HIGHSPOT

Highest rated. **Most adopted.**

MAIN SUBSCRIPTION AGREEMENT

Customer:	AppDynamics LLC and its Affiliates
Address:	303 Second Street, North Tower, Eighth Floor, San Francisco, CA 94017
Effective Date:	June 28, 2021

This Main Subscription Agreement (the "*Agreement*") is made on the Effective Date by and between Highspot, Inc., a Delaware corporation headquartered at 2211 Elliott Avenue, Suite 400, Seattle, WA 98121 ("*Highspot*") and AppDynamics LLC and its Affiliates ("*Customer*"). "*Affiliate*" means any entity that directly or indirectly controls, is controlled by, or is under common control with the subject entity. Control means direct or indirect ownership or control of more than 50% of the voting interests of the subject entity. The "*Services*" means the products that are ordered by Customer under an Order Form and made available by Highspot. "*User*" means an individual who is authorized by Customer to use a Service, for whom Customer has purchased a subscription (or for whom a Service has been provisioned), and to whom Customer has supplied user identification and authentication.

1. COMMERCIALS

1.1. **Fees, Invoicing, and Payment**. The "*Fees*" means the fees, expenses, and other amounts specified in this Agreement and applicable Order Form. "*Order Form*" means the ordering document specifying Services to be provided hereunder that is entered into between Customer and Highspot. By entering into an Order Form, an Affiliate agrees to be bound by this Agreement as if it were an original party hereto.   All amounts payable are: (i) denominated and payable in United States Dollars, (ii) payment obligations are non-cancelable and fees paid are non-refundable, and (iii) quantities purchased cannot be decreased during the relevant subscription term. The Fees listed in the Order Form will be fixed for the term listed in the Order. Except as otherwise set forth in the applicable Order Form (a) Customer shall pay invoices within sixty (60) days after receipt of electronic invoice; and (b) payment shall be made by ACH or wire transfer to the bank account designated by Highspot or by check to the address in the Order Form.

1.2. **Subscriptions and True up.** Unless otherwise provided in the applicable Order Form, (a) Services are purchased as subscriptions for the term stated in the applicable Order Form, (b) subscriptions for a Service may be added during a subscription term at the same pricing as the underlying subscription pricing for that Service, prorated for the portion of that subscription term remaining at the time the subscriptions are added, and (c) any added subscriptions will terminate on the same date as the underlying subscriptions. Customer agrees that its purchases are not contingent on any future functionality or features, or dependent on any oral or written public comments made by Highspot regarding future functionality or features. If Customer's user count exceeds the current number of subscriptions (determined on a monthly basis), then Highspot will notify Customer (email sufficing) of such overage. If Customer does not reduce the number of actual users to the number of authorized Users within 30 days, Highspot will notify Customer (email acceptable) and invoice Customer for the excess users at the Price Per User Per Month for the applicable product set forth in the applicable Order Form (who will then become additional authorized Users), prorated for the remainder of the then-current subscription term.

1.3. **Term**. This Agreement commences on the Effective Date and continues until all subscriptions hereunder have expired or have been terminated. Each subscription term is specified in the applicable Order Form.

1.4. **Termination**. A party may terminate this Agreement for cause (i) upon 30 days written notice to the other party of a material breach if such breach remains uncured at the expiration of such period, or (ii) if the other party becomes the subject of a petition in bankruptcy or any other proceeding relating to insolvency, receivership, liquidation or assignment for the benefit of creditors. If this Agreement is terminated by Customer in accordance

with this section, Highspot will refund Customer any prepaid fees covering the remainder of the term of all Order Forms after the effective date of termination. Upon expiration or termination of the subscription term or applicable Order Form, access to the Services will terminate and Customer will immediately cease accessing and using the Services.

1.5. **Taxes**. Fees do not include any taxes, levies, duties or similar governmental assessments, including, for example, value-added, sales, use or withholding taxes, assessable by any jurisdiction ("***Taxes***"). Customer is responsible for paying all Taxes associated with its purchases hereunder. If Highspot has the legal obligation to pay or collect Taxes for which Customer is responsible under this section, Highspot will invoice Customer and Customer will pay that amount unless Customer provides Highspot with a valid tax exemption certificate authorized by the appropriate taxing authority. For clarity, Highspot is solely responsible for taxes assessable against it based on its income, property, and employees.

2. **PARTY RESPONSIBILITIES, INTELLECTUAL PROPERTY, AND CONFIDENTIALITY**

2.1. **Highspot Provision of Services.** Subject to the terms of this Agreement, Highspot (a) grants to Customer and its Affiliates a non-exclusive, non-transferable, non-sublicensable worldwide right and license to use the Service subject to the terms of relevant Order Form, the Documentation, and this Agreement, and (b) provide the Services in accordance with laws and government regulations applicable to Highspot's provision of its Services to its customers generally (i.e., without regard for Customer's particular use of the Services). Highspot will be responsible for the performance of its personnel (including its employees, subcontractors, and contractors) and their compliance with Highspot's obligations under this Agreement.

2.2. **Highspot Protection of Customer Data.** Highspot will maintain SOC 2 certification and appropriate administrative, physical, and technical safeguards for protection of the security, confidentiality and integrity of Customer Data. "***Customer Data***" means electronic data and information submitted by or for Customer to the Services. Those safeguards will include, but will not be limited to, measures designed to prevent unauthorized access to or disclosure of Customer Data (other than by Customer or Users) and to detect and prevent intrusions to the Service. Highspot will require obligations consistent with the foregoing of Highspot's contractors with access to Customer Data and ensure such contractors are subject to appropriate information security diligence reviews. The terms of the data processing agreement ("***DPA***") attached as Exhibit A will apply to the extent Customer Data includes Personal Data, as defined in the DPA. With respect to any processing of personal data by Highspot under this Agreement, Highspot agrees to comply with the requirements set forth in Exhibit A (Data Processing Agreement). To the extent Personal Data from the European Economic Area (EEA), the United Kingdom and Switzerland are processed by Highspot, the Standard Contractual Clauses will apply, as further set forth in the DPA. For the purposes of the Standard Contractual Clauses, Customer and its applicable Affiliates are each the data exporter, and Customer's acceptance of this Agreement, and any applicable execution of an Order Form by Company or an Affiliate, will be treated as its execution of the Standard Contractual Clauses and related Appendices.

