DATA PROTECTION ADDENDUM

(EJ2 Communications as Vendor)

This Data Protection Addendum (the "Addendum") shall apply if and to the extent EJ2 Communications, Inc. d/b/a Flashpoint (the "Vendor") collects or otherwise processes Customer Personal Data as a data processor in connection with the performance of its obligations under the Agreement. The parties agree that this Addendum shall be incorporated into and form part of the Agreement. Capitalized terms used in this Addendum but not defined herein will be as defined in the Agreement.

1. Definitions and Interpretation

1.1. "**Affiliate**" means any entity that directly or indirectly controls, is controlledby, or is under common control with Customer or Vendor, as applicable.

1.2. "**Agreement**" means all agreements between Vendor and Customer.

1.3. "**Customer**" means the Subscriber (as defined in the applicable Agreement) tothe Flashpoint Services.

1.4. "**Customer Personal Data**" means any Personal Data in respect of which Customer or a Customer Affiliate is a data controller or another entity's data processor that is processed by Vendor as a data processor or subprocessor, respectively, in connection with its performance of the Services.

1.5. "**Personal Data**" means any data concerning individuals located in the European Economic Area (the "**EEA**") falling within the definition of "personal data" under Directive 95/46/EC of the European Parliament and of the Council (the "**Directive**") or any replacement legislation, as applicable, including the General Data Protection Regulation 2016/679 (the "**GDPR**") and the Member State implementations of the GDPR (collectively, "**EU Data Protection Laws**"). Personal Data also means any data of California consumers or households falling within the definition of "personal information" as defined under the California Consumer Privacy Act ("**CCPA**").

1.6. "**Services**" means the services and/or products provided by Flashpoint toCustomer under the Agreement.

1.7. "**Vendor**" means EJ2 Communications, Inc. d/b/a Flashpoint or "Flashpoint".

1.8. Terms defined in the Agreement shall have the same meaning when used in thisAddendum, unless defined in this Addendum. Terms defined in the EU Data Protection Laws including, but not limited to, "controller" and "processor," shall have the same meaning when used in this Addendum, unless differently definedin this Addendum.

2. Nature of the Processing

The data processing activities carried out by the Vendor as a processor under theAgreement are described in Annex A to this Addendum.

3. Processor Obligations

a) Customer and Vendor acknowledge and agree that Customer (or a Customer Affiliate on whose behalf it is authorized to instruct Vendor) is the controller of Customer Personal Data and Vendor is the processor of Customer Personal Data pursuant to the Agreement. In certain instances, Customer (or a Customer Affiliate on whose behalf it is authorized to instruct Vendor) may be the processor of Customer Personal Data, in which case Vendor is appointed as a subprocessor of such Customer Personal Data pursuant to the Agreement. Whether Vendor is serving as a processor or subprocessor, Vendor's obligations shall remain pursuant to this Addendum, which align with Vendor's obligations as a processor pursuant to EU Data Protection Laws.

b) Vendor shall only use, disclose, or otherwise process Customer Personal Data (including transfers to third countries from the EEA), on behalf of and in accordance with Customer's documented instructions, unless otherwise required under applicable law.

c) Customer hereby authorizes Vendor to transfer Customer Personal Data to the United States for provision of the Services and performance under the Agreement, which has been determined by the EC not to provide an adequate level of privacy protection. Accordingly, the Parties hereby agree to enter into and abide by Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council ("Model Clauses") with respect to Customer Personal Data, as applicable, which Model Clauses are available at https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj?uri=CELEX:32021D0914&locale=en.%20%20Module%202%20and%20Module%203 (referencing Module 2: Transfer controller to processor or Module 3: Transfer processor or processor, as appropriate). If the Customer Personal Data includes the Personal Data of individuals in the United Kingdom, then the Parties hereby agree to enter into and abide by the Commission Decision C(2010)593 Standard Contractual Clauses (Processors), as applicable, which Model Clauses are available at https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32010D0087. Customer is the data exporter and Vendor is the data importer. The parties' signatures on the Agreement or this Addendum constitutes their signatures for purposes of the Model Clauses. The applicable governing law for the Model Clauses is the Republic of Ireland; for UK Personal Data, the governing law is the United Kingdom. The Parties agree that if the Model Clauses are updated, replaced or are no longer available for any reason, the parties will cooperate in good faith to implement updated or replacement Model Clauses or identify an alternative mechanism to authorize such transfers.

