

Participating Addendum To Cloud Services Agreement

This Participating Addendum dated August 30, 2019, by and between AppDynamics LLC ("AppDynamics") and LeanData, Inc. ("LeanData") (the "Addendum"), supplements the Services Agreement (the "Agreement"), dated February 22, 2017, by and between LeanData, Inc. (the "Supplier" or "LeanData") and Cisco Systems, Inc. and its Affiliates ("Cisco").

WHEREAS, Cisco, the parent company of AppDynamics, entered into the Agreement to procure software solutions from Supplier;

WHEREAS, AppDynamics, a wholly-owned subsidiary of Cisco, wishes to also procure software solutions from Supplier in connection with AppDynamics' rights as an Affiliate (as defined in the Agreement) of Cisco as set forth in the Agreement; and

WHEREAS, AppDynamics and Supplier wish to enter into this Addendum to: (i) facilitate AppDynamics' purchases of Software under the Agreement and (ii) include certain additional rights and obligations on the parties.

Therefore, the parties agree as follows:

I. AMENDMENT TERMS AND CONDITIONS.

A. **GENERALLY.** Capitalized terms not otherwise defined herein shall be deemed to have the meanings set forth in the Agreement. The term "[t]his Agreement" shall mean the Agreement as amended by this Addendum.

B. **APPLICABILITY.** Supplier hereby acknowledges that (i) AppDynamics is an Affiliate pursuant to Section 1.1 of the Agreement; (ii) AppDynamics is permitted to access and use the Service pursuant to Section 4.1 of the Agreement; (iii) pursuant to Section 4.1, at all times for which the Agreement is deemed to be a separate agreement between Supplier and AppDynamics, such separate Agreement shall fully incorporate the changes set forth in Section C of this Addendum. For clarity, nothing in this Addendum will amend the Agreement as between Supplier and Cisco, or such parties' rights and obligations thereunder.

C. **AMENDMENT.** The Agreement is hereby amended as follows:

1. The term "Cisco" throughout the Agreement shall be a reference to "AppDynamics."

2. Section 2.1(a) is hereby amended as restated with the following:

Complete the Work described in each SOW or order form using all commercially diligent and good faith efforts by or before the associated Milestone;

3. The first sentence of Section 3.3 (Supplier Services) is hereby amended with the following:

Supplier shall provide the Service described in the applicable SOW or order form to Cisco.

4. Section 4.3 is hereby amended and restated in its entirety with the following:

Restriction of Use. Cisco will not (i) use the Services in a manner that knowingly download content in violation of a third party's rights; (ii) impersonate any person or entity, including without limitation any employee or representative of LD; (iii) transmits a virus, trojan horse, worm, time bomb, or other harmful computer code, file, or program to Supplier's systems; or (iv) to decompile, reverse engineer, disassemble, attempt to derive the source code of, or decrypt the Services and/or Software; or make any modification, adaptation,

improvement, enhancement, translation, or derivative work from the Services and/or Software.

5. Section 9.5 (Existing NDA) is hereby deleted in its entirety.
6. Section 14.1 (Consequential Damages Waiver; Liability Cap) is hereby amended and replaced in its entirety with the following:

Except for liability arising out of Cisco's breach of Section 4.3 (iv) (reverse engineering restriction), in no event shall either party be liable under this agreement for any indirect, incidental, special, punitive or consequential damages, including damages for loss of revenues or profits, loss of use, business interruption, or loss of data, whether in an action in contract or tort, even if the other party has been advised of the possibility of such damages.

Except for liability arising out of Cisco's breach of Section 4.3 (iv) (reverse engineering restriction) or either party's Section 13 (Indemnification) obligations, neither party's liability for any damages (whether for breach of contract, misrepresentations, negligence, strict liability, other torts or otherwise) under this agreement shall exceed an amount equal to the total fees paid (plus fees payable) to Cisco during the 12 months immediately preceding the claim giving rise to such damages. These limitations shall apply notwithstanding any failure of essential purpose of any remedy.

7. Section 16.1 is hereby deleted and replaced with the following:

This Agreement shall commence on the Effective Date and will continue unless terminated pursuant to Section 16 (the "Term").

8. Section 19 (Data Usage and Protection) is hereby deleted and replaced in its entirety with the following:

19. DATA USAGE AND PROTECTION. If Supplier has access to AppDynamics content and data, Supplier and Supplier Personnel shall during the term of this Agreement comply with all applicable laws, regulations, regulatory requirements and codes of practice in connection with its data processing obligations under this Agreement, including as set forth in Exhibit D (Data Protection Schedule).

9. With respect to Section 20.5, AppDynamics address for notice shall be the following:

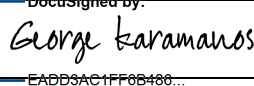
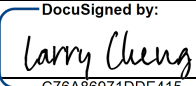
To AppDynamics:
AppDynamics LLC
303 Second Street, North Tower, 8th Fl
San Francisco, CA 94107

10. Attachment A to this Addendum is hereby added as Exhibit D (Data Protection Schedule) to the Agreement.

- II. **CONFLICTS.** In the event of a conflict between the terms of this Amendment and the Agreement, the terms of this Amendment shall govern. Except as expressly modified herein, the terms of the Agreement shall remain in full force and effect.
- III. **AUTHORITY.** The person signing this Amendment for each party represents that s/he is duly authorized by all necessary and appropriate corporate action to enter into this Amendment on behalf of such party.

