our company is built upon, and we cannot agree that a Customer could have any limit on direct damages if they attempt to take that Intellectual Property. Sprinklr does understand that breaches of confidentiality and breaches of data protection are important to our customers, and, as a result, we agree to offer a separate, higher liability cap for these breaches (Two times (2x) twelve (12) months fees).

MASTER SERVICES AGREEMENT (EUROPE-CH)

1. DEFINITIONS

"**Account Information**" means any Content other than Customer Content and Inbound Content (including Customer Care Data). Account Information which includes Customer's Personal Data (as defined in the Data Processing Addendum) shall be deemed to constitute Customer Content.

"**Acceptable Use Policy**" means Sprinklr's Acceptable Use Policy, located at www.sprinklr.com/legal.

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

"**Agency**" means Customer's representatives, advertising agencies and/or other Customer service providers.

"**Business Associate Agreement**" or "**BAA**" Sprinklr's standard HIPAA Business Associate Agreement located at www.sprinklr.com/legal, unless a separate Business Associate Agreement is executed by the parties, in which case such executed Business Associate Agreement shall apply.

"**Connected Services**" means the various channels and integrations supported by the Platform that Customer connects to, or authorizes a third party to connect to, through the Platform, including the social media services.

"**Connected Services Authorization**" means the authorization relating to the Customer's Connected Services accounts, which enable the Platform to interact with Customer's Connected Services accounts.

"**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.

"**Contractor**" means subcontractors, suppliers, resellers and advisors.

"**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).

"**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 or (ii) 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 and Agency's employees and contractors.

"**Data Processing Addendum**" means Sprinklr's Data Processing Addendum, located at www.sprinklr.com/legal

"**Force Majeure Event**" means circumstances beyond a party's reasonable control, including but not limited to acts of God, fire, labor difficulties, terrorism, failure of third party networks or the public internet, power outages, or governmental demands or restrictions.

"**HIPAA**" means the Health Insurance Portability and Accountability Act, as amended, and its implementing regulations.

"**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.

"**Internal Use**" means use of the Sprinklr Services for Customer's and/or Customer Affiliates' general business use, solely for the benefit of Customer and/or Customer Affiliates, but does not include use of the Sprinklr Services to provide any services for the benefit of third parties.

"**Order Form**" means a written order executed by the parties which defines the respective order parameters and Platform information, such as, modules purchased, term and associated fees.

"**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.

"**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 SOW.

"**Protected Health Information**" or "**PHI**" is as defined by HIPAA.

"**SLA**" means Sprinklr's Service Level Agreement, located at www.sprinklr.com/legal.

"**SOW**" (Statement of Work) means a written order executed by the parties which identifies the Professional Services ordered by Customer, including the description, and associated fees.

"**Sprinklr Account**" means Customer's password restricted account to access and use the Platform.

"**Sprinklr Services**" means the Platform and Professional Services.

"**Updates**" means modifications, updates and changes made by Sprinklr to the Platform which Sprinklr makes generally available to its customers at no additional fee. Updates exclude new features, functions and capabilities which are offered for an additional fee and must be specified in an Order Form or SOW.

"**User Guides**" means Sprinklr materials made available to Customer through the support portal to assist users of the Platform, as such materials may be updated during the Term.

2. INTELLECTUAL PROPERTY, RIGHTS OF USE

2.1 Customer owns all right, title and interest in and to all Customer Content uploaded, stored, processed or transmitted through the Platform under the Sprinklr Account.

2.2 Sprinklr owns all right, title and interest in and to the Platform, User Guide and all Sprinklr Services.

2.3 Subject to the terms and conditions of this Agreement, Sprinklr grants to Customer a non-exclusive, non transferable right to access and use the licensed modules of the Platform for Internal Use, during the Term. The Platform may be accessed and used solely by the number of Customer Users specified in the applicable Order Form(s). Sharing of Customer User accounts (user identification and password) is prohibited. Customer User accounts may only be reassigned to a new individual replacing one who will no longer use the Sprinklr Services. Customer Users shall be individual human beings, and shall not be, without limit, any form of bot, computer, AI or machine learning.

2.4 Subject to the terms and conditions of this Agreement, Customer's Affiliates and Agencies may access and use the Platform for Internal Use. All obligations of Customer shall apply equally to each Customer Affiliate and Agency that uses the Sprinklr Services; provided however, Customer shall be responsible for ensuring that all Customer Users comply with this Agreement (including, but not limited to the Acceptable Use Policy) and all acts or omissions of its Affiliates and Agencies under this Agreement.