d) Vendor shall treat Customer Personal Data as confidential information and not disclose such confidential information without Customer's prior written consent. Vendor shall ensure that its personnel authorized to process Customer Personal Data are subject to a duty of confidentiality

by contract or are under an appropriate statutory obligation of confidentiality with respect to Customer Personal Data.

e) Vendor shall implement appropriate technical, physical and organizational measures with respect to the Customer Personal Data, after 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 data subjects, for the purpose of ensuring a level of security appropriate to the risk. Upon Customer's request, Vendor to provide to Customer a written description of its implemented Security Measures with respect to the Customer Personal Data.

f) Upon becoming aware of an accidental or unlawful destruction, loss, alteration, unauthorized disclosure, access, or use of Customer Personal Data (each, a "Security Incident"), Vendor shall notify Customer without undue delay. Vendor shall further assist Customer in fulfilling its personal data breach notification obligations under the GDPR, taking into account the nature of the processing and the information available to the Vendor.

g) Customer hereby consents to Vendor's use of Vendor Affiliates, as applicable, and third-party subprocessors ("Downstream Subprocessors") to process Customer Personal Data pursuant to the Agreement. The list of Vendor's approved Downstream Subprocessors is provided on Annex A. Vendor to provide notice to Customer regarding new or replacement Downstream Subprocessors during the term of the Agreement. If Customer reasonably objects in writing to a new or replacement Downstream Subprocessor within seven (7) calendar days after receipt of such notice, and the parties cannot resolve Customer's reasonable objection within fourteen (14) calendar days after receipt of such objection, then Customer may terminate the Services impacted by the new or replacement Downstream Subprocessor on written notice to Vendor without penalty and receive a pro-rata refund of any fees paid in advance.

h) Notwithstanding the foregoing, Vendor may replace or add a Downstream Subprocessor without prior notice to Customer if, in its sole discretion, such action is necessary to prevent or mitigate risk to the Services, Personal Data, technology infrastructure, or customers. Vendor shall notify Customer of the replacement or additional Downstream Subprocessor as soon as possible, and Customer shall retain the right to object to such Downstream Subprocessor as described in (g) above upon receipt of such notice.

i) Vendor shall enter into written contracts with its Downstream Subprocessors that include data protection obligations that are at least as strict as the standard set forth in this Addendum and shall remain liable for any breach by Downstream Subprocessor under this Addendum as if it were a breach by Vendor.

j) Taking into account the nature of the processing, and to the extent Customer cannot fulfil such obligations directly via the Services, Vendor shall provide commercially reasonable assistance, including through appropriate technical or organizational measures, insofar as this is possible, to Customer to fulfill its obligations to respond to data subject rights requests, specifically the right to access, rectification, erasure, restriction, objection, or portability, as applicable under the Directive or GDPR. If Vendor receives a request directly from a data subject, it will notify Customer of the request (including all relevant details provided by data subject) and await Customer's instructions.

k) Vendor shall notify Customer without undue delay if a supervisory authority or law enforcement authority makes any inquiry or request for disclosure of Customer Personal Data.

l) Vendor shall provide Customer with reasonable assistance should Customer conduct a data protection impact assessment regarding the Services, including providing information reasonably necessary for Customer's prior consultation with a supervisory authority regarding such data protection impact assessment.

m) Vendor shall make available to Customer all information necessary to demonstrate compliance with the obligations laid down in this Addendum and, at Customer's expense, allow for and contribute to audits, including inspections, conducted by the Customer or an independent third-party auditor mandated by the Customer. Vendor shall inform Customer immediately if, in its opinion, a Customer instruction infringes the GDPR or other EU or Member State data protection provision.