- IV. LAW AND JURISDICTION. The parties agree that this Amendment and any dispute arising hereunder shall be governed by the laws of the State of California to settle any dispute or claim (whether contractual or non-contractual) that arises out of or in connection with this Amendment or its subject matter or formation.

IN WITNESS WHEREOF, the parties hereto have executed this Amendment as of the Amendment Effective Date.

AppDynamics LLC:	LeanData, Inc.:
Signature: <small>DocuSigned by:</small> 	Signature: <small>DocuSigned by:</small> 
Name: <small>EADD3AC1FF6B488...</small> George Karamanos	Name: <small>C76A86971DDE415...</small> Larry Cheng
Title: General Counsel	Title: VP Finance
Date: September 5, 2019	Date: September 5, 2019

Attachment A

Schedule D

Data Protection Schedule

1. Data Protection

1.1. **Definitions:** In this Schedule, the following terms shall have the following meanings:

"**controller**", "**processor**", "**data subject**", "**personal data**" and "**processing**" (and "**process**") shall have the meanings given in the Data Protection Law; and

"**Data Protection Law**" shall mean: (i) prior to 25 May 2018, Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data; (ii) on and after 25 May 2018, Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation); (ii) any guidance issued by the Article 29 Working Party or a supervisory authority.

1.2. **Relationship of the parties:** AppDynamics (the controller) appoints the Supplier as a processor to process the personal data described in Annex A (the "**Data**"). The Supplier shall, and shall ensure that its agents or subcontractors shall, comply with the obligations that apply to Supplier under Data Protection Law.

1.3. **Purpose limitation:** The Supplier shall process the Data solely to the extent necessary to perform its obligations under this Agreement and strictly in accordance with any documented instructions of AppDynamics (the "**Permitted Purpose**"), except where otherwise required by any European Union (or any EU Member State) law. The Supplier shall promptly inform AppDynamics if, in the Supplier's opinion, any instruction given by AppDynamics to the Supplier contravenes Data Protection Law.

1.4. **International transfers:** The Supplier shall not transfer the Data (nor permit the Data to be transferred) outside of the European Economic Area ("**EEA**") unless (i) it has first obtained AppDynamics' prior written consent; and (ii) it takes measures to ensure the transfer is in compliance with Data Protection Law.

1.5. **Confidentiality of processing:** The Supplier shall ensure that it shall only disclose the Data to, or allow access to the Data by, the employees of the Supplier or those of its agents or sub-contractors (as applicable) (an "**Authorised Person**") who are subject to a strict duty of confidentiality (whether a contractual duty or a statutory duty). The Supplier shall ensure that all Authorised Persons process the Data only as necessary for the Permitted Purpose.

1.6. **Reliability of Authorised Persons:** The Supplier shall take reasonable steps to ensure the reliability of all Authorised Persons (including, without limitation, appropriate training in data protection and security, integrity and confidentiality of personal data).

1.7. **Security:** The Supplier represents that it has, and shall continue to maintain (taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons), appropriate technical and organisational measures to protect the Data (i) from accidental or unlawful destruction, and (ii) loss, alteration, unauthorised disclosure of, or access to the Data (a "**Security Incident**").