2.5 Customer grants to Sprinklr during the term of this Agreement a royalty-free, non-exclusive, non-transferable, worldwide right and license: (i) to copy, cache, store, reproduce, perform, display, use, distribute, transmit and generally make available the Customer Content in electronic form via the Internet, through wireless communications services and social media through the Platform in order to provide the Sprinklr Services to Customer in accordance with this Agreement; and (ii) to access Customer's accounts on the Connected Services in order to provide the Sprinklr Services.

2.6 The Acceptable Use Policy, in its current version at the Effective Date of this Agreement, shall be incorporated into this Agreement, in its entirety, and Customer will comply with the Acceptable Use Policy.

2.7 The SLA, in its current version at the Effective Date of this Agreement, shall be incorporated into this Agreement, in its entirety, and Sprinklr will provide the Sprinklr Services in accordance with the SLA.

2.8 Customer will not, directly or indirectly (i) misappropriate or infringe any intellectual property rights of the Platform, including Sprinklr's and any third party rights thereto, (ii) reverse engineer, decompile, disassemble, disclose or otherwise attempt to discover the source code, object code or underlying structure, ideas or algorithms of the Platform; (iii) modify, translate, or create derivative works based on the Platform; (iv) use the Sprinklr Services for purposes of a third party or otherwise for the benefit of a third party (other than an Affiliate as permitted hereunder); or (v) use or view the Platform for the purposes of developing, directly or indirectly, a product or service competitive to the Sprinklr Services.

3. TERM AND TERMINATION

3.1 The term of this Agreement will begin on the Effective Date and continue until expiration or termination of all Order Form's and/or SOW's (the "Term"). Each Order Form and SOW will have its own term as stated in such document.

3.2 Either party may terminate this Agreement and all Order Forms and SOW's in the event that the other party (i) commits a non-remediable, material breach of the Agreement or (ii) fails to cure any remediable material breach of this Agreement, and/or any Order Form or SOW, within thirty (30) days following receipt of written notice of such breach. Notice of any material breach must be provided within ninety (90) days from learning of the material breach, for this Section 3.2 to be applicable.

3.3 Upon expiration or termination of this Agreement: (i) in the event of termination due solely to a breach by Sprinklr, then Sprinklr shall refund any prepaid fees for Services that would have been rendered after the date of termination; (ii) in the event of termination due solely to a breach by Customer, then Customer shall pay all fees through the date of termination, plus all fees through the remainder of the term of the applicable Order Form and/or SOW; (iii) all rights to use the Platform immediately cease and provision of Professional Services immediately ends; (iv) within thirty (30) days, each party will return or destroy at the disclosing party's request the other party's Confidential Information; and (v) Sections 1-2 and 6-11 shall survive, as well as any other provisions which by their terms or sense are intended to survive.

3.4 Within thirty (30) days after the effective date of termination Sprinklr will, upon Customer's request, extract all available Customer Content from the Platform. Both parties will agree to an acceptable transfer methodology, (typically Sprinklr provides an SFTP for the transfer). If Customer accounts are deactivated prior to the termination date, data contained within those accounts is not available anymore, therefore Customer must extract the data prior to deactivating accounts. After such thirty (30) day period, Sprinklr shall have no obligation to maintain or return any Customer Content. Any reasonable expenses incurred by Sprinklr as a result of this extraction shall be the responsibility of Customer.

4. FEES AND PAYMENT

4.1 Customer shall pay Sprinklr all fees set forth in each applicable Order Form and/or SOW (collectively, "Fees") within thirty (30) days of the invoice date, unless stated otherwise in an applicable Order Form and/or SOW. Customer may withhold payment of any Fees that are the subject of a good faith dispute of which Customer has provided Sprinklr written notice within five (5) business days of invoice receipt ("Disputed Fees"); provided that all Fees which are not Disputed Fees shall be timely paid, and the Disputed Fees shall be paid within ten (10) days of resolution of the dispute.

4.2 All Fees are payable in advance, are non-cancelable, and are based on the Sprinklr Services purchased, unless stated otherwise in an applicable Order Form and/or SOW.