Subject to applicable laws and the DPA, Highspot will notify Customer without undue delay, but, where feasible, not later than 72 hours, to security@appdynamics.com of any actual Security Incident (as defined below) involving Customer Data. For clarity, Customer Data is Customer's Confidential Information. The notification provided to Customer shall include, if known, and to Highspot's knowledge as of the time of notice: (i) the general circumstances and extent of any unauthorized access to Customer Data or intrusion into the computer systems or facilities on or in which Customer Data is maintained; (ii) which categories of Customer Data were involved; (iii) the identities of all individuals whose Personal Information was affected (if and as required by applicable laws); and (iv) steps taken to secure the data and preserve information for any necessary investigation. Subject to applicable laws, Highspot shall reasonably cooperate with Customer in investigating and responding to any Security Incident in order for Customer to fulfil its data breach reporting obligations under and in accordance with the timescales required by applicable law. "**Security Incident**" is when Highspot knows that: (i) Highspot has experienced an incident resulting in the unauthorized acquisition or unauthorized use of unencrypted Customer Data, or encrypted Customer Data and the confidential process or key that is capable of compromising the security, confidentiality or integrity of Customer Data that creates a substantial risk of identity theft or fraud; or (ii) Customer Data was acquired or used by an unauthorized person or used for an unauthorized purpose. In the

event of any Security Incident, Highspot will reasonably assist Customer to provide notification to affected individuals and otherwise comply with applicable law with respect to such Security Incident. Notwithstanding anything to the contrary in this paragraph, for the avoidance of doubt, Highspot shall have no obligations hereunder in the event the Security Incident arises from permissions granted by Customer within the Service.

2.3. **Customer Compliance.** Customer will (a) be responsible for its Users' compliance with this Agreement and Order Forms, (b) be responsible for the accuracy, quality, and legality of Customer Data, the means by which Customer acquired Customer Data, Customer's use of Customer Data with the Services, (c) use commercially reasonable efforts to prevent unauthorized access to or use of the Services, and notify Highspot promptly of any such unauthorized access or use, and (d) use the Services only in accordance with this Agreement, Order Forms, and applicable laws and government regulations. If Customer breaches its payment obligations, Highspot may suspend delivery of the Services after providing 30 days' notice (including by phone or email) in the event such breach remains uncured at the end of such period.

2.4. **Reservation of Intellectual Property Rights.** Subject to the limited rights expressly granted hereunder, Highspot and its licensors reserve their right, title, and interest in and to the Services, including all of their related intellectual property rights. No rights are granted to Customer hereunder other than as expressly set forth herein.

2.5. **License by Customer to Highspot.** Customer grants Highspot, its Affiliates and applicable contractors a worldwide, limited-term license to host, copy, use, transmit, and display any Customer Data and program code created by or for Customer using a Service or for use by Customer with the Services, each as appropriate for Highspot to provide and ensure proper operation of the Services and associated systems in accordance with this Agreement. Subject to the limited licenses granted herein, Highspot acquires no right, title, or interest from Customer or its licensors under this Agreement in or to any Customer Data or such program code.

2.6. **IP Infringement**. If Highspot receives information about an infringement or misappropriation claim related to a Service, Highspot may in its discretion and at no cost to Customer (i) modify the Services so that they are no longer claimed to infringe or misappropriate, without breaching Highspot's warranties under "Highspot Warranties" below, (ii) obtain a license for Customer's continued use of that Service in accordance with this Agreement, or (iii) terminate Customer's subscriptions for that Service upon 30 days' written notice and refund Customer any prepaid fees covering the remainder of the term of the terminated subscriptions.

2.7. **Confidential Information.** "Confidential Information" means all information disclosed by a party ("Disclosing Party") to the other party ("Receiving Party"), whether orally or in writing, that is designated as confidential or that reasonably should be understood to be confidential given the nature of the information and the circumstances of disclosure. Confidential Information of Customer includes Customer Data; Confidential Information of Highspot includes the Services, the terms and conditions of this Agreement, and all Order Forms (including pricing). Confidential Information of each party includes technology and technical information, product plans, and designs, and business processes disclosed by such party. However, Confidential Information does not include any information that (i) is or becomes generally known to the public without breach of any obligation owed to the Disclosing Party, (ii) was known to the Receiving Party prior to its disclosure by the Disclosing Party without breach of any obligation owed to the Disclosing Party, (iii) is received from a third party without breach of any obligation owed to the Disclosing Party, or (iv) was independently developed by the Receiving Party.

2.8. **Protection of Confidential Information.** Each party retains all ownership rights in and to its Confidential Information. The Receiving Party will use the same degree of care it uses to protect its own confidential information of like kind to limit access to Confidential Information of the Disclosing Party to those of its and its Affiliates' employees and contractors, and sub contractors who need that access for purposes consistent with this Agreement and who have signed confidentiality agreements with the Receiving Party that are not materially less protective than those herein. Neither party will disclose the terms of this Agreement or any Order Form to any third party other than its Affiliates, legal counsel, and accountants without the other party's prior written consent, provided that such Disclosing Party remains responsible for its Affiliates, legal counsel, and accountants' compliance with this section. The Receiving Party may disclose Confidential Information of the Disclosing Party to the extent compelled by law, provided the Receiving Party gives the Disclosing Party prior notice (to the extent legally permitted) and reasonable assistance, at the Disclosing Party's cost, if the Disclosing Party wishes to contest the disclosure. If the Receiving Party is compelled by law to disclose the Disclosing Party's Confidential

Information as part of a civil proceeding to which the Disclosing Party is a party, and the Disclosing Party is not contesting the disclosure, the Disclosing Party will reimburse the Receiving Party for its reasonable cost of compiling.

3. **REPRESENTATIONS, WARRANTIES, AND DISCLAIMERS**

    3.1. Representations and Warranties. Each Party represents that it has validly entered into this Agreement and has the legal power to do so. This Agreement and the Documentation accurately describes the administrative, physical, and technical safeguards for protecting the security, confidentiality, and integrity of Customer Data, and Highspot warrants, during an applicable subscription term, that: (a) Highspot will not materially decrease the overall security of the Services without prior written notification to Customer; (b) the Services will perform materially in accordance with the applicable Documentation; (c) Highspot will not materially decrease the overall functionality of the Services; (d) Highspot will not discontinue any integrations that would materially decrease the overall functionality of the Services purchased by Customer; and (e) the Service has been tested for viruses. For any breach of a warranty above, Customer's exclusive remedies are set forth in the "Termination" section.

    3.2. Disclaimers. EXCEPT AS EXPRESSLY PROVIDED HEREIN, NEITHER PARTY MAKES ANY WARRANTY OF ANY KIND, WHETHER EXPRESS, IMPLIED, STATUTORY OR OTHERWISE, AND EACH PARTY SPECIFICALLY DISCLAIMS ALL IMPLIED WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, TO THE MAXIMUM EXTENT PERMITTED BY LAW.

