GDPR DATA PROTECTION ADDENDUM

EJ2 Communications as Vendor

(July 2024)

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.

1. Definitions and Interpretation

(a) "**Affiliate**" means any entity that directly or indirectly controls, is controlled by, or is under common control with Customer or Vendor, as applicable.

(b) "**Agreement**" means all agreements between Vendor and Customer.

(c) "**Customer**" means the company or other entity that purchases the Flashpoint Services as identified in the Agreement.

(d) "**Customer Personal Data**" means any Personal Data in respect of which Customer or a Customer Affiliate is a controller or processor that is processed by Vendor as a processor or subprocessor, respectively, in connection with its performance of the Services.

(e) "**Data Protection Laws"** means all applicable and binding privacy and data protection laws and regulations, including such laws and regulations of the European Union ("EU"), the European Economic Area ("EEA") and their Member States, Switzerland, and the United Kingdom ("UK"), as applicable to the processing of Personal Data under the Agreement including (without limitation) the GDPR, the UK GDPR, the Swiss FADP and EEA/EU Member State laws.

(f) "**Personal Data**" means any information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, to or with an identified or identifiable natural person (a **"Data Subject**").

(g) "**Services**" means the services and/or products provided by Flashpoint to the Customer under the Agreement and as further described in Appendix 1 to this Addendum.

(h) **"Standard Contractual Clauses"** or "**SCCs"** means the standard contractual clauses for the transfer of Personal Data, in accordance with Privacy Laws, to Controllers and Processors established in Third Countries, the approved version of which is in force at the date of signature of the Agreement that are in the European Commission's Decision 2021/914 of 4 June 2021, as such standard contractual clauses are available at https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en, and as may be amended or replaced by the European Commission from time to time.

(i) **"Swiss FADP"** means the Federal Act on Data Protection of June 19, 1992 (DPA) of Switzerland (as updated September 1, 2023) and its implementing ordinances.

(j) **"UK GDPR"** means the GDPR as incorporated into UK law by the Data Protection Act 2018 and amended by the Data Protection, Privacy and Electronic Communications (Amendments, etc.) (EU Exit) Regulations 2019.

(k) **"UK Transfer Addendum"** means the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses issued by the UK Information Commissioner's Office (Version B1.0, in force as of 21 March 2022).

(l) "**Vendor**" means EJ2 Communications, Inc. d/b/a Flashpoint or "Flashpoint".

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

2. Processing of Personal Data

(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 a sub-processor for such Customer Personal Data.

(b) Customer shall ensure that (i) all instructions to Vendor with respect to the processing of Customer Personal Data are at all times in accordance with Data Protection Laws; and (ii) all Customer Personal Data provided to Vendor has been collected in accordance with Data Protection Laws and that Customer has all authorizations and/or consents necessary to provide such Customer Personal Data to Vendor.

(c) The processing activities carried out by the Vendor as a processor (or sub-processor) under the Agreement are described in Appendix 1 to this Addendum.

3. Processor Obligations

(a) Vendor will process Customer Personal Data only for the purpose of providing the Services and in accordance with Customer's documented lawful instructions, as set forth in the Agreement and this Addendum. Processing outside the scope of the Agreement or this Addendum (if any) will require prior agreement between Customer and Vendor and set forth in additional written instructions for processing.

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

(c) 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.

(d) 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. A description of Vendor's minimum implemented security measurers is provided in Appendix 2 hereto. Customer acknowledges that the security measures are subject to technical progress and development and that Vendor may update or modify the security measures from time to time provided that such updates and modifications do not result in the degradation of the overall security of the Services purchased by the Customer.

(e) Upon becoming aware of an accidental or unlawful destruction, loss, alteration, unauthorized disclosure, access, or use of Customer Personal Data (each, a "**Personal Data Breach**"), Vendor shall notify Customer without undue delay; provided, however, Vendor's notice does not constitute an admission of fault by Vendor or its Downstream Sub-processors for the Personal Data Breach. Vendor shall further assist Customer in fulfilling its Personal Data Breach notification obligations under Data Protection Laws, taking into account the nature of the processing and the information then available to the Vendor regarding the Personal Data Breach.