4.3 Sprinklr reserves the right to charge Customer interest at the rate of the lesser of 1.5% per month, or the maximum rate permitted by law on any Fees not received by Sprinklr within fifteen (15) days of the payment due date. Additionally, in the event any Fees or expenses are more than thirty (30) days overdue, Sprinklr may (i) suspend its performance of the Sprinklr Services, and (ii) require full payment before Sprinklr resumes performance.

4.4 All Fees exclude taxes and Customer agrees to pay any applicable taxes charged arising from this Agreement in a timely manner, other than those based on Sprinklr's income. If Customer is tax-exempt, Customer shall provide Sprinklr with its tax-exemption number and certificate within five (5) business days after the Effective Date. Customer shall be responsible for any liability or expense incurred by Sprinklr as a result of Customer's failure or delay in paying taxes due or if Customer's claimed tax exemption is rejected. If Customer is legally required to withhold tax from its payment of Fees to Sprinklr, and/or to pay any equalization taxes, Customer agrees to gross up all Fees that are subject to such withholding tax, and shall not be entitled to reduce the Fees on an Order Form and/or SOW by any equalization taxes, such that the net payment received by Sprinklr is the full originally stated amount of such Fees.

5. WARRANTIES

5.1 Each party represents and warrants that it has the right and authority to enter into and perform its obligations under this Agreement and shall comply with all applicable laws.

5.2 Sprinklr warrants that during the Term, when used by Customer as expressly permitted hereunder, the Platform shall substantially conform to the User Guides the Sprinklr Services shall perform and be performed in all material respects in accordance with the terms of this Agreement and each Order Form or SOW. In the event Customer determines that the Platform or Sprinklr Services have not met the foregoing warranty, Customer shall give Sprinklr prompt notice of the deficiency, including details sufficient to allow Sprinklr to replicate the deficiency, and in such event Sprinklr will use commercially reasonable efforts to remedy the identified deficiency. If Sprinklr does not remedy the deficiency, either party may terminate the affected Order Form or SOW and in such case Sprinklr will refund to Customer the amount of any pre-paid Fees for the period after termination as its exclusive remedy. This warranty does not cover any problem with or damage to the Platform to the extent caused by: (i) Customer's negligence, abuse, misuse, improper handling and/or use, (ii) modifications by anyone other than Sprinklr or its Contractors; (iii) failure to operate the Platform in accordance with the User Guides; or (iv) a Force Majeure Event.

5.3 TO THE MAXIMUM EXTENT PERMITTED UNDER APPLICABLE LAW, THE SOLE AND EXCLUSIVE WARRANTIES AND WARRANTY REMEDIES ARE SET FORTH IN THIS SECTION AND, EXCEPT AS EXPRESSLY STATED IN THIS AGREEMENT, THE SPRINKLR SERVICES, INCLUDING ALL FUNCTIONS THEREOF, ARE PROVIDED ON AN "AS IS" BASIS, WITHOUT REPRESENTATIONS OR WARRANTIES OF ANY KIND WHATSOEVER, WHETHER EXPRESS, IMPLIED, ORAL OR WRITTEN, INCLUDING WITHOUT LIMITATION, ACCURACY OF CONTENT, NON-INFRINGEMENT, NON-INTERFERENCE, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR THAT THE SPRINKLR SERVICES WILL BE UNINTERRUPTED, TIMELY OR ERROR-FREE.

6. INDEMNIFICATION

6.1 Sprinklr shall indemnify, defend and hold harmless Customer and its Affiliates (the "Customer Parties") from and against any losses, liabilities, costs, expenses (including reasonable attorneys' fees and expenses), penalties, judgments, settlement amounts and damages ("Losses") incurred by a Customer Party arising from a claim, suit, action or proceeding brought by a third party (a "Claim") against any Customer Party alleging that the Sprinklr Services (excluding the Content and use of the Connected Services Authorization) when used by Customer as permitted hereunder infringes any third party intellectual property right. In the event it is held (or in Sprinklr's reasonable opinion it is likely to be held) that the Sprinklr Services when used in accordance with this Agreement and the applicable Order Form and/or SOW infringe a third party's rights, Sprinklr shall at its expense either (x) procure for Customer the right to continue using the affected elements of the Sprinklr Services, or (y) replace or modify the affected elements of the Sprinklr Service, in whole or in part, so that it becomes non-infringing but provides substantially equivalent

functionality. If Sprinklr, in its sole discretion, determines that neither (x) nor (y) are commercially reasonable, Sprinklr may terminate the provision of the affected Sprinklr Services and refund to Customer the amount of any pre-paid Fee applicable to the terminated Sprinklr Services for the period after termination. Customer acknowledges that its right to obtain indemnification and the rights described in the preceding sentence are its sole and exclusive rights in the event of such a claim. The foregoing obligation does not apply to the extent that the infringement arises from: (i) use of the Sprinklr Services in breach of the terms of this Agreement, (ii) use of the Sprinklr Services in connection with third party products used by Customer, to the extent the infringement is caused by such third party products, and (iii) any changes made to the Sprinklr Services by or on behalf of Customer.