4. **MUTUAL INDEMNIFICATION**

    4.1. Indemnification. Each Party (the "Indemnifying Party") will defend the other Party (the "Indemnified Party") and its Affiliates against any claim, suit or proceeding made or brought against the Indemnified Party by a third party alleging that the Services provided by Highspot, or any modification or alteration of the Services by Customer, infringes or misappropriates such third party's intellectual property rights (a "Claim"), and will indemnify the Indemnified Party from any damages, attorney fees, and costs finally awarded against the Indemnified Party as a result of, or for amounts paid by, the Indemnified Party under a settlement approved by the Indemnifying Party in writing of, a Claim, provided that the Indemnified Party: (a) promptly gives the Indemnifying Party written notice of the Claim; (b) gives the Indemnifying Party sole control of the defense and settlement of the Claim (except that the Indemnifying Party may not settle any Claim unless it unconditionally releases the Indemnified Party of all liability); and (c) gives Indemnifying Party all reasonable assistance, at the Indemnifying Party's expense.

    4.2. The defense and indemnification obligations in Section 4.1 do not apply if the Claim arises: (1) from Customer's use or combination of the Services with software, hardware, data, or processes that are not provided by Highspot or authorized by Highspot in writing, if the Services or use thereof would not infringe without such combination; (2) in whole or in part from the Indemnified Party's breach of this Agreement, Documentation, or Order Forms; (3) from Customer's modification or alteration of the Services in a manner not authorized by Highspot in writing, if the Services would not infringe without such modification or alteration; or (4) from the Indemnified Party's own malfeasance.

5. **LIMITATION OF LIABILITY**

    5.1. Limitation of Liability. A PARTY AND ITS AFFILIATES AGGREGATE LIABILITY ARISING OUT OF OR RELATED TO THIS AGREEMENT WILL IN NO EVENT EXCEED THE TOTAL AMOUNT PAID BY CUSTOMER AND ITS AFFILIATES HEREUNDER IN THE TWELVE MONTHS PRECEDING THE FIRST INCIDENT OUT OF WHICH THE LIABILITY AROSE. THE EXISTENCE OF MORE THAN ONE CLAIM SHALL NOT ENLARGE ANY LIABILITY LIMIT. THE FOREGOING LIMITATION WILL APPLY WHETHER AN ACTION IS IN CONTRACT OR TORT AND REGARDLESS OF THE THEORY OF LIABILITY, BUT WILL NOT LIMIT CUSTOMER'S AND ITS AFFILIATES' PAYMENT OBLIGATIONS UNDER THE "FEES, INVOICING, AND PAYMENT" SECTION.

    5.2. Exclusion of Consequential and Related Damages. IN NO EVENT WILL EITHER PARTY OR ITS AFFILIATES HAVE ANY LIABILITY ARISING OUT OF OR RELATED TO THIS AGREEMENT FOR ANY LOST PROFITS, REVENUES, GOODWILL, OR INDIRECT, SPECIAL, INCIDENTAL, CONSEQUENTIAL, COVER, BUSINESS INTERRUPTION OR PUNITIVE DAMAGES, WHETHER AN ACTION IS IN CONTRACT OR TORT AND REGARDLESS OF THE THEORY OF LIABILITY, EVEN IF A PARTY

OR ITS AFFILIATES HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES OR IF A PARTY'S OR ITS AFFILIATES' REMEDY OTHERWISE FAILS OF ITS ESSENTIAL PURPOSE. THE FOREGOING WILL NOT APPLY TO THE EXTENT PROHIBITED BY LAW.

5.3. Excluded Claims. Section 5.1 does not apply to claims arising under Customer's breach of Section 1.1 (Fees, Invoicing, and Payment), or either party's breach of Sections 2.7 and 2.8 (Confidential Information and Protection of Confidential Information, respectively), or Section 4.1 (Indemnification).

6. CORE OPERATIONAL TERMS

6.1. Usage Data. Highspot may store and use metadata associated with Customer's use of the Services, including but not limited to IP addresses, stored sessions, and network metadata (collectively, "Customer Metadata") for the purpose of providing the Services to Customer. In addition, Highspot may track and analyze the usage of the Services for purposes of security and helping Highspot improve both the Services and the user experience in using the Services. For example, to improve product functionality we may use this information to understand and analyze trends or track which features are used most often. Highspot may aggregate Customer Data and Customer Metadata with data and metadata from other Highspot customers or other sources, provided that such data and metadata is not identifiable as Customer Data or Customer Metadata and Customer cannot be recognized as its source. Highspot may share anonymous usage data with Highspot's service providers for the purpose of helping Highspot in such tracking, analysis, and improvements. Additionally, Highspot may share such anonymous usage data on an aggregate basis in the normal course of operating our business.

6.2. Feedback. Customer grants to Highspot and its Affiliates a worldwide, perpetual, irrevocable, royalty- free license to use and incorporate into its services any suggestion, enhancement request, recommendation, correction, or other feedback provided by Customer or Users relating to the operation or use of the Services. Highspot acknowledges that Customer provides all feedback and suggestions "as-is," and that Customer makes no representation or warranty, express or implied, as to the accuracy, non-infringement, or completeness thereof.

6.3. Upload and Transmission Restrictions. Customer agrees that sensitive personal data may not be submitted to the Services, including images, text, sounds or other data containing or revealing government-issued identification numbers; financial information (such as credit or debit card numbers, any related security codes or passwords, and bank account numbers); racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, information concerning health or sex life; information related to an individual's physical or mental health; and information related to the provision or payment of health care. Additionally, Customer may not use the Services to create or analyze biometric identifiers such as face prints, voiceprints, fingerprints, or scans of eyes, hands or facial geometry, nor may Customer use the Services for the purposes of analyzing, profiling or targeting someone's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, age, gender, sex life, sexual orientation, criminal convictions, disability, health status or medical condition. Customer will not use the Services to (a) store or transmit infringing, libelous, or otherwise unlawful or tortious material, or to store or transmit material in violation of third-party rights, (b) store or transmit malicious code (*e.g.*, code, files, scripts, agents, or programs intended to do harm, including, viruses, worms, time bombs, and Trojan horses).

6.4. Customer Usage Restrictions. Customer will not (a) make the Services available to anyone other than Customer, Affiliates or its Users, or use the Services for the benefit of anyone other than Customer or its Affiliates, (b) sell, resell, license, sublicense, distribute, make available, rent or lease the Services, or include the Services in a service bureau or outsourcing offering, (c) interfere with or disrupt the integrity or performance of the Services, (d) attempt to gain unauthorized access to the Services or related systems or networks, (e) use the Services to access or use any of Highspot intellectual property except as permitted under this Agreement, (f) modify, copy, or create derivative works based on the Services or any part, feature, function, or user interface thereof, (g) frame or mirror any part of the Services, other than framing on Customer's own intranets or otherwise for its own internal business purposes or as permitted in the Documentation, (h) except to the extent permitted by applicable law, disassemble, reverse engineer, or decompile the Services or access it to (1) build a competitive product or service, or (2) build a product or service using similar ideas, features, functions or graphics of the Services.