(f) Notwithstanding the foregoing, Customer agrees that, except as may otherwise be set forth in this Addendum, Customer is responsible for its secure use of the Services, including securing its account authentication credentials, protecting the security of Customer Personal Data when in transit to and from the Services and taking any appropriate steps to securely encrypt or backup any Customer Data uploaded to the Services.

(g) Customer hereby provides general written authorization to Vendor's use of Vendor Affiliates, as applicable, and third-party sub-processors ("Downstream Sub-processors") to process Customer Personal Data pursuant to the Agreement and this Addendum. The list of Vendor's approved Downstream Sub-processors is provided on Appendix 3 hereto. Vendor shall provide no less than 30 days prior notice to Customer (including by way of posting a new list for the attention of all customers) regarding proposed new or replacement Downstream Sub-processors during the term of the Agreement. If Customer reasonably objects in writing to a new or replacement Downstream Sub-processor based on concrete data security concerns within 10 calendar days publication date of such notice, and the parties cannot resolve Customer's reasonable objection within 30 calendar days after receipt of such objection, then Customer may terminate the Services directly impacted by the new or replacement Downstream Sub-processor on written notice to Vendor without penalty and receive a pro-rata refund of fees paid in advance with respect to the remainder unused period of the directly impacted Services.

(h) Vendor shall enter into written contracts with its Downstream Sub-processors that include data protection obligations that are at least as strict as set forth in this Addendum applicable to Vendor and shall remain liable for the processing by its Downstream Sub-processors. .

(i) 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 Data Protection Laws. 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.

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

(k) 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.

(l) Vendor shall make available to Customer all information necessary to demonstrate compliance with the obligations set forth 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. Any such audits or inspections shall be limited to once in any rolling 12-month period unless ordered by a supervisory authority or other competent legal authority or upon the occurrence of a Personal Data Breach. If the requested audit scope is addressed in an SSAE 16/ISAE 3402 Type 2, ISO, NIST or similar audit report performed by a qualified third-party auditor ("Audit Report") within twelve (12) months of Customer's audit request and Vendor confirms there are no known material changes in the controls audited, Customer agrees to accept those findings in lieu of requesting an audit of the controls covered by the Audit Report.

(m) To the extent Vendor's processing of Customer Personal Data includes data subjects in the EEA, Switzerland and/or UK, Customer and Vendor acknowledge and agree that such Customer Personal Data may be transferred to third countries, including countries that are not recognized by the European Commission, UK or Switzerland as providing an adequate level of protection for Personal Data. More specifically, Customer acknowledges and agrees that Customer Personal Data may be transferred to Vendor in the United States, which has not received an adequacy determination. Customer hereby consents to the transfer of Customer Personal Data to Vendor in the United States as set forth herein.

(n) As of the Effective Date of the Agreement, Vendor is certified under the EU-US Data Privacy Framework, the Swiss-US Data Privacy Framework and the UK Extension to the EU-US Data Privacy Framework (collectively, "DPF"). The Parties agree that the DPF apply to the contemplated cross-border transfers of Personal Data to Vendor in the United States.

(o) For Customer Personal Data of Data Subjects in the EEA, the Standard Contractual Clauses (Module 2 or Module 3, as applicable) are implemented as follows:

- Clause 7, the "Docking Clause (Optional)", shall be deemed incorporated;
- In Clause 9, the parties choose Option 2, General Written Authorization, with a time period of 30 days;
- The optional wording in Clause 11 shall be deemed not incorporated;
- Clause 17 and Clause 18, the governing law and forum shall be the Republic of Ireland; and
- Appendixes 1, 2 and 3 attached hereto serve as Annexes I, II and III of the Standard Contractual Clauses.

(p) For Customer Personal Data of Data Subjects in Switzerland, the Standard Contractual Clauses (as revised herein) are implemented as follows:

