Data Processing Addendum

This Data Processing Addendum (the "**DPA**") applies to the processing of Customer Data by Flare Systems, Inc. ("**Flare**") and the party identified in the Principal Agreement, including customer, partners and resellers ("**Customer**").

This DPA enters into force upon the execution of the Principal Agreement and continues in full force for as long as Customer Data, or Personal Data, is processed by either party pursuant to the Agreement.

In the event of any conflict, inconsistency, or ambiguity between the provisions of this DPA and the remaining of the Principal Agreement, the provisions of this DPA will take precedence and prevail to the extent of such conflict, inconsistency, or ambiguity, solely with respect to the processing of Personal Data and the parties' respective data protection obligations.

1. DEFINITIONS

1.1. The terms not otherwise defined below are defined in the Principal Agreement.

- **Aggregated Data:** Data that no longer identifies a person nor Customer. For instance, aggregated performance metrics over the Flare Platform which no longer identifies Customer.
- **Agreement**: The Principal Agreement, any Order Form(s), the SLA, the Security Addendum, and this DPA, along with any amendments, attachments.
- **Anonymized Data**: Customer Data which no longer allows for the identification of an individual. For the avoidance of doubts, Anonymized Data does not include Personal Data.
- **Customer Data:** Any data, information or materials provided or submitted by Customer to Flare while using the services.
- **Data Protection Laws**: Any laws, treaties, and regulations applicable to the processing of Personal Data by either party pursuant to the Principal Agreement, including, as applicable, the EU's *General Data Protection Regulation* ("**GDPR**"), the UK's *Data Protection Act 2018*, United States Federal Laws and Regulations and any state's law in the United States related to the protection of Personal Data, Canada's *Personal Information Protection and Electronic Documents Act***,** Quebec's *Act Respecting the Protection of Personal Information in the Private Sector*s and any Canadian provincial privacy laws.
- **Intelligence Data:** The Public Data, along with any complementary and related data provided through the Flare Platform, including, search bar results, industry trends, threat intelligence, enriched data, threat scores and recommendations, which are obtained from the Flare Platform.
- **Order Form**: An order form, a quote, a purchase order, change order, statement of work or procurement document executed pursuant to the Principal Agreement and describing the services.
- **Personal Data**: Data that can directly or indirectly identify an individual.
- **Principal Agreement**: Agreement between the parties, including, the Terms of Services, the Partner Terms, any other service agreement and reseller agreement, including any Order Forms.
- **Personal Data Breach**: Shall have the meaning set forth in Article 4 of the *General Data Protection Regulation* ("**GDPR**"), and shall include, for the avoidance of doubts, any access, use, or communication of Personal Data that is not authorized by Data Protection Laws, or any other breach of the protection afforded to Personal Data, including the loss or theft of Personal Data.
- **Public Data**: Any data which is made available through the Flare Platform, including on the dark net and other monitored sources. Public Data can be retrieved through the Retrieval Function and is not Customer Data.
- **Restricted Transfers**: Transfer of Personal Data from the European Union, the United Kingdom or other relevant jurisdiction, to another jurisdiction that has not been subject to an adequacy decision, or another transfer mechanism recognized under Data Protection Laws applicable in these jurisdictions.
- **Security Addendum**: The technical and organizational measures applicable to the provision of the services at https://flare.io/legal/Flare-Security-Addendum , as modified from time to time.

`

- The terms "**controller**," "**processor**," "**service providers**" and "**subprocessors**" and shall have the meaning set forth in Data Protection Laws.

2. INTERPRETATION

2.1. **Structure**: This DPA outlines the terms and conditions applicable to the processing of Customer Data by the parties pursuant to the Principal Agreement and include the following schedules, which form an integral part of this DPA. If you are in the European Union, Schedule B.1 applies to any Restricted Transfers outside of the European Union, and if you are in the United Kingdom, Schedule B.2 applies to Restricted Transfers outside of the United Kingdom.

- **Schedule A**: Personal Data Processing.
- **Schedule B**: Independent Processing.
- **Schedule B.1**: EU Restricted Transfers (GDPR only).
- **Schedule B.2**: UK Addendum for Restricted Transfer (UK GDPR only).