6.5. Return and Deletion of Customer Data. Highspot will make the Customer Data available for up to 60 days after the Agreement ends to enable Customer to extract its Customer Data. Highspot will provide Customer with reasonable assistance to download and export the Customer Data. Such download will be in a mutually agreed upon file format. After such 60-day period, Highspot will have no obligation to maintain or provide any Customer Data. No more than 180 days after expiration or termination of a subscription to Highspot, Highspot disables the account and deletes all Customer Data from the domain. Once the maximum retention period for any data has elapsed, the data is rendered unrecoverable.

6.6. Documentation. Highspot's online help FAQs, user guides, training manuals and similar product documentation of the Services, as updated or revised by Highspot from time to time, found here (the "Documentation").

7. GENERAL PROVISIONS

7.1. Assignment. Neither party may assign any of its rights or obligations in this Agreement without the other party's prior written consent (not to be unreasonably withheld); provided, however, either party may assign this Agreement (including all Order Forms), without the other party's consent to its Affiliate or in connection with a merger, acquisition, corporate reorganization, or sale of all or substantially all assets; provided, however, if a party is acquired by, sells substantially all its assets to, or undergoes a change of control in favor of, a direct competitor of the other party, then such other party may terminate this Agreement upon written notice. In the event of such a termination, Highspot will refund any prepaid Fees covering the remainder of the term of all subscriptions for the period after the effective date of such termination.

7.2. Relationship of the Parties and Third-Party Beneficiaries. The parties are independent contractors. This Agreement does not create a partnership, franchise, joint venture, agency, fiduciary or employment relationship between the parties. Each party will be solely responsible for payment of all compensation owed to its employees, as well as all employment-related taxes. There are no third-party beneficiaries under this Agreement.

7.3. Surviving Provisions. The sections titled "Fees, Invoicing, and Payment," "Reservation of Intellectual Property Rights," "Protection of Confidential Information," "Disclaimers," "Mutual Indemnification," "Limitation of Liability," "Core Platform Operational Terms," and "General Provisions" will survive any termination or expiration of this Agreement, and the section titled "Protection of Customer Data" will survive any termination or expiration for so long as Highspot retains possession of Customer Data.

7.4. Export Compliance and Anti-Corruption. The Services may be subject to export laws and regulations of the United States and other jurisdictions. Highspot and Customer each represent that it is not named on any U.S. government denied-party list. Customer will not permit any User to access or use any Service in a U.S. embargoed country or region or in violation of any U.S. export law or regulation. Neither party has received or been offered any illegal or improper bribe, kickback, payment, gift, or thing of value from an employee or agent of the other party in connection with this Agreement. Reasonable gifts and entertainment provided in the ordinary course do not violate the above restriction.

7.5. Force Majeure. Neither Party will be in breach due to any delay or failure to perform resulting from any cause or condition beyond such Party's reasonable control. If a force majeure event delays or prevents Highspot's performance, the Fees will be equitably adjusted. The Party seeking relief from performance must (i) provide notice of the circumstances as soon as practicable; (ii) use commercially reasonable efforts to avoid or mitigate them; and (iii) resume performance as soon as practicable. If the failure or delay continues for more than 30 days, then the other Party may terminate this Agreement without liability, except that, if Customer terminates this Agreement for Highspot's failure, Highspot shall provide a pro-rated refund for any prepaid Fees for the remaining portion of the subscription term for the Services. This section will not apply to any accrued payment obligations.
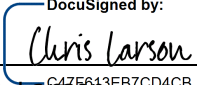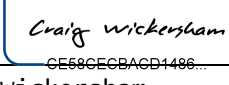
7.6. Notices, Governing Law. This Agreement is governed by the laws of the state of New York, USA, without regard to conflict-of-laws principles. Except as otherwise specified in this Agreement, all notices related to this Agreement will be in writing and will be effective upon (a) personal delivery, (b) the second business day after mailing, to the parties at the address in the applicable Order Form or (c), except for notices of termination, dispute, lawsuit, or an indemnifiable claim ("Legal Notices"), which shall clearly be identifiable as Legal Notices, the day of sending by email: to Highspot at legal@highspot.com or to Customer at the email provided in the Order Form.

7.7. Entire Agreement, Order of Precedence, Waiver, and Severability. This Agreement is the entire agreement between Highspot and Customer regarding Customer's use of Services and supersedes all prior and contemporaneous agreements, proposals, or representations (written or oral) concerning its subject matter. Any term or condition stated in any other Customer order documentation (excluding Order Forms) is void. In the event of any conflict or inconsistency among the following documents, the order of precedence shall be the: (1) applicable Order Form, (2) Agreement, and (3) Documentation. Titles and headings of sections of this Agreement are for convenience only. No failure or delay by either party in exercising any right under this Agreement will constitute a waiver of that right. If any provision of this Agreement is held by a court of competent jurisdiction to be contrary to law, the provision will be deemed null and void, and the remaining provisions of this Agreement will remain in effect.

[SIGNATURES TO FOLLOW ON NEXT PAGE]

Highspot, Inc.		AppDynamics LLC	
By:	*Chris Larson* (DocuSigned by)	By:	*Craig Wickersham* (DocuSigned by)
Name: Chris Larson		Name: Craig Wickersham	
Title: Chief Financial Officer		Title: General Counsel	
Date: July 15, 2021		Date: July 15, 2021	

SERVICE LEVEL ADDENDUM

This Service Level Addendum is part of the Agreement between Highspot and Customer.

1) **Customer Support**. Highspot customer support is available 24 hours a day, 7 days a week. Customer may reach Highspot customer support through the Services or by email to support@highspot.com. Customer must designate a maximum of two support delegates for Standard Support and a maximum of four support delegates for Premier Support. Support delegates are the designated persons for Highspot to contact when Customer's input is required to resolve an issue. For example, if an Authorized User requests access to a spot that he/she doesn't have permission to see or requests access that is controlled via Customer's SSO system. Alternatively, instead of designating individual support delegates, Customer may create an email alias (such as "highspotsupport@[customer].com") for Highspot to send support delegate emails.

2) **Response Time**. For Standard and Premier Support, Highspot will respond to Customer support inquiries in accordance with the following response time schedule:

Level	Description	Target Initial Response Time
Level 1	The Services are inaccessible to all users due to software or hardware failure	2 Hours
Level 2	The Services are accessible but a significant subset of functionality is unavailable to all users due to software or hardware failure	4 Hours
Level 3	Any issues regarding the Services that are not Level 1 or Level 2	24 Hours
Inquiry	Application usage request or service enhancement request	72 Hours

3) **Error Reporting**. Customer will report bugs to their Customer Success Specialist for processing by Highspot.