- The Swiss Federal Data Protection and Information Commissioner shall be the sole Supervisory Authority for the transfers exclusively subject to the Swiss FADP;
- The terms "General Data Protection Regulation" or "Regulation (EU) 2016/679" as utilized in the Standard Contractual Clauses shall be interpreted to include the Swiss FADP with respect to the transfers;
- References to Regulation (EU) 2018/1725 are removed;
- References to the "Union", "EU" and "EU Member State" shall not be interpreted in such a way as to exclude data subjects in Switzerland from the possibility of exercising their rights in their place of habitual residence (Switzerland) in accordance with Clause 18(c) of the Standard Contractual Clauses;
- Where the transfers are exclusively subject to the Swiss FADP, all references to the GDPR in the Standard Contractual Clauses are to be understood to be references to the Swiss FADP;
- Where the transfers are subject to both the Swiss FADP and the GDPR, all references to the GDPR in the Standard Contractual Clauses are to be understood to be references to the Swiss FADP insofar as the transfers are subject to the Swiss FADP; and

(q) For Customer Personal Data of Data Subjects in the UK, the UK Transfer Addendum is implemented as follows:

- Tables 1, 2 and 3 are completed with the information provided in subpart (o), above.
- For Table 4, the Parties agree as follows: Either Customer or Vendor can end this UK Transfer Addendum as set out in Section 19 of the UK Transfer Addendum.

B. Table 2: Selected SCCs, Modules and Selected Clauses

The Approved EU SCCs, including the Appendix Information and with only the following modules, clauses or optional provisions of the Approved EU SCCs brought into effect for the purposes of this UK Transfer Addendum:

- Module in operation: Module 2: Transfers Controller to Processor and/or Module 3: Transfers Processor to Processor
- Clause 7 (docking clause): Yes.
- Clause 9: General authorization and 30 days.
- Clause 11 (option): No

C. Table 3: Appendix Information

- Annex IA: The list of parties (Customer and Vendor) is provided in the Agreement.
- Annex IB: Description of Transfer: A description of the transfer is provided in Appendix 1 of this Data Protection Addendum.
- Annex II: Technical and organizational measures including technical and organizational measures to ensure the security of the data: Vendor's implemented security measures are described in Appendix 2 of this Data Protection Addendum.
- Annex III: Vendor's list of sub-processors is provided in Appendix 3 of this Data Protection Addendum.

D. Table 4: Ending this UK Transfer Addendum when the Approved Addendum Changes

Either Customer or Vendor can end this UK Transfer Addendum as set out in Section 19 of the UK Transfer Addendum.

(r) The parties further agree that if the Standard Contractual Clauses or the UK Transfer Addendum are updated, replaced or are no longer available for any reason, the parties will cooperate in good faith to implement updated or replacement Standard Contractual Clauses or UK Transfer Addendum, as appropriate, or identify an alternative mechanism(s) to authorize the contemplated cross-border transfers.

(s) Upon termination or expiration of the Agreement, at Customer's request Vendor will either promptly (i.e., in no more than 30 days) return or destroy the Customer Personal Data in its possession or control. This requirement shall not apply to the extent Vendor is required by applicable to retain some or all of the Customer Personal Data, or to Customer Personal Data it has archived on back-up systems, which Customer Personal Data Vendor shall securely isolate and protect from any further processing, except to the extent required by applicable law. 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 retains the Customer Personal Data.

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) 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.

(c) 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.

(d) 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.

APPENDIX 1

DESCRIPTION OF DATA PROCESSING

A. LIST OF PARTIES

Data exporter(s):

Name: Customer identified in the Agreement

Address: Address listed in the Agreement

Contact person's name, position and contact details: Contact information provided in the Agreement

Activities relevant to the data transferred under these Clauses: (1): Subscription Services for access to and use of Vendor's data processing services including but not limited to, Platform Access, DDC Access, API Access, Advisory Services, Flashpoint Collaboration, RFIs, Monitoring for performance, analytics, security and operation of the Flashpoint Platform; and (2) associated Support and Professional Services (if purchased).

Signature and date: See data importer's signature in the Agreement

Role: Controller/Processor

Data importer(s):

Name: EJ2 Communications, Inc. d//b/a Flashpoint

Address: 6218 Georgia Avenue NW, Suite #1, PMB 3032, Washington, DC, 20011 USA

Contact person's name, position and contact details: legal@flashpoint-intel.com

Activities relevant to the data transferred under these Clauses: (1): Subscription Services for access to and use of Vendor's data processing services including but not limited to, Platform Access, DDC Access, API Access, Advisory Services, Flashpoint Collaboration, RFIs. Monitoring for performance, analytics, security and operation of the Flashpoint Platform; and (2) .associated Support and Professional Services (if purchased)

Signature and date: See Data importer's signature in the Agreement

Role: Processor/Sub-processor

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

- Data exporter's employees, agents, representatives and other persons authorized by data exporter

Categories of personal data transferred

- Name
- Title
- Business address
- Business email
- Business phone number
- Associated service usage data

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions

(including access only for staff having followed specialized training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

- None

The frequency of the transfer (e.g., whether the data is transferred on a one-off or continuous basis).