2.2. **Relationship:** Schedule A set forth the terms and conditions applicable to the processing of Personal Data by Flare, on behalf of Customer. They are designed to cover the needs of our clients in various jurisdictions, including the GDPR. Schedule B contains the terms and conditions applicable to the use of Personal Data which Flare does not process on behalf of Customer, but as an independent controller, including Public Data.

2.3. **Partners**: When Flare processes data on behalf of Partner, this DPA shall find application with the following adjustments: any reference to "Customer Data" in this DPA will be interpreted as "Partner Data" and all references to the "Principal Agreement" will refer to the "Partner Terms."

3. CUSTOMER DATA

3.1. **License:** For the period indicated in an Order Form (the "**Subscription Term**"), Customer grants Flare a limited, non-exclusive, non-transferable (except as set forth in the Agreement) and revocable license to use Customer Data solely to: (a) provide the products and services pursuant to the Agreement; (b) comply with its obligations under the Agreement and applicable Data Protection Laws; (c) monitor and improving the performance and security of the services; and (d) generating Aggregated Data and Anonymized Data, provided that such data no longer identifies individuals or the Customer directly or indirectly. Customer is responsible for ensuring that it has all the rights, consents and approval required for Flare to process Customer Data pursuant to the Agreement

3.2. **Anonymized Data:** Flare may create Anonymized Data from Customer Data in accordance with applicable Data Protection Laws. For the duration of the Subscription Term, Customer grants Flare a perpetual, non-exclusive, royalty-free, irrevocable, and transferable license to use, modify, and exploit Anonymized Data for improving the products and services, conducting research and development, and similar legitimate and internal business purpose.

3.3. **Aggregated Data**: Aggregated Data shall be the exclusive property of Flare, and Flare may use this data without restriction, provided that such data does not identify or re-identify Customer or any individual.

3.4. **Hosting Location**. Customer Data will be hosted in the United States.

4. SECURE DELETION

4.1. **Secure Deletion.** Flare will, upon Customer's request or within 30 days of the end of the then-current Subscription Term, securely delete, or return and securely delete the Customer Data. Notwithstanding the foregoing, Flare may retain Customer Data longer strictly as required under applicable laws, or for to ensure business continuity in encrypted back-ups. This DPA, along with the Security Addendum, shall continue to find application for as long as either party is processing Customer Data, or Personal Data, pursuant to the Agreement.

`

5. COLLABORATION

5.1. **Breach.** Each party will notify the other party in writing without undue delay of a breach of this DPA or Data Protection Laws ("**Violation**") within 48 hours of becoming aware of such a Violation. The parties will collaborate in good faith to mitigate the impacts of any Violation, and prevent the recurrence of the Violation.

5.2. **Compliance**. If required by Data Protection Laws, Flare may change this DPA by providing a prior notice of 30 days to Customer. If Customer disagrees with the changes during this period, Customer may contact Flare at privacy@flare.io; otherwise, the changes will be considered in force after this period.

6. AUDITS AND COMPLIANCE

6.1. **Audit Rights**: Once per calendar year, upon giving Flare at least 30 days' written notice, Customer may audit Flare's compliance with this DPA (including the Security Addendum). Flare will provide all information reasonably required to demonstrate compliance. All information provided by Flare during these audits shall remain confidential.

6.2. **Audit Process**: Audits must be conducted by individuals bound by confidentiality obligations and during regular business hours to minimize disruption to Flare's operations. In case of any identified non-compliance, the parties will agree on a remediation plan, and Flare will provide regular updates on its completion

6.3. **Follow-Up Audits**: If an audit reveals any material non-compliance, Customer may conduct a follow-up audit within the same calendar year to verify that the remediation plan has been properly implemented.

7. LAW ENFORCEMENT

7.1. **Legal Request:** Flare will not disclose Personal Data to law enforcement or a governmental authority (a "**Legal Request**") unless it reasonably believes that it is required by applicable laws. If Flare receives such as a Legal Request, Flare will attempt to redirect the law enforcement and governmental authority to Customer, and to the full extent permitted under applicable laws, Flare will inform Customer of Legal Requests before complying with a Legal Request, including to give Customer the reasonable opportunity to object to the Legal Request. At Customer's costs and expenses, Flare will assist Customer to object and contest such Legal Request, where practicable.