4) **Maintenance**. Highspot reserves the right to limit Customer's access to the Services in order to perform maintenance or repairs, to make modifications or as a result of circumstances beyond Highspot's reasonable control.

5) **Services Availability**. Highspot agrees that the Services will be available for access and use not less than 99.5% of the time in a given month, provided that (a) that downtime due to regularly scheduled maintenance and exclusion events (as defined below) will not count as time during which the Services is not available, and (b) Highspot shall not be responsible for unavailability due to Customer's loss of Internet connectivity (the "**Uptime Commitment**"). Unavailability is the time that the Services is not available to the Customer as a function of failures in Highspot's or its hosting provider's hardware or software.

6) **Exclusion Events**. Highspot will not be responsible for any service level deficiency resulting from any of the following ("*exclusion events*"):

   a) A failure or interruption of any component or service for which Highspot is not responsible, including but not limited to, electrical power, networking equipment, computer hardware or software, or Internet and telecommunications service;

   b) Any Force Majeure event;

   c) Viruses, other malicious code or denial of service attacks, unless Highspot fails to implement commercially reasonable threat management solutions or the service level deficiency resulted from Highspot's failure to property update such threat management solutions;

   d) Acts or omissions of Customer or its employees, agents, third party contractors or Highspots (except for Highspot); or

    e)   Customer inaccessibility, where such inaccessibility either caused the problem or prevents or delays its resolution.

7) **Service Credits.** If Highspot fails to meet the Uptime Commitment during a month, Customer will be entitled to a credit equal to the percentage of the Monthly Fee for that month according to the schedule below ("Service Credit"). "Monthly Fee" means 1/12 of the annual subscription fee for the Licensed Product.

	Uptime Percentage	Service Credit
a)	Uptime Percentage	Service Credit
b)	Equal or greater than 99.0% but less than 99.5%	5% of Monthly Fee
c)	Equal or greater than 98.0% but less than 99.0%	10% of Monthly Fee
d)	Equal or greater than 95.0% but less than 98.0%	15% of Monthly Fee
e)	Less than 95.0%	20% of Monthly Fee

To be eligible for the Service Credit, Customer must notify Highspot within 30 days after the end of the calendar month giving rise to the Service Credit. Upon receipt of notification, Highspot will perform the research necessary to verify whether Customer is entitled to the Service Credit and will apply the appropriate amount to Customer's next invoice.

8) **Right to Terminate.** Customer may terminate this Agreement immediately by notice in writing to Highspot if:
    a)   Highspot fails to meet the Uptime Commitment more than once in any rolling period of 3 consecutive months; or
    b)   Highspot fails to meet the Uptime Commitment more than 3 times in any rolling period of 12 consecutive months.

If the Agreement is terminated under this subsection (8), Highspot will refund to Customer any pre-paid license fees for the unused portion of the Subscription Term.

EXHIBIT A
DATA PROCESSING AGREEMENT

This Data Processing Agreement, including its Schedules and Appendices, **("DPA")** forms part of the Highspot Main Subscription Agreement for the purchase of online services (including associated Highspot offline or mobile components) from Highspot (identified either as "Services" or otherwise in the applicable agreement , and hereinafter defined as "Services ") (the "Agreement") to reflect the parties' agreement with regard to the Processing of Personal Data.

Customer enters into this DPA on behalf of itself and, to the extent required under applicable laws, rules, regulations, and orders of governmental authorities having jurisdiction, in the name and on behalf of its Authorized Affiliates, if and to the extent Highspot processes Personal Data for which such Authorized Affiliates qualify as the Controller. For the purposes of this DPA only, and except where indicated otherwise, the term "Customer" shall include Customer and Authorized Affiliates. All capitalized terms not defined herein shall have the meaning set forth in the Agreement. In the course of providing the Services to Customer pursuant to the Agreement, Highspot may Process Personal Data on behalf of Customer and the Parties agree to comply with the following provisions with respect to any Personal Data, each acting reasonably and in good faith. Any ambiguity in this DPA shall be resolved to permit AppDynamics to comply with all Applicable Laws. In the event and to the extent that the Applicable Laws impose stricter obligations on the Service Provider than under this DPA, which cannot be varied by the mutual written agreement of the parties, the Applicable Laws shall prevail.

DATA PROCESSING TERMS

DEFINITIONS

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

"Authorized Affiliate" mean s any of Customer's Affiliate(s) which (a) is subject to the data protection laws and regulations of the European Union, the European Economic Area and/or their member states, Switzerland and /or the United Kingdom, and (b) is permitted to use the Services pursuant to the Agreement between Customer and Highspot, but has not signed its own Order Form with Highspot and is not a "Customer" as defined under this DPA.

"CCPA" means the California Consumer Privacy Act, Cal. Civ. Code§ 1798.100 *et seq.,* and its implementing regulations.

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

"Customer" means the entity that executed the Agreement together with its Affiliates (for so long as they remain Affiliates) which have signed Order Forms.

"Customer Data" means what is defined in the Agreement as "Customer Data" or "Your Data", provided that such data is electronic data and information submitted by or for Customer to the Services. This DPA does not apply to Content or Non-Highspot Applications as defined in the Agreement.

"Data Subject" means the identified or identifiable person to whom Personal Data relates.

"GDPR" means the Regulation (EU) 2016 /679 of the European Parliament and of the Council of 27 April 2016 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 Protect ion Regulation).

"Personal Data" means any information relating to (i) an identified or identifiable natural person and , (ii) an identified or identifiable legal entity (where such information is protected similarly as personal data or personally identifiable information under applicable laws, rules, regulations, and orders of governmental authorities having jurisdiction), where for each (i) or (ii), such data is Customer Data.

"Processing" means any operation or set of operations which is performed upon Personal Data, whether or not by automatic means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

"Processor" means the entity which Processes Personal Data on behalf of the Controller, including as applicable any "service provider" as that term is defined by the CCPA.

"Security and Architecture Documentation" means the Security and Architecture Documentation applicable to the specific Services purchased by Customer, as updated from time to time as set forth in the Documentation.

"Highspot Group" means Highspot and its Affiliates engaged in the Processing of Personal Data.

"Standard Contractual Clauses" or "SCC" means the agreement executed by and between Customer and Highspot, Inc., and attached hereto as Schedule 5 pursuant to the European Commission's decision (C (2010)593) of 5 February 2010 on Standard Contractual Clauses for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection.

"Sub-processor" means any Processor engaged by Highspot or a member of the Highspot Group.

"Supervisory Authority" means an independent public authority which is established by an EU Member State pursuant to the GDPR.