- Continuous

Nature of the processing

- Data importer processes personal data solely to provide, secure, operate, manage, maintain, and enhance the Services pursuant to the Agreement with the Customer.

Purpose(s) of the data transfer and further processing

- Subscription Services as set forth in the Agreement and relevant Order and/or Statement of Work. .
- Support and Professional Services (if purchased) as set forth in the Agreement and/or relevant Order or Statement of Work:

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

- For the Term set forth in the Agreement.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

- To support data importer's provisioning of the Services to data exporter pursuant to the Agreement and as set forth in this Appendix I.

C. COMPETENT SUPERVISORY AUTHORITY

- The competent supervisory authority is the Data Protection Commission of Ireland

APPENDIX 2

TECHNICAL AND ORGANIZATIONAL MEASURES INCLUDING TECHNICAL AND ORGANIZATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

1. Strong encryption of Personal Data in transit and at rest, as applicable, that meets industry best practices, is robust against cryptanalysis, is not susceptible to interference or unauthorized access, and for which key access is limited to specific authorized individuals with a need to access Personal Data in order to engage in processing or, wherever practicable, such key access is limited solely to the Customer;
2. Wherever practicable with respect to processing, pseudonymization sufficient to cause Personal Data to no longer be attributable to a specific individual, provided safeguards are in place to prevent reidentification and the algorithmic process or key to re-establish identity is held only by the Customer;
3. If agreed by the Parties, or as otherwise practicable, physical locations in which Sensitive Personal Information are processed will be limited to the applicable third countries deemed adequate to receive such Personal Dat under the Data Protection Laws of the applicable third country;
4. Access restrictions and procedures, including unique user identification, to limit processing to authorized Vendor workforce and devices authorized explicitly by Vendor through proper separation of duties, role-based access, on a need-to-know and least privilege basis;
5. Multi-factor authentication and use of a virtual private network for any remote access to Vendor systems or Personal Data;
6. Physical security procedures, including the use of monitoring 24 hours /7 days a week, access controls and logs of access, and measures sufficient to prevent physical intrusions to any Vendor facility where Personal is Data processed;
7. Secure disposal of equipment and physical and electronic media that contain Personal Data;
8. Ongoing vulnerability identification, management and remediation of systems including applications, databases, and operating systems used by Vendor to Process Personal Data;
9. Logging and monitoring to include security events, all critical assets that Process Personal Data, and system components that perform security functions for Vendor's network (e.g., firewalls, IDS/IPS, authentication servers) intended to identify actual or attempted access by unauthorized individuals and anomalous behavior by authenticated users;
10. Monitoring, detecting, and restricting the flows of Personal Data on a multi-layered basis, including but not limited to the use of network segmentation, secure configuration of firewalls, intrusion detection and/or prevention systems, denial of service protections;
11. Remote work procedures that require "clean desk" standards in place and a remote work management program that limits use to only devices authorized pursuant to Vendor's security program;
12. Data protection program elements, such as technical measures or documented procedures, to address data minimization and limited retention, data quality, and implementation of data subject rights, appropriate to the nature of the processing and Services;
13. Appropriate IT governance processes that address risk management, system configuration, and process assurance, including regular and periodic testing and evaluation of the sufficiency of Vendor's data protection program and technical controls;
14. Business continuity and disaster recovery plans intended to ensure integrity, resiliency, and availability of Vendor systems and Personal Data, as well as timely restoration of access to Personal Data; and
15. Vendor shall, at the request of Customer, promptly provide a copy of its most recent Vendor SOC2 Type II report, PCI Attestation of Compliance and/or industry certification such as ISO/IEC 27001 or any successor standards for information security management. If Vendor does not hold such certification(s), it must conduct, at its own expense no less than annually, an independent third-party audit of Vendor's security program and systems, and facilities used to Process Personal Data, with a detailed summary of the report to be provided to data exporter.