6.2 Customer shall indemnify, defend and hold harmless Sprinklr and its Affiliates, (the "Sprinklr Parties") from and against any Losses arising from a Claim against any Sprinklr Party resulting from a breach of the Acceptable Use Policy.

6.3 The indemnification obligations contained in this Agreement are conditioned upon: (i) notice by the party seeking indemnity ("Indemnitee") to the party from whom indemnity is sought ("Indemnitor") of any Claim for which indemnity is claimed within five (5) days of the Indemnitee receiving notice of such claim (failure to meet this condition does not exempt the Indemnitor of its indemnification obligation, except to the extent that failure has materially prejudiced the Indemnitor's ability to defend the Claim); (ii) complete control of the defense and settlement of the Claim by the Indemnitor, provided that no settlement may be made without the consent of the Indemnitee, such consent not to be unreasonably withheld or delayed; and (iii) reasonable cooperation by the Indemnitee in the defense as the Indemnitor may request. The Indemnitee has the right to participate in the defense against the indemnified Claims with counsel of its choice and at its own expense but may not confess judgment, admit liability or take any other actions prejudicial to the defense. Further, the Indemnitee may not settle an Indemnified claim unless such settlement includes an unconditional release of the other party from all liability on all Claims, or the other party gives its prior written consent, which shall not be unreasonably withheld.

6.4 THIS SECTION STATES EACH PARTY'S ENTIRE LIABILITY TO THE OTHER AND EACH PARTY'S SOLE REMEDY FOR ANY THIRD-PARTY CLAIM DESCRIBED IN THIS SECTION.

7. LIMITATIONS OF LIABILITY

7.1 TO THE MAXIMUM EXTENT PERMITTED UNDER APPLICABLE LAW, IN NO EVENT SHALL EITHER PARTY BE LIABLE FOR ANY INDIRECT, SPECIAL, INCIDENTAL, PUNITIVE, OR CONSEQUENTIAL DAMAGES IN CONNECTION WITH THIS AGREEMENT, INCLUDING WITHOUT LIMITATION LOSS OF REVENUE OR ANTICIPATED PROFITS OR LOST BUSINESS OR LOST SALES OR ANY OTHER MATTER RELATING TO THE SPRINKLR SERVICES.

7.2 EXCEPT FOR (I) EITHER PARTY'S GROSS NEGLIGENCE OR WILLFUL MISCONDUCT; (II) THE PARTIES' INDEMNIFICATION OBLIGATIONS; AND/OR (III) A BREACH OF SECTION 2.8, IN NO EVENT SHALL THE TOTAL LIABILITY OF ONE PARTY TO THE OTHER PARTY FOR ANY AND ALL DAMAGES, LOSSES, AND CAUSES OF ACTION (WHETHER IN CONTRACT OR TORT, INCLUDING, BUT NOT LIMITED TO, NEGLIGENCE OR OTHERWISE), ARISING FROM THIS AGREEMENT OR CUSTOMER'S USE OF THE SPRINKLR SERVICES, EXCEED, IN THEAGGREGATE:

(I) WITH RESPECT TO A BREACH OF (a) EITHER PARTY'S CONFIDENTIALITY OBLIGATIONS HEREIN, (b) EITHER PARTY'S DATA PROTECTION OBLIGATIONS HEREIN, (c) EITHER PARTY'S SECURITY OBLIGATIONS HEREIN, AND/OR (d) EITHER PARTY'S OBLIGATIONS IN A BUSINESS ASSOCIATE AGREEMENT (IF APPLICABLE), TWOTIMES (2x) THE TOTAL FEES RECEIVED BY OR PAYABLE TO SPRINKLR FROM CUSTOMER UNDER THISAGREEMENT IN THE TWELVE (12) MONTHS IMMEDIATELY PRECEDING THE EVENT GIVING RISE TO THE LIABILITY;

(II) FOR ALL OTHER CAUSES OF ACTION, THE TOTAL FEES RECEIVED BY OR PAYABLE TO SPRINKLR FROM CUSTOMER UNDER THIS AGREEMENT IN THE TWELVE (12) MONTHS IMMEDIATELY PRECEDING THE EVENT GIVING RISE TO THE LIABILITY.