1. PROCESSING OF PERSONAL DATA

1.1   Roles of the Parties. The parties acknowledge and agree that with regard to the Processing of Personal Data, Customer is the Controller, Highspot is the Processor and that Highspot or members of the Highspot Group will engage Sub-processors pursuant to the requirements set forth in Section 4 "Sub-processors" below.

1.2   Customer's Processing of Personal Data. Customer shall, in its use of the Services, Process Personal Data in compliance with applicable laws, rules, regulations, and orders of governmental authorities having jurisdiction, including any applicable requirement to provide notice to Data Subjects of the use of Highspot as Processor. For the avoidance of doubt, Customer's instructions for the Processing of Personal Data shall comply with applicable laws, rules, regulations, and orders of governmental authorities having jurisdiction. Customer shall have sole responsibility for the accuracy, quality, and legality of Personal Data and the means by which Customer acquired Personal Data. Customer specifically acknowledges that its use of the Services will not violate the rights of any Data Subject that has opted-out from sales or other disclosures of Personal Data, to the extent applicable under the CCPA.

1.3   Highspot's Processing of Personal Data. Highspot shall treat Personal Data as Confidential Information and shall Process Personal Data on behalf of and only in accordance with Customer's documented instructions for the following purposes: (i) Processing in accordance with the Agreement and applicable Order Form(s) and the Documentation; (ii) Processing initiated by Users in their use of the Services; and (iii) Processing to comply with

other documented reasonable instructions provided by Customer (e.g., via email) where such instructions are consistent with the terms of the Agreement.

1.4 **Details of the Processing.** The subject-matter of Processing of Personal Data by Highspot is the performance of the Services pursuant to the Agreement. The duration of the Processing, the nature and purpose of the Processing, the types of Personal Data and categories of Data Subjects Processed under this DPA are further specified in Schedule 2 (Details of the Processing) to this DPA.

2. RIGHTS OF DATA SUBJECTS

Data Subject Request. Highspot shall, to the extent legally permitted, promptly notify Customer if Highspot receives a request from a Data Subject to exercise the Data Subject's right of access, right to rectification, restriction of Processing, erasure (" right to be forgotten"), data portability, object to the Processing, or its right not to be subject to an automated individual decision making , each such request being a "Data Subject Request". Taking into account the nature of the Processing, Highspot shall assist Customer by appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of Customer's obligation to respond to a Data Subject Request under all applicable laws, rules, regulations, and orders of governmental authorities having jurisdiction. In addition , to the extent Customer, in its use of the Services, does not have the ability to address a Data Subject Request, Highspot shall upon Customer's request provide commercially reasonable efforts to assist Customer in responding to such Data Subject Request, to the extent Highspot is legally permitted to do so and the response to such Data Subject Request is required under all applicable laws, rules, regulations, and orders of governmental authorities having jurisdiction. To the extent legally permitted, Customer shall be responsible for any costs arising from Highspot' s provision of such assistance.

3. HIGHSPOT PERSONNEL

3.1 **Confidentiality.** Highspot shall ensure that its personnel engaged in the Processing of Personal Data are informed of the confidential nature of the Personal Data and have a binding written contractual obligation to keep the Personal Data confidential, have received appropriate training on their responsibilities and have executed written confidentiality agreements. Highspot shall ensure that such confidentiality obligations survive the termination of the personnel engagement.

3.2 **Reliability.** Highspot shall take commercially reasonable steps to ensure the reliability of any Highspot personnel engaged in the Processing of Personal Data.

3.3 **Limitation of Access.** Highspot shall ensure that Highspot's access to Personal Data is limited to those personnel performing Services in accordance with the Agreement.

4. SUB-PROCESSORS

4.1 **Appointment of Sub-processors.** Customer acknowledges and agrees that (a) Highspot's Affiliates may be retained as Sub-processors; and (b) Highspot and Highspot's Affiliates respectively may engage third-party Sub-processors in connection with the provision of the Services. Highspot or an Highspot Affiliate has entered into a written agreement with each Sub-processor containing data protection obligations containing terms at least as protective of Customer's Personal Data as this DPA and with applicable data protection laws with respect to the protection of Customer Data to the extent applicable to the nature of the Services provided by such Sub-processor.

4.2 **List of Current Sub-processors and Notification of New Sub-processors.** Highspot shall make available to Customer in the Documentation the current list of Sub-processors for the Services. Customer may find a mechanism to subscribe to notifications of new Sub-processors for each applicable Service, to which Customer shall subscribe, and if Customer subscribes, Highspot shall provide notification of a new Sub-processor(s) before authorizing any new Sub-processor(s) to Process Personal Data in connection with the provision of the applicable Services.

4.3 **Objection Right for New Sub-processors.** Customer may object to Highspot's use of a new Sub-processor by notifying Highspot promptly in writing within fifteen (15) business days after receipt of Highspot's notice in accordance with the mechanism set out in Section 6. In the event Customer objects to a new Sub-processor, as permitted in the preceding sentence, Highspot will use reasonable efforts to make available to Customer a change in the Services or recommend a commercially reasonable change to Customer's configuration or use of the Services to avoid Processing of Personal Data by the objected-to new Sub- processor without unreasonably burdening Customer. If Highspot is unable to make available such change within a reasonable period of time, which shall not exceed thirty (30) days, Customer may terminate the applicable Order Form(s) with respect only to those Services which cannot be provided by Highspot without the use of the objected-to new Sub-processor by providing written notice to Highspot. Highspot will refund Customer any prepaid fees covering the remainder of the term of such Order Form(s) following the effective date of termination with respect to such terminated Serv ices, without imposing a penalty for such termination on Customer.

4.4 **Liability.** Highspot shall be liable for the acts and omissions of its Sub-processors to the same extent Highspot would be liable if performing the services of each Sub-processor directly under the terms of this DPA, except as otherwise set forth in the Agreement.

5. SECURITY

5.1 **Controls for the Protection of Customer Data.** Highspot shall maintain appropriate technical and organizational measures for protection of the security (including protection against unauthorized or unlawful Processing and against accidental or unlawful destruction, loss or alteration or damage, unauthorized disclosure of, or access to, Customer Data), confidentiality and integrity of Customer Data, as set forth in the Security and Architecture Documentation. Highspot regularly monitors compliance with these measures. Highspot will not materially decrease the overall security of the Services during a subscription term.