APPENDIX 3

AUTHORIZED DOWNSTREAM SUBPROCESSORS

Subprocessors	**Services provided**	**Contact Details**
Google LLC Google Cloud Platform	Google hosts all the systems Flashpoint uses for the SaaS platform	Google LLC 1600 Amphitheatre Parkway Mountain View, CA 94043 USA
SendGrid	SendGrid sends out reports from the SaaS platform for relevant services	sendgrid.com 101 Spear Street, 1st Floor, San Francisco, California, 94105, United States of America
Google LLC Google Workspace	Google Workspace is used as our internal Identity Provider. Emails will be sent from Google Workspace accounts.	Google LLC 1600 Amphitheatre Parkway Mountain View, CA 94043 USA
Atlassian JIRA	Processes services in regards to Request For Information (RFI) workflow and hours.	https://www.atlassian.com/company/contact 350 Bush Street Floor 13 San Francisco, CA 94104 United States
Pendo.io	Pendo.io Processes platform telemetry and anonymized user analytics	https://www.pendo.io/about/ 301 Hillsborough St., Suite 1900, Raleigh, NC 27603
Segment.io Inc	Segment.io provides customer support metrics	https://segment.com/contact/ 101 Spear Street, Ste 500 San Francisco, CA 94105, USA
Amazon Web Services	AWS is hosts the Automate Platform, Hosts all systems for VulnDB, CRA, YourCISO, and The Platform. Also used for log aggregation	https://aws.amazon.com/contact-us/ 410 Terry Avenue North, Seattle, WA 98109-5210, U.S.A.
Salesforce inc	Salesforce is our customer resource management platform used primarily for contract management, sales, and related activity	415 Mission Street San Francisco, CA 94105 https://www.salesforce.com/company/contact-us/
Box	Box is used to share files with external customers	900 Jefferson Ave Redwood City, CA 94063 United States

ChurnZero	Customer success metrics	717 D St NW 2nd floor, Washington, DC 20004 United States
Twilio	Being used to send SMS notifications to customers	101 Spear Street, Ste 500 San Francisco, CA 94105, USA
Okta	Okta is our user management and SSO / SAML provider	100 First Street, 6th Floor San Francisco, CA 94105, USA United States https://www.okta.com/contact/
Fullstory	Used for session analytics, and error tracking	1745 Peachtree St NE Atlanta, GA 30309 United States
Intercom	Used for documentation sharing and customer communications on the website	55 2nd Street, 4th Floor, San Francisco, CA 94105 https://www.intercom.com/about
ReadMe.io	ReadMe is used to share interactive API Documentation	445 Bush St. #800, San Francisco, CA 94108 support@readme.io
Sentry.io	Tracks error logging in the SaaS apps	45 Fremont Street, 8th Floor, San Francisco, CA 94105 compliance@sentry.io.
Google Analytics	Platform analytics and usage	Google LLC 1600 Amphitheatre Parkway Mountain View, CA 94043 USA
Beamer	Announcement center within the application to notify users of changes.	212 W. 29th St., Suite 1106, New York, NY 10001 legal@getbeamer.com
Datadog	Cloud service providing application performance monitoring	New York Times Bldg, 620 8th Ave, New York, NY 10018 privacy@datadoghq.com
Heap	Product usage metrics	225 Bush St. 2nd Floor, San Francisco, CA 94104 privacy@contentsquare.com
LaunchDarkly	Service for feature flag management within application	1999 Harrison St Suite 1100, Oakland, CA 94612 privacy@launchdarkly.com
LogDNA	Cloud service for monitoring application logs	2059 Camden Ave # 297, San Jose, CA 95124, USA privacy@mezmo.com

Mailchimp	The system uses MailChimp's transactional email service Mandril to send email notifications	405 N Angier Ave. NE Atlanta, GA 30308 USA privacy@intuit.com
Microsoft Azure	Cloud services and infrastructure for the application. Secondary identity provider for software development services.	Microsoft Corporation, One Microsoft Way, Redmond, Washington 98052, USA https://go.microsoft.com/fwlink/p/?linkid=2126612
Zendesk	Cloud service that stores customer support tickets	989 Market St San Francisco, CA 94103 euprivacy@zendesk.com