- 1.8. Security incidents: Upon becoming aware of an actual or suspected Security Incident, the Supplier shall inform AppDynamics without undue delay, and in any event, within one business day, and shall provide all such timely information and cooperation as AppDynamics may require in order for AppDynamics to fulfil its data breach reporting obligations under (and in accordance with the timescales required by) Data Protection Law. The Supplier shall further take such measures and actions necessary to remedy or mitigate the effects of the Security Incident and shall keep AppDynamics informed of all developments in connection with the Security Incident. The Supplier shall provide AppDynamics with a detailed report on any Security Incident as soon as practicable following the Security Incident including details of (i) the cause and nature of the Security Incident; (ii) whether any Data was corrupted, destroyed, lost or accessed without authorisation, and, if so, which Data; (iii) the steps taken by the Supplier to mitigate the effects of the Security Incident; and (iv) measures put in place to prevent the reoccurrence of the Security Incident.
- 1.9. Loss or corruption of data: If any Data in the possession and/or control of the Supplier is lost, corrupted or rendered unusable for any reason, the Supplier shall promptly notify AppDynamics and restore such Data including by using its back up and/or disaster recovery procedures, at no cost to AppDynamics.
- 1.10. Rectification of Data: The Supplier, its agents and subcontractors, shall promptly carry out any request from AppDynamics requiring the Supplier to amend, transfer, copy or delete any Data or any subsets of Data in a format and on media reasonably specified by AppDynamics.
- 1.11. Return or Deletion of Data: On the expiry or termination of this Agreement, the Supplier shall immediately cease to use, and shall procure that its agents and subcontractors cease to use, the Data and shall arrange for its safe return or destruction as shall be required by AppDynamics at the relevant time (unless European Union, Member State and/or UK law requires storage of the personal data).
- 1.12. Subcontracting: The Supplier shall not subcontract any processing of the Data to a third party subcontractor without the prior written consent of AppDynamics. Notwithstanding this, AppDynamics consents to Supplier engaging third party subcontractors to process the Data provided that (i) the Supplier provides at least 30 days' prior notice of the addition or removal of any subcontractor (including details of the processing it performs or will perform) to legal@appdynamics.com; (ii) the Supplier enters into a written agreement with the subcontractor that imposes data protection terms that protect the Data to at least the same standard provided for by this Schedule; and (iii) the Supplier remains fully liable and responsible for any subcontractor's processing of the Data. If AppDynamics refuses to consent to the Supplier's appointment of a subcontractor on reasonable grounds, then either the Supplier will not appoint the subcontractor or AppDynamics may terminate this Agreement, without penalty and the Supplier will promptly provide a pro-rata refund of any fees paid in advance for unused or unprovided goods or services.
- 1.13. Data subjects' rights: The Supplier shall notify AppDynamics of any requests received from a data subject exercising their rights under Data Protection Law. The Supplier shall provide reasonable assistance to AppDynamics to enable AppDynamics to respond to any request from a data subject to exercise any of its rights under Data Protection Law (including its rights of access, correction, objection, erasure and data portability, as applicable).
- 1.14. Consultation and impact assessments: The Supplier shall, if requested by AppDynamics, provide AppDynamics with reasonable assistance to enable AppDynamics to conduct a data protection impact assessment or supervisory authority consultation taking into account the nature of processing and information available to the Supplier.
- 1.15. Notices from Data Protection Authorities: The Supplier, its agents and sub-contractors, shall promptly notify AppDynamics promptly upon receipt of a notice from any regulatory or government body,

including any supervisory authority, which relates directly or indirectly to the processing of the Data and shall cooperate on request with any relevant EU or Member State supervisory authority.

- 1.16. Records of Processing: The Supplier shall maintain a written record of all categories of processing activities carried out on behalf of AppDynamics, containing all information required under Data Protection Law, and make this record available on request to AppDynamics or any relevant EU or Member State supervisory authority.
- 1.17. Security Information: The Supplier shall provide to AppDynamics any information or assurance necessary to demonstrate compliance with its obligations under this Schedule, or as may be reasonably required by AppDynamics to comply with its obligations under Data Protection Law (including the security of any data processed by the Supplier or its agents or subcontractors).
- 1.18. Audit: The Supplier shall, and shall procure that its agents and subcontractors shall, make available to AppDynamics, all information necessary and allow for and contribute to audits of such data processing facilities, procedures, records and documentation which relate to the processing of the Data, including without limitation, inspections (on reasonable written notice) by AppDynamics, its auditors or agents or any regulatory or government body, including any supervisory authority, in order to ascertain compliance with the terms of this Agreement or Data Protection Law.

Annex A

Data

Subject Matter of Processing

The analysis of Controller's Data within its Salesforce instance.

Duration of Processing

During the term of the Agreement.

Nature and Purpose of Processing

Processor shall process data only in connection with the provision of services pursuant to the terms of the Agreement and this Data Processing Addendum.

Type of Personal Data and Categories of Personal Data

Elements of the Personal Data available for input into Controller's Salesforce instance, including name, contact information (e.g., phone, email address, address), user name and password.

Data Subjects

Data about Controller's employees, contacts, and customers.

Personal details

Included in this category are classes of data which identify the data subject and their personal characteristics. Examples are names, addresses, job title, employer, contact details, age, sex, date of birth, physical descriptions, identifiers issued by public bodies, e.g. NI number.

Family, lifestyle and social circumstances

Included in this category are any matters relating to the family of the data subject and the data subject's lifestyle and social circumstances. Examples are details about current marriage and partnerships and marital history, details of family and other household members, habits, housing, travel details, leisure activities, membership of charitable or voluntary organisations.

Education and training details

Included in this category are any matters which relate to the education and any professional training of the data subject. Examples are academic records, qualifications, skills, training records, professional expertise, student and pupil records.

Employment details

Included in this category are any matters relating to the employment of the data subject. Examples are employment and career history, recruitment and termination details, attendance record, health and safety records, performance appraisals, training records, security records.

Financial details

Included in this category are any matters relating to the financial affairs of the data subject. Examples are income, salary, assets and investments, payments, creditworthiness, loans, benefits, grants, insurance details, pension information.

Goods or services provided

Included in this category are classes of data relating to goods and services which have been provided. Examples are details of the goods or services supplied, licences issued, agreements and contracts.

IT information

Included in this category is any information relating to an individual's use of technology or software including IP addresses, any information about the computing or mobile device a person is using, location data gathered from such devices, usernames and passwords, social media handles.