7.3 CUSTOMER ACKNOWLEDGES THAT SPRINKLR HAS SET ITS PRICES AND ENTERED INTO THIS AGREEMENT IN RELIANCE UPON THE LIMITATIONS OF LIABILITY AND THE DISCLAIMERS OF WARRANTIES AND DAMAGES SET FORTH HEREIN, AND THAT THE SAME FORM AN ESSENTIAL BASIS OF THE BARGAIN BETWEEN THE PARTIES. THE PARTIES AGREE THAT THE LIMITATIONS AND EXCLUSIONS OF LIABILITY AND DISCLAIMERS SPECIFIED IN THIS AGREEMENT WILL SURVIVE AND APPLY EVEN IF FOUND TO HAVE FAILED OF THEIR ESSENTIAL PURPOSE. IN NO EVENT SHALL THE LIMITATIONS IN THIS SECTION APPLY TO FEES DUE FOR THE SPRINKLR SERVICES UNDER THIS

AGREEMENT.

7.4   Neither party will be liable to the other for any failure to perform, or delay in the performance of, any obligation under this Agreement caused by a Force Majeure Event.

8.   CONFIDENTIALITY

8.1   "Confidential Information" means: (i) business or technical information, including product plans, designs, source code, marketing plans, business opportunities, personnel, research, development or know-how (all of the foregoing as they relate to the Sprinklr Services, including the Platform (current or planned), are Sprinklr's Confidential Information, and all of the foregoing as they relate to Customer's business, are Customer's Confidential Information); and (ii) information designated by the disclosing party as "confidential" or "proprietary" or which, under the circumstances taken as a whole, would reasonably be deemed to be confidential. Confidential Information includes information disclosed prior to or during the Term of this Agreement. Confidential Information shall not include information which: (i) is or becomes generally available to the public other than as a result of wrongful disclosure by the receiving party; (ii) is or becomes available to the receiving party on a non-confidential basis from a third party that rightfully possesses the Confidential Information and has the legal right to make such disclosure; or (iii) is developed independently by the receiving party without use of any of disclosing party's Confidential Information and by persons without access to such Confidential Information.

8.2   Customer and Sprinklr each agree not to use any Confidential Information of the other party for any purpose other than as necessary to perform its obligations under this Agreement. During and after the Term, neither receiving party will disclose any Confidential Information of the disclosing party to any third party without the prior written consent of the disclosing party, except (i) where such disclosure is necessary for the performance of the receiving party's obligations under this Agreement; or (ii) as may be required by Laws (provided that the party obligated to make the disclosure shall give the other party advance notice of such requirement to the extent legally permitted). Each receiving party shall be responsible for compliance with this Section and applicable provisions of this Agreement by its employees and Contractors, and shall obtain the agreement by each employee and Contractor to keep the Confidential Information of the disclosing party confidential and to use it solely as required for the performance of the receiving party's obligations hereunder. For purposes of clarity, Customer may publicly disclose the fact that it is using the Sprinklr Services, but all details about the uses, functionalities or other aspects of the   Sprinklr   Services (including screenshots and specific features of the Platform) are Confidential Information of Sprinklr and may not be disclosed.

9.   DATA PROTECTION AND SECURITY

9.1   The parties acknowledge and agree that with regard to the Processing of Personal Data and within the meaning of the definitions set out in the Data Processing Addendum, Sprinklr is the Processor and, unless otherwise stated in the Data Processing Addendum, Customer is the Controller, as such terms are defined in the Data Processing Addendum. During the Term of this Agreement, Sprinklr shall comply with the security measures further defined in the Enterprise Security Addendum, attached hereto as Addendum 1.

9.2   Customer acknowledges and agrees that it will not provide Sprinklr with any access to Protected Health Information without executing an applicable Order Form, SOW and Business Associate Agreement. Such terms will govern Sprinklr's access, use, and disclosure of Protected Health Information. Customer is responsible for informing Sprinklr if there will be any Protected Health Information in the Customer Content and only using HIPAA Enabled Sprinklr Services for the processing of such Protected Health Information. If not informed, or if Customer uses Sprinklr Services other than the HIPAA Enabled Sprinklr Services for the processing of Protected Health Information, Sprinklr is not liable for such Protected Health Information.