6. CUSTOMER DATA INCIDENT MANAGEMENT AND NOTIFICATION

Highspot maintains security incident management policies and procedures specified in the Security and Architecture Documentation and shall notify Customer without undue delay after becoming aware of the accidental or unlawful destruct ion, loss, alteration, unauthorized disclosure of, or access to Customer Data, including Personal Data, transmitted, stored or otherwise Processed by Highspot or its Sub-processors of which Highspot becomes aware (a **"Customer Data Incident").** Highspot shall make reasonable efforts to identify the cause of such Customer Data Incident and take those steps as Highspot deems necessary and reasonable in order to remediate the cause of such a Customer Data Incident to the extent the remediation is within Highspot's reasonable control. The obligations herein shall not apply to incidents that are caused by Customer or Customer' s Users.

7. RETURN AND DELETION OF CUSTOMER DATA

Highspot shall return Customer Data to Customer and, to the extent allowed by applicable law, delete Customer Data in accordance with the procedures and timeframes specified in the Security and Architecture Documentation.

8. AUTHORIZED AFFILIATES

8.1 **Contractual Relationship.** The parties acknowledge and agree that, by executing the Agreement, Customer enters into the DPA on behalf of itself and, as applicable , in the name and on behalf of its Authorized Affiliates, thereby establishing a separate DPA between Highspot and each such Authorized Affiliate subject to the provisions of the Agreement and this Section 8 and Section 9. Each Authorized Affiliate agrees to be bound by the obligations under this DPA and, to the extent applicable, the Agreement. For the avoidance of doubt, an Authorized Affiliate is not and does not become a party to the Agreement and is only a party to the DPA. All access to and use of the Services and Content by Authorized Affiliates must comply with the terms and conditions of the Agreement and any violation of the terms and conditions of the Agreement by an Authorized Affiliate shall be deemed a violation by Customer.

8.2 **Communication.** The Customer that is the contracting party to the Agreement shall remain responsible for

coordinating all communication with Highspot under this DPA and be entitled to make and receive any communication in relation to this DPA on behalf of its Authorized Affiliates.

8.3 **Rights of Authorized Affiliates.** Where an Authorized Affiliate becomes a party to the DPA with Highspot, it shall to the extent required under applicable laws, rules, regulations, and orders of governmental authorities having jurisdiction be entitled to exercise the rights and seek remedies under this DPA, subject to the following: except where applicable laws, rules, regulations, and orders of governmental authorities having jurisdiction require the Authorized Affiliate to exercise a right or seek any remedy under this DPA against Highspot directly by itself, the parties agree that (i) solely the Customer that is the contracting party to the Agreement shall exercise any such right or seek any such remedy on behalf of the Authorized Affiliate, and (ii) the Customer that is the contracting party to the Agreement shall exercise any such rights under this DPA not separately for each Authorized Affiliate individually but in a combined manner for itself and all of its Authorized Affiliates together.8.5 **Audit**. Highspot shall make available to Customer, 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 Customer, 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.

9. LIMITATION OF LIABILITY

Each party's and all of its Affiliates' liability, taken together in the aggregate, arising out of or related to this DPA, and all DPAs between Authorized Affiliates and Highspot, whether in contract or tort under any other theory of liability, is subject to the 'Limitation of Liability' section of the Agreement, and any reference in such section to the liability of a party means the aggregate liability of that party and all of its Affiliates under the Agreement and all DPAs together.

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

10. EUROPEAN SPECIFIC PROVISIONS

10.1 **GDPR.** Highspot will Process Personal Data in accordance with the GDPR requirements directly applicable to Highspot's provision of its Services.

10.2 **Data Protection Impact Assessment.** Upon Customer's request, Highspot shall provide Customer with reasonable cooperation and assistance needed to fulfil Customer's obligation under the GDPR to carry out a data protection impact assessment related to Customer's use of the Services , to the extent Customer does not otherwise have access to the relevant information, and to the extent such information is available to Highspot. Highspot shall provide reasonable assistance to Customer in the cooperation or prior consultation with the Supervisory Authority in the performance of its tasks relating to Section 10.2 of this DPA, to the extent required under the GDPR.

10.3 **Transfer mechanisms for data transfers.** Subject to the additional terms in Schedule 1, Highspot makes available the transfer mechanisms listed below which shall apply, in the order of precedence as set out in Section 10.4, to any transfers of Personal Data under this DPA from the European Union, the European Economic Area and/or their member states, Switzerland and the United Kingdom to countries which do not ensure an adequate level of data protection within the meaning of all applicable laws, rules, regulations, and orders of governmental authorities of the foregoing territories , to the extent such transfers are subject to such applicable laws.

List of Schedules
Schedule 1: Transfer Mechanisms for European Data Transfers
Schedule 2: Details of the Processing
Schedule 3: Standard Contractual Clauses

[SIGNATURES TO FOLLOW ON NEXT PAGE]

Highspot, Inc.

By: _Chris Larson_
DocuSigned by:
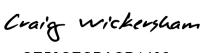C47F613EB7CD4CB...

Name: Chris Larson

Title: Chief Financial Officer

Date: July 15, 2021

AppDynamics LLC

By: _Craig Wickersham_
DocuSigned by:
CE58CECBACD1486...

Name: Craig Wickersham

Title: General Counsel

Date: July 15, 2021

SCHEDULE 1 - TRANSFER MECHANISMS FOR EUROPEAN DATA TRANSFERS

1. ADDITIONAL TERMS FOR SCC SERVICES

1.1   Customers covered by the Standard Contractual Clauses. The Standard Contractual Clauses and the additional terms specified in this Section 2 apply to (i) Customer which is subject to the data protection laws and regulations of the European Union, the European Economic Area and /or their member states, Switzerland and/or the United Kingdom and, (ii) its Authorized Affiliates. For the purpose of the Standard Contractual Clauses and this Section 3, the aforementioned entities shall be deemed "data exporters."

1.2   Instructions. This DPA and the Agreement are Customer' s complete and final documented instructions at the time of signature of the Agreement to Highspot for the Processing of Personal Data. Any additional or alternate instructions must be agreed upon separately. For the purposes of Clause 5(a) of the Standard Contractual Clauses, the following is deemed an instruction by the Customer to process Personal Data: (a) Processing in accordance with the Agreement and applicable Order Form(s); (b) Processing initiated by Users in their use of the SCC Services and (c) Processing to comply with other reasonable documented instructions provided by Customer (e.g., via email) where such instructions are consistent with the terms of the Agreement.

1.3   Appointment of new Sub-processors and List of current Sub-processors. Pursuant to Clause 5(h) of the Standard Contractual Clauses, Customer acknowledges and expressly agrees that (a) Highspot' s Affiliates may be retained as Sub- processors; and (b) Highspot and Highspot's Affiliates respectively may engage third-party Sub-processors in connection with the provision of the SCC Services. Highspot shall make available to Customer the current list of Sub-processors in accordance with Section 4.2 of this DPA.