n) Upon termination or expiration of the Agreement, Vendor shall, in accordance with the terms of the Agreement, delete or return to Customer all relevant Customer Personal Data (and delete all copies) in Vendor's possession, save to the extent that Vendor is required under any applicable law to retain some or all Customer Personal Data. In such event, Vendor shall extend the protections of the Agreement and this Addendum to such Customer Personal Data and limit processing of such Customer Personal Data to only those purposes required by applicable law, for so long as Vendor maintains the Customer Personal Data.

o) To the extent Customer discloses Personal Information of California consumers or households to Vendor to provide Services to Customer, Vendor may be considered a "service provider" as defined in CCPA Section 1798.140(v), as applicable. Vendor acknowledges and agrees that Customer discloses Personal Information to Vendor solely for: (i) a valid business purpose; and (ii) Vendor to perform the Services as set forth in this Agreement. Vendor is prohibited from: (i) selling Personal Information if the California consumer or household has opted out of the sale of their Personal Information; (ii) retaining, using, or disclosing Personal Information for a commercial purpose other than providing the Services to Customer; (iii) retaining, using, or disclosing the Personal Information outside of the direct business relationship between Vendor and Customer; or (iv) using the Personal Information to provide services to another person or entity. Vendor hereby certifies it understands and will comply with these obligations and restrictions in accordance with the CCPA. Furthermore, Vendor agrees to reasonably assist Customer in responding to any requests from a California consumer or household exercising their rights under the CCPA. For purposes of this Notice, "Personal Information" is defined in CCPA Section 1798.140(o). Further, this Notice is effective for the Term of the Agreement.

4. General Provisions

a) Each party hereby represents and warrants to the other party that it complies, and will continue to comply, with applicable EU Data Protection Laws including, but not limited to, Customer's and Vendor's obligations regarding Customer Personal Data pursuant to the Agreement and this Addendum.

b) Customer hereby grants Vendor the right to anonymize and aggregate Customer Personal Data (the "**Anonymized Data**") and process the Anonymized Data for the purposes of statistics, usage reporting, data analytics, industry analysis, market research, and other similar purposes, and for general business purposes including, but not limited to, the sale and/or license of Anonymized Data to third parties.

c) The headings of any sections, subsections, and paragraphs of this Addendum are inserted for convenient reference only and are not intended to be part of or to affect the meaning or interpretation of this Agreement.

d) Except to the extent amended by this Addendum, the Agreement shall remain in full force and effect. If there is a conflict between this Addendum and the Agreement, this Addendum shall control with respect to its subject matter.

e) Any claims brought in connection with this Addendum shall be subject to the terms and conditions including, but not limited to, the exclusions and limitations set forth in the Agreement.

Data Protection Addendum –
Annex A

Description of Data Processing

The data processing activities carried out by the Vendor under the Agreement may be described as follows:

1. **Subject matter**
   The subject matter concerns the provision by Vendor of data processing services including but not limited to, Platform Access, DDC Access, API Access, Advisory and Professional Services, Flashpoint Collaboration, RFIs.

2. **Duration**
   Vendor will process the data during the effective dates of any Agreements with Customer.

3. **Nature and purpose**
   Vendor processes data solely to provide, secure, operate, manage, maintain, and enhance the services under any Agreements with the Customer.

4. **Data categories**
   Vendor shall process the following categories of personal data: Service usage data provided by the Customer.

5. **Data subjects**
   Processing concerns the following categories of data subjects: Customer Personal Data.

6. **Downstream Subprocessors**
   Vendor uses the following Downstream Subprocessors:

Entity Name	Type of Service	Location
Google Cloud Platform	Google hosts all the systems Flashpoint uses for the SaaS platform	United States
Google Suite	G-suite is used as our internal Identity Provider. Emails will be sent from G-suite accounts.	United States
Salesforce, Inc.	Salesforce is our customer resource management platform used primarily for	United States

	contract management, sales, and related activity	
SendGrid, Inc.	SendGrid sends out reports from the SaaS platform for relevant services	United States
AWS	AWS is used for Backup of Platform Data	United States
Box	Box is used to share files with external customers	United States
ChurnZero	Customer success metrics	United States
Twilio	Being used to send SMS notifications to customers	United States
Okta	Okta will be our user management and SSO / SAML provider	United States
Fullstory	Used for session analytics, and error tracking	United States

Updated September 13, 2021