10.   GOVERNING LAW

This Agreement and any dispute or claim (including non-contractual disputes or claims) arising out of or in connection with it or its subject matter or formation shall be governed by and construed in accordance with the laws of Switzerland, excluding the United Nations Convention on Contracts for the International Sale of Goods. Each party irrevocably agrees that the courts of Bern, Switzerland shall have exclusive jurisdiction to settle any dispute or claim arising out of or in connection with this Agreement or its subject matter or formation (including non-contractual disputes or claims).

11.   MISCELLANEOUS

11.1 This Agreement incorporates any exhibits, appendices and other documents referred to in it, including, but not limited to, the Acceptable Use Policy, the SLA and/or, if applicable, any data processing agreement, and Business Associate Agreement. This Agreement together with each Order Form and/or SOW is the entire agreement between the parties relating to this subject matter, and supersedes (i) any pre-printed terms on a purchase order, which shall have no effect, and (ii) all prior or contemporaneous understandings of the parties related thereto, including any separate non-disclosure agreement between the parties relating to this subject matter as it relates to confidential information disclosed after the date of and pursuant to this Agreement. Sprinklr may amend this Agreement at any time upon giving notice to you. Such notice shall be made by sending an email to you or by publication of the amendment on the Sprinklr's website. If the amendment of this Agreement materially affects your rights related to the use of the Sprinklr Services, you may terminate the use of said Services. If you continue to use the Sprinklr Services after notice of the amendment of this Agreement is given, you shall be deemed to have agreed to this Agreement as amended. By executing this Agreement, Customer affirms and agrees that Sprinklr has not made any representations to induce Customer to enter this Agreement except for those representations explicitly set forth in this Agreement or in an Order Form or SOW entered into under this Agreement. Customer disclaims reliance upon any representations of any kind whatsoever except for those set forth in this Agreement or Order Form or SOW.

11.2 Except as may be expressly provided herein, all remedies provided for in this Agreement are non-exclusive remedies.

11.3 Either party may assign this Agreement in whole or in part (i) to an Affiliate; (ii) in connection with a merger wherethe contracting entity does not survive such merger, or (iii) in connection with the sale of all or substantially all of the contracting entity's assets related thereto. Except as expressly stated in this section, neither party may assign itsrights or obligations under this Agreement without obtaining the other party's prior written consent. Any assignment in contravention of this section is void.

11.4 Customer agrees (a) that Sprinklr may identify Customer as a Sprinklr customer in Sprinklr's marketing materials, promotional presentations, customer lists, website and other written and electronic materials (name and logo) and (b) to participate in Sprinklr customer amplification activities. Provided that all materials shall be duly approved by the Customer prior to publication, Customer agrees to the following: (i) a press release announcing the partnership within the first four (4) weeks of contract execution, (ii) one (1) named customer case study within twelve (12) months of the Order Effective Date (inclusive of video testimonial), (iii) inclusion in 3rd party analyst reports (i.e., Forrester   Total Economic Impact Report), and (iv) commitment to be a customer presentation at a first party event (i.e., Sprinklr ASKO) and/or third party event (i.e., CX Network webinar), as and when requested by Sprinklr.

11.5 Sprinklr has the worldwide, perpetual, irrevocable right and license to use non-personal aggregated and anonymized statistical data or, as applicable, information that is de-identified in accordance with HIPAA, in each case as derived from the operation and use of the Sprinklr Services ("Statistical Data") for internal business and/or operating purposes only, provided that Sprinklr does not share with any third party Statistical Data which reveals the identity of Customer, Customer Users, or Customer's Confidential Information except as permitted pursuant to Section 8 in accordance with applicable law.

11.6 Nothing in this Agreement will create any association, partnership, or joint venture between the parties. No party has been induced to enter into this Agreement by, nor is any party relying on, any representation or warranty outside those expressly stated in this Agreement. If a court of competent jurisdiction finds any provision of this Agreement unenforceable, all other provisions will remain in full force and effect and the unenforceable provision will be replaced with an enforceable provision that most nearly achieves the intent and economic effect of the unenforceable provision.

