



## Data Processing Addendum

This Data Processing Addendum (“DPA”) is made and entered into by and between Sprinklr, Inc. (“Sprinklr”) and the customer specified in the table below (“Customer”). This DPA forms part of the Master Services Agreement between Customer and Sprinklr, Inc. (“MSA”). It reflects the parties’ agreement with regard to the Processing of Customer Data, including Personal Data, in accordance with the requirements of Data Protection Laws and Regulations. It includes the „EU Standard Contractual Clauses for the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection“ („EU Standard Contractual Clauses“). This DPA shall not replace any additional rights relating to Processing of Customer Data previously negotiated by Customer in the MSA (including any existing data processing addendum to the MSA).

Data Processor/Data Importer:	Data Owner/Data Exporter:
<p>Sprinklr, Inc. 29 W. 35th Street, 8th Floor New York, NY 10001, USA</p> <p>Name: Greg Czaja</p> <p>Title: Senior Counsel</p> <p>Date: February 16, 2016</p> <p>Signature:  <i>Greg Czaja</i></p>	<p>Name:</p> <p>Title:</p> <p>Date:</p> <p>Signature:</p>

This DPA is pre-signed on behalf of Sprinklr. To enter into this DPA, please complete the Customer information above, sign above and submit the completed and signed DPA to [privacy@sprinklr.com](mailto:privacy@sprinklr.com).

Upon receipt of the validly completed DPA at this email address, this DPA will become legally binding. If Customer makes any deletions or other revisions to this Addendum, then this Addendum will be null and void. Customer signatory represents to Sprinklr that he or she has the legal authority to bind Customer. This DPA will terminate automatically upon termination of the MSA, or as earlier terminated pursuant to the terms of this DPA.



## EU Standard Contractual Clauses

Customer (“Data Exporter” and/or “Non-Sprinklr Entity”) and Sprinklr (the “Data Importer”), each a “party”; together “the parties”, have agreed on the following EU Standard Contractual Clauses in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the Data Exporter to the Data Importer of the personal data specified in Appendix 1.

### Clause 1: Definitions

For the purposes of the Clauses:

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

(b) ‘the **Data Exporter**’ means the controller who transfers the personal data;

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

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

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

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

### Clause 2: Details of the transfer

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

### Clause 3: Third-party beneficiary clause

1. The Data Subject can enforce against the Data Exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

2. The Data Subject can enforce against the Data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the Data Exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the Data Exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the Data Exporter, in which case the Data Subject can enforce them against such entity.

3. The Data Subject can enforce against the Subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the Data Exporter and the Data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the Data Exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the Data Subject can enforce them against such entity. Such third-party liability of the Subprocessor shall be limited to its own processing operations under the Clauses.

4. The parties do not object to a Data Subject being represented by an association or other body if the Data Subject so expressly wishes and if permitted by national law.

#### Clause 4 Obligations of the Data Exporter

The Data Exporter agrees and warrants:

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

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

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

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

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

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

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

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

(i) that, in the event of sub-processing, the processing activity is carried out in accordance with Clause 11 by a Subprocessor providing at least the same level of protection for the personal data and the rights of Data Subject as the Data Importer under the Clauses; and

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

#### **Clause 5: Obligations of the Data Importer**

The Data Importer agrees and warrants:

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

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

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

(d) that it will promptly notify the Data Exporter about:

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

(ii) any accidental or unauthorized access; and

(iii) any request received directly from the Data Subjects without responding to that request, unless it has been otherwise authorized to do so;

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

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

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

(h) that, in the event of sub-processing, it has previously informed the Data Exporter and obtained its prior written consent;

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

(j) to send promptly a copy of any Subprocessor agreement it concludes under the Clauses to the Data Exporter.

#### Clause 6: Liability

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

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

3. If a Data Subject is not able to bring a claim against the Data Exporter or the Data Importer referred to in paragraphs 1 and 2, arising out of a breach by the Subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the Data Exporter and the Data Importer have factually disappeared or ceased to exist in law or have become insolvent, the Subprocessor agrees that the Data Subject may issue a claim against the data Subprocessor with regard to its own processing operations under the Clauses as if it were the Data Exporter or the Data Importer, unless any successor entity has assumed the entire legal obligations of the Data Exporter or Data Importer by contract or by operation of law, in which case the Data Subject can enforce its rights against such entity. The liability of the Subprocessor shall be limited to its own processing operations under the Clauses.

4. Without prejudice to paragraphs 1, 2 and 3 of Clause 6, each party's aggregate liability to the other under or in connection with these Clauses (whether in contract, tort or otherwise) is limited to the amount paid for the services by the non-Sprinklr entity which is party to the MSA in the 12 months immediately preceding the event (or first in a series of connected events) giving rise to the liability. Any limitations of liability agreed in the MSA shall prevail to this paragraph 4 of Clause 6.