1.4   Notification of New Sub-processors and Objection Right for new Sub-processors. Pursuant to Clause 5(h) of the Standard Contractual Clauses, Customer acknowledges and expressly agrees that Highspot may engage new Sub-processors as described in Sections 4.2 and 4.3 of the DPA.

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

1.6   Audits and Certifications. The parties agree that the audits described in Clause 5(f) and Clause 12(2) of the Standard Contractual Clauses shall be carried out in accordance with the following specifications: Upon Customer's request , and subject to the confidentiality obligations set forth in the Agreement , Highspot shall make available to Customer that is not a competitor of Highspot (or Customer's independent, third-party auditor that is not a competitor of Highspot) information regarding the Highspot Group's compliance with the obligations set forth in this DPA in the form of the third-party certifications and audits set forth in the Security, Privacy and Architecture Documentation to the extent Highspot makes them generally available to its customers. Customer may contact Highspot in accordance with the "Notices" Section of the Agreement to request an on-site audit of the procedures relevant to the protection of Personal Data. Customer shall reimburse Highspot for any time expended for any such on-site audit at the Highspot Group's then-current professional services rates, which shall be made available to Customer upon request. Before the commencement of any such on-site audit, Customer and Highspot shall mutually agree upon the scope, timing, and duration of the audit in addition   to the reimbursement rate for which Customer shall be responsible. All reimbursement rates shall be reasonable, taking into account the resources expended by Highspot. Customer shall promptly notify Highspot with information

regarding any non-compliance discovered during the course of an audit.

1.7 **Certification of Deletion.** The parties agree that the certification of deletion of Personal Data that is described in Clause 12(1) of the Standard Contractual Clauses shall be provided by Highspot to Customer only upon Customer's request.

1.8 **Conflict.** In the event of any conflict or inconsistency between the body of this DPA and any of its Schedules (not including the Standard Contractual Clauses) and the Standard Contractual Clauses in Schedule 5, the Standard Contractual Clauses shall prevail.

SCHEDULE 2 - DETAILS OF THE PROCESSING

Nature and Purpose of Processing

Highspot will Process Personal Data as necessary to perform the Services pursuant to the Agreement, as further specified in the Documentation, and as further instructed by Customer in its use of the Services.

Duration of Processing

Subject to Section 7 of the DPA, Highspot will Process Personal Data for the duration of the Agreement, unless otherwise agreed upon in writing.

Categories of Data Subjects

Customer may submit Personal Data to the Services, the extent of which is determined and controlled by Customer in its sole discretion, and which may include, but is not limited to Personal Data relating to the following categories of data subjects:

- Prospects, customers, business partners and vendors of Customer (who are natural persons)
- Employees or contact persons of Customer's prospects, customers, business partners and vendors
- Employees, agents, advisors, freelancers of Customer (who are natural persons)
- Customer's Users authorized by Customer to use the Services

Type of Personal Data

Customer may submit Personal Data to the Services, the extent of which is determined and controlled by Customer in its sole discretion, and which may include, but is not limited to the following categories of Personal Data:

- First and last name
- Title
- Position
- Employer
- Contact information (company, email, phone, physical business address)
- ID data
- Professional life data
- Personal life data
- Localization data

SCHEDULE 3 - STANDARD CONTRACTUAL CLAUSES

Standard Contractual Clauses (processors)

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.

Name of the data exporting organization: AppDynamics International Ltd

Address: 5 Market Yard Mews, 194-204 Bermondsey Street, London SE1 3TQ, United Kingdom

Tel.:_____   fax:_____   e-mail:

Other information needed to identify the organisation:

(the data **exporter**)

And

Name of the data importing organisation: Highspot, Inc.

Address: 2211 Elliott Ave, Suite 400, Seattle, WA 98121

Tel.:; +1-206-981-2383e-mail: legal@highspot.com

Other information needed to identify the organisation: Not applicable

(the data **importer**)
each a "party"; together "the parties",

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

Clause 1

Definitions

For the purposes of the Clauses:

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

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

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

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

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

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

Clause 2

Details of the transfer

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

Clause 3

Third-party beneficiary clause

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

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

3.   The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually

disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

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

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

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

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

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

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

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

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

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

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

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

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

Clause 5

Obligations of the data importer

The data importer agrees and warrants:

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

(b)   that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions

received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

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

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

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

(ii)   any accidental or unauthorised access, and

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

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

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

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

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

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

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

Clause 6

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

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

The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.

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

Clause 7

Mediation and jurisdiction

1.   The data importer agrees that if the data subject invokes against its third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

(a)   to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

(b)   to refer the dispute to the courts in the Member State in which the data exporter is established.

2.   The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8

Cooperation with supervisory authorities

1.   The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

2.   The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

3.   The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

Clause 9

Governing Law

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

Clause 10

Variation of the contract

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

Clause 11

Subprocessing

1.   The data importer shall not subcontract any of its processing operations performed on behalf of the data

exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses. Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.

2.   The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

3.   The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.

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

Clause 12

Obligation after the termination of personal data processing services

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

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

APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed by the parties.

The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix.

Data exporter

The data exporter is (please specify briefly your activities relevant to the transfer:

Data Exporter is the legal entity specified in Section 2.1 of Schedule 1 of the DPA.

Data importer

The data importer is (please specify briefly activities relevant to the transfer):

Highspot, Inc. provides a 'software as a service' sales enablement platform which processes personal data upon the instruction of the data exporter in accordance with the terms of the Agreement

Data subjects

The personal data transferred concern the following categories of data subjects (please specify):

Data exporter may submit personal data to the Service which may include, but is not limited to personal data relating to the following categories of data subjects:

- Prospects, customers, business partners and vendors of data exporter (who are natural persons)
- Employees or contact persons of data exporter's prospects, customers, business partners and vendors
- Employees, agents, advisors, freelancers of data exporter (who are natural persons)
- Data exporter's Users authorized by data exporter to use the SCC Services

Categories of data

The personal data transferred concern the following categories of data (please specify):

Data exporter may submit personal data to the Services which may include, but is not limited to the following categories of personal data:

- First and last name
- Title
- Position
- Employer
- Contact information (company, email, phone, physical business address)
- ID data
- Professional life data

- Personal life data
- Connection data
- Localization data

Special categories of data (if appropriate)

The personal data transferred concern the following special categories of data (please specify):

Data exporter may submit special categories of data to the Services, and which is for the sake of clarity personal data with information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life.

Processing operations

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

The objective of processing of personal data by data importer is the performance of the Services pursuant to the Agreement.

APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses:

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

Data importer will maintain administrative, physical, and technical safeguards for protection of the security, confidentiality and integrity of personal data contained in Customer Data, as described in the Highspot Security Documentation. Data Importer will not materially decrease the overall security of the Services during a subscription term.