11.7 In the event of a conflict between any provision of this Agreement and an SOW or Order Form, the terms of the SOW or Order Form shall prevail with respect to the matters covered by the applicable SOW and/or Order Form. In the event of a conflict arising between the terms of this Agreement and, to the extent applicable, the DPA and the Business Associate Agreement, the terms of the DPA and/or the Business Associate Agreement, as applicable, shall prevail with respect to the matters covered by the applicable DPA and/or the Business Associate Agreement.

Addendum 1

Sprinklr Enterprise Security Addendum

This Enterprise Security Addendum ("ESA") applies to all data processed on behalf of our customers in the Sprinklr Platform and in the provision of the Sprinklr Services, including any Sprinklr owned or leased servers that host Customer's data.

The following technical and organizational measures are implemented by Sprinklr, in accordance with industry standards, to ensure an appropriate level of security related to use of the Sprinklr Platform. For access to documentation evidencing each of the measures listed below, including relevant certifications, please visit Sprinklr's Trust Center.

Information Security Program

Sprinklr has a dedicated security team chartered to define, supervise implementation of, and monitor all relevant security and privacy policies, standards, and controls (the "Security Team"). The Security Team is supported by Sprinklr's Board of Directors and the Executive Leadership Team and is independent from Sprinklr's Research & Development team, the IT team, and other operational teams. By independently validating the implementation of application security controls and reporting the outcome to Sprinklr leadership, the Security Team ensures proper accountability and a risk-informed decision process for maintaining and evolving the security program. In addition, Sprinklr's internal Governance, Risk, and Compliance function, alongside third-party auditors, provides oversight on Sprinklr's overall security posture and internal controls for risk management.

Security Manual

The Security Manual, available upon request, is maintained by the Security Team and provides an overview of all applicable security and privacy policies, controls, and procedures, as well as processes for the management of actual or reasonably suspected security incidents, including through (a) training personnel with access to the Sprinklr Platform and Customer data to recognize and report potential or actual security incidents; and (b) conducting post-incident reviews of events and actions taken.

Audit and Assurance

The Sprinklr Platform undergoes annual, independent audit and assurance assessments according to risk-based plans and policies. Sprinklr maintains the following: Reports – SOC 1 Type II, SOC 2 Type II, and SOC 3 and Certification – ISO 27001:2013, or an industry equivalent.

Sprinklr shall make available to Customer information necessary to demonstrate compliance with this ESA and shall reasonably allow for and contribute to audits by Customer as further defined in Sprinklr's standard Data Processing Addendum or as otherwise agreed to by Sprinklr and Customer in a separate agreement.

Regular Risk Assessment Of Information Security Program

Sprinklr conducts information security risk assessments annually, or whenever there is a material change in Sprinklr's business or technology practices that materially impact the privacy, confidentiality, security, integrity, or availability of Customer data. These risk assessments include the validation of administrative, procedural, and technical controls and are conducted by independent third parties (e.g., third-party assessors and penetration testers) or the independent internal Security Team. Remediation of any material findings is tracked and validated.

Controls

- **Physical Access and Environmental Controls**

For all production systems, Sprinklr leverages our public cloud provider capabilities for the implementation and maintenance of physical controls to protect servers, networks, and facilities from unauthorized access. Controls include secure building with multiple secure access zones; secure perimeters; 24/7 video surveillance; on-site guard service; suitable environmental protections including climate-controlled data rooms and uninterruptible power sources; and other services as required by applicable regulations or requirements. Sprinklr periodically validates the suitability of these controls through third-party security audit reports and/or vendor audits.

- **Logical Access Controls**

Logical access to Sprinklr servers is limited to only those Sprinklr IT personnel who have the need and approval to directly access the servers. The Sprinklr Platform is set behind perimeter security controls jointly managed by the cloud provider and Sprinklr. No direct communication sessions originating from the Internet pass directly through the internal network. Sprinklr continuously monitors the key parameters for all Sprinklr Services for any unusual access activity.

- **Network Transport Controls**

Sprinklr has implemented industry standard security controls designed to protect all Customer data in transit from attacks against confidentiality or integrity. These controls include the implementation of applicable network protocols, encryption schemes, hashing of data, cryptographic signature, etc. Cryptographic keys and other secrets are managed using industry standard practices.

- **Data Storage Controls**

All media containing Customer data is protected from unauthorized physical access. Where applicable, Customer data at rest is encrypted using current and industry standard encryption mechanisms. Cryptographic keys are managed by Sprinklr in accordance with industry standard practices. Sprinklr's third party cloud hosting providers utilize NIST SP800-88 data destruction techniques. Customer data is deemed irrecoverable once deleted.