### **Clause 7: Mediation and Jurisdiction**

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

### **Clause 8: Cooperation with supervisory authorities**

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

### **Clause 9: Governing Law**

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

### **Clause 10: Variation of the contract**

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

### **Clause 11: Subprocessing**

1. The Data Importer shall not subcontract any of its processing operations performed on behalf of the Data Exporter under the Clauses without the prior written consent of the Data Exporter. Where the Data Importer subcontracts its obligations under the Clauses, with the consent of the Data Exporter, it shall do so only by way of a written agreement with the Subprocessor which imposes the same obligations on the Subprocessor as are imposed on the Data Importer under the Clauses. Where the Subprocessor fails to fulfill its data protection obligations under such written agreement the Data Importer shall remain fully liable to the Data Exporter for the performance of the Subprocessor's obligations under such agreement.
2. The prior written contract between the Data Importer and the Subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the Data Subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the Data Exporter or the Data Importer because they

have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the Data Exporter or Data Importer by contract or by operation of law. Such third-party liability of the Subprocessor shall be limited to its own processing operations under the Clauses.

3. The provisions relating to data protection aspects for sub-processing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the Data Exporter is established.

4. The Data Exporter shall keep a list of sub-processing agreements concluded under the Clauses and notified by the Data Importer pursuant to Clause 5(j), which shall be updated at least once a year. The list shall be available to the Data Exporter's data protection supervisory authority.

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

1. The parties agree that on the termination of the provision of data processing services, the Data Importer and the Subprocessor shall, at the choice of the Data Exporter, return all the personal data transferred and the copies thereof to the Data Exporter or shall destroy all the personal data and certify to the Data Exporter that it has done so, unless legislation imposed upon the Data Importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the Data Importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

2. The Data Importer and the Subprocessor warrant that upon request of the Data Exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.



## Appendix 1 to the Standard Contractual Clauses

**This Appendix forms part of the Clauses.**

### **Data Exporter**

The Data Exporter is the non-Sprinklr legal entity that is a party to the Clauses. The Data Exporter is a licensee of Sprinklr's Software as a Service (SaaS).

### **Data Importer**

The Data Importer is Sprinklr, Inc., a global provider of an enterprise social media management system as a Software as a Service (SaaS).

### **Data Subjects**

The personal data transferred concern the Data Exporter's customers, followers, fans and other Internet users who use social networking platforms and websites, including, but not limited to Twitter, Facebook, YouTube, LinkedIn, Google+, SlideShare, Instagram, Vkontakte, Sina Weibo, RenRen, WeChat, QQ, Blogs & blog comments, mainstream news sources and forums, and websites owned by the Data Exporter where the Data Importer provides social and content management functionality on the Data Exporter's behalf. Data Subjects also includes individuals collaborating and communicating with the Data Exporter's customers, followers, fans and other Internet users who use social networking platforms and Data Exporter's employees, Data Exporter's agents and Data Exporter's subcontractors' employees operating Sprinklr's social media management system (hereinafter "Customer Employees").

### **Categories of data**

The personal data transferred concern publicly available user IDs, social network profile names, social network communications, information shared across social networking platforms and websites, including, but not limited to Twitter, Facebook, YouTube, LinkedIn, Google+, SlideShare, Instagram, Vkontakte, Sina Weibo, RenRen, WeChat, QQ, Blogs & blog comments, mainstream news sources and forums. Where the Data Importer is providing functionality on the Data Exporter's behalf on their websites, personal data may include real names, email addresses, location, age, gender and other personal data defined by the Data Exporter. Personal data transferred also includes other electronic data submitted, stored, sent or received by Data Exporter via the Services

Customer Employees' personal data transferred concern identification data (name, login), contact information (business email address) and work related information (usage/performance data, social contact handling data).

### **Processing operations**

The personal data transferred will be subject to the following basic processing activities:

#### *Scope of Processing:*

The Clauses reflect the parties' agreement with respect to the processing and transfer of personal data specified in this Appendix pursuant to the provision of the "Services" as defined under the MSA.



Personal data may be processed for the following purposes: (a) to provide the Services, (which may include the detection, prevention and resolution of security and technical issues); (b) to respond to customer support requests; and (c) otherwise to fulfill the obligations under the MSA.

The Data Exporter instructs the Data Importer to process personal data in countries in which the Data Importer or its Subprocessors maintain facilities as necessary for it to provide the Services.

**Term of Data Processing.**

Data processing will be for the term specified in the MSA. For the term of the MSA, and for a reasonable period of time after the expiry or termination of the MSA, the Data Importer will provide the Data Exporter with access to, and the ability to export, the Data Exporter's personal data processed pursuant to the MSA.