- **Authentication Controls**

Sprinklr implements industry standard identity governance processes and authentication mechanisms to ensure that only authorized users can interact with systems. This includes multi-factor authentication, single-sign-on architecture where technically feasible, and timely user provisioning and deprovisioning processes. All user actions, including successful and unsuccessful login attempts, user's first name and last name, IP address, date, and time stamp are logged.

- **Data Access Controls (Authorization)**

Access to specific data, systems, or services is limited to users with a need to know, following a strict implementation of least privilege access authorization. Role Based Access Control ("RBAC") is used where feasible and periodic access recertifications are in place.

- **Remote Access Controls**

Remote access to Sprinklr's backend systems is restricted to selective and authorized personnel based on their role. The access follows the principle of least privilege and a multi-tiered security protocol which includes employees with backend access to connect to the bastion host through Sprinklr's VPN which is whitelisted. Once authenticated, SSH is utilized to access the server. Username and password are required as the next step and two (2) Factor Authentication as the final step**.** Device validation is performed during sign on.

- **Communication Controls**

Sprinklr verifies and establishes the parties to which personal data have been or may be transmitted, or otherwise made available. Sub-processors used by Sprinklr are initially - and afterwards periodically - assessed for data security and privacy practices consistent with Sprinklr's own data security and privacy practices. Sprinklr does not sell, furnish, or otherwise share Customer data without the consent of the Customer or the data subject, as applicable.

- **Input Controls**

Sprinklr limits, monitors, and logs where applicable how data is entered into our systems. Standard software development security controls are in place to sanitize potentially harmful external input. This includes industry standard controls designed to prevent the introduction or spread of malicious software ("Malware").

- **Processing Controls**

All processing by Sprinklr is conducted on behalf of and at the instruction of the Customer. Processes and technical controls in place to enforce this control are reviewed on a periodic basis.

- **Availability Controls**

All data critical for the operation of Sprinklr's Platform and Customer data is protected by multiple controls to ensure continuous protection of such data such as runtime mechanisms including redundant storage of operational data and multiple backups (with the exception of Sprinklr Services that, by design, do not persist Customer data), and other industry standard controls as applicable.

Personnel

Sprinklr performs a thorough background check against its employees. The check includes:

- Criminal record check
- Employment claims check
- Education claims check

Employees also undergo security awareness training at least annually.

Application Security and Vulnerability Management

Sprinklr has a rigorous security testing and vulnerability management program in place. Application level and infrastructure level penetration testing is performed using an external party on an annual basis. Identified vulnerabilities are remediated in accordance with Sprinklr's vulnerability management standard using the following timeline:

Rating	Remediation Timeline
Critical	7 Days

High	30 Days
Medium	60 Days
Low	180 Days

Static and dynamic security scans are performed for every major code release and significant issues are remediated prior to implementation of the new software.

Sprinklr adheres to a secure Software Development Lifecycle ("SDLC:) based on industry standard guidelines and practices. Developers undergo secure code training which incorporates OWASP Top 10 guidelines. Source code management and deployment follow segregation of duties and least privilege principles. Sprinklr maintains separate environments for testing, QA, and production. Production data is not stored or used in testing environments.

Data and Systems Recovery

Production systems and services are implemented to achieve a Recovery Time Objective (RTO) of 24 hours with a Recovery Point Objective (RPO) of 24 hours. The associated processes are periodically reviewed and tested where applicable.

Integrity

Sprinklr has implemented protective controls designed to ensure that stored data cannot be corrupted by means of a malfunctioning of the system. Such controls include system redundancy, cryptographic hashing, checksumming, and other industry standard measures as applicable. Once data is entered into our systems, Sprinklr has appropriate development and operational controls to ensure the data quality of our systems.

Purpose Limitation

All data is collected and processed for specific purposes. Personal Data or data derived from Personal Data collected for a specific purpose is not used for other purposes without permission from the Customer or the data subject, as applicable. Production data is not used for testing or development purposes unless explicit permission is given.

Secure Configuration

Sprinklr leverages industry standard security baseline definitions and vendor best-practices to ensure suitable secure configuration of Sprinklr production environments. Unused services are turned off and blocked. Configurations are reviewed and updated periodically by operational staff and the Security Team. These include suitable configurations for event logging and monitoring, which are alerted to the Network Operation Center ("NOC"), the Security Team, and other operational staff.