*Data Deletion:*

For the term of the MSA, the Data Importer will provide the Data Exporter with the ability to delete the Data Exporter's personal data from the Services. After termination or expiry of the MSA, the Data Importer will delete the Data Exporter's personal data in accordance with the MSA.

*Access to Data:*

For the term of the MSA, the Data Importer will provide the Data Exporter with the ability to correct, block, export and delete the Data Exporter's personal data from the Services in accordance with the MSA.

*Subprocessors:*

The Data Importer may engage Subprocessors to provide parts of the Services. The Data Importer will ensure Subprocessors only access and use the Data Exporter's personal data to provide the Services and not for any other purpose. The Data Importer will conclude EU Standard Contractual Clauses with any Subprocessors processing Data Exporter's personal data outside of the European Economic Area (EEA).



## Appendix 2 to the Standard Contractual Clauses

### **This Appendix forms part of the Clauses.**

Description of the technical and organizational security measures implemented by the Data Importer in accordance with Clauses 4(c) and 5(c) (or document/legislation attached):

The Data Importer currently abides by the security standards in this Appendix 2. The Data Importer may update or modify these security standards from time to time provided such updates and modifications will not result in a material degradation in the security of the Services during the term of the MSA.

#### **1. Data Storage & Network Security.**

##### **(a) Data Storage.**

Infrastructure. The Data Importer maintains Amazon Web Service (AWS) for its data storage. The Data Importer stores all production data through this secure service. An overview of Amazon Web Services Security Processes is available at [http://d0.awsstatic.com/whitepapers/Security/AWS\\_Security\\_Whitepaper.pdf](http://d0.awsstatic.com/whitepapers/Security/AWS_Security_Whitepaper.pdf).

The physical security and the security of the network outside of Sprinklr servers are managed by AWS. The hardware/software maintenance agreement with AWS are detailed at <http://aws.amazon.com/agreement/>.

The AWS SLA is available at: <http://aws.amazon.com/ec2-sla/>.

##### **(b) Network Security.**

Disaster Recovery Objectives. In case of a major disaster, all processes and personnel should be in place to fully restore the service within 6 hours. That is RTO (Recovery Time Objective) is 6 hours and RPO (Recovery Point Objective) is 24 hours.

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

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

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

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



Businesses Continuity. The Data Importer replicates data over multiple systems to help to protect against accidental destruction or loss. The Data Importer has designed and regularly plans and tests its business continuity planning/disaster recovery programs.

**(c) Networks & Transmission.**

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

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

**2. Access and Site Controls.**

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

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

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

All sensitive data used by the system is stored encrypted, and direct access privilege to data store instances is given to database administrators only. There is no direct end-user access to data store. End-user access is available only via the application.

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

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

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

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

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

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

### **3. Data.**

Data Storage, Isolation, Authentication, Backup and Restoration. A full snapshot of the production environment database is performed on a daily basis. Database backups (DB) are taken using tools provided by Sprinklr cloud vendor (AWS) and database snapshots (DB Snapshots) are taken on on-demand (during critical releases). The automated backup enables point-in-time recovery of your DB Instance. When automated backups are turned on for DB Instance, AWS tools automatically perform a full daily snapshot of the data and captures transaction logs (as updates to DB Instance are made). When a point-in-time recovery is initiated, transaction logs are applied to the most appropriate daily backup in order to restore the DB Instance to the specific time that is required. All backups are retained for user-specified period of time called the retention period, which is set to thirty-five (35) days.

### **4. Personnel Security.**

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

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

### **5. Subprocessor Security.**

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

### **6. Data Privacy Officer.**

The Data Privacy Officer of the Data Importer can be contacted at [privacy@sprinklr.com](mailto:privacy@sprinklr.com).

# Signature Certificate

 Document Reference: 9D3XX6IA2537ZLR8ULLS7W

**RightSignature**  
Easy Online Document Signing



Greg Czaja  
Party ID: C4U7BWJAR2838EWXH3F32B  
IP Address: 98.253.4.226

VERIFIED EMAIL: gczaja@sprinklr.com

Electronic Signature:

Multi-Factor  
Digital Fingerprint Checksum

ada0075a45a97bf807b99e6f102b77a5b30038e7



## Timestamp

2016-02-16 05:37:25 -0800

2016-02-16 05:37:25 -0800

2016-02-16 05:37:15 -0800

2016-02-16 01:50:38 -0800

## Audit

All parties have signed document. Signed copies sent to: Greg Czaja and christian.

Document signed by Greg Czaja (gczaja@sprinklr.com) with drawn signature. - 98.253.4.226

Document viewed by Greg Czaja (gczaja@sprinklr.com). - 98.253.4.226

Document created by christian (christian.schmoll@sprinklr.com). - 188.22.196.176



This signature page provides a record of the online activity executing this contract.