7.2. **Response:** Upon receipt of a Legal Request, Flare will make a prompt and careful assessment of its legality, validity and appropriateness. If Flare must respond to the Legal Request, it will respond only to the extent required under applicable laws.

7.3. **Measures:** Flare will adopt reasonable and proportional policies and procedures designed to ensure that Legal Requests are handled in accordance with this DPA and Data Protection Laws. These measures will include proper documentation of Legal Requests.

`

SCHEDULE A: PERSONAL DATA PROCESSING

This Schedule A outlines the terms and conditions under which Flare processes Personal Data on behalf of the Customer. All references to "Personal Data" in this Schedule are related to the data processed by Flare on behalf of the Customer under the Principal Agreement, as part of the services.

1. INSTRUCTIONS

1.1. **Instructions:** Flare will process the Personal Data based on the instructions of Customer, including, as described in the technical documentation, or in the Agreement. If Flare becomes aware that such instructions are in violation of Data Protection Laws, Flare will inform Customer without undue delays. Flare may refuse to process Personal Data based on an instruction it believes is in violation of Data Protection Laws.

1.2. **Processing**. To the extent applicable under Data Protection Laws, Customer is the controller of the personal data, and Flare is the processor of the personal data. The data processing is substantially as described below.

Nature and Subject-matter	As described in the Documentation.
Categories of Data Subjects	● Platform end users ● Monitored individuals The categories of data subjects concerned by the processing depends on the nature of the identifiers selected by Customer.
Duration	For the Subscription Term
Categories of Personal Data	As described in the Product Privacy Policy.

1.3. **Legal Obligation:** If Flare must process the Personal Data to comply with applicable laws, or the administration thereof, Flare will inform Customer of such obligation prior to processing the Personal Data, unless prevented so under such applicable laws.

1.4. **GDPR/UK GDPR.** For clarity, as further described in the DPA, Flare will assist Customer in ensuring compliance obligations pursuant to Articles 32 to 36 of the GDPR/UK GDPR, considering the nature of processing and the information available to Flare.

1.5. **Anonymization**: Flare may generate Anonymized and Aggregated data from the Personal Data provided by Customer. Flare will only de-identify or anonymize Personal Data as permitted under Data Protection Laws, including in accordance with authorities' guidelines on de-identification and anonymization. Anonymized Data, if any, will be anonymized using industry-standard methods and in a manner such as to prevent the re-identification of individuals as required under such Data Protection Laws.

1.6. **Security:** The technical and organizational measures implemented to protect the Personal Data are described in the Security Addendum. Flare will ensure that all personal authorized to process Personal Data are bound by confidentiality obligations, either through contractual agreements or statutory requirements, and have received appropriate training on their responsibilities.

1.7. **DPIA:** If Customer must perform a privacy impact assessment ("**PIA**") or data protection impact assessment ("**DPIA**") pursuant to Data Protection Laws, Flare will collaborate in good faith, such as by making information reasonably requested available in a timely manner. Additional support by Flare to Customer in this regard may be subject to payment of additional fees by Customer to Flare.

2. DATA SUBJECT RIGHTS

`

2.1. **Response:** Each party agrees to collaborate with the other party to respond to requests from concerned individuals regarding their Personal Data (a "**Data Subject Request**"). Flare will promptly inform Customer if it receives a Data Subject Request. Customer is responsible for responding to the Data Subject Requests.
2.2. **Measures:** Flare will implement and maintain necessary technical and organizational measures to respond to Data Subject Requests in accordance with Data Protection Laws. These measures will include, to the extent applicable under Data Protection Laws, measures for concerned individuals to obtain copies of their Personal Data.

3. SUBPROCESSORS

3.1. **Authorization.** Customer hereby authorizes the use of the subprocessors listed at https://flare.io/legal/ , as modified from time to time in accordance with this Agreement.
3.2. **Due Diligence:** Prior to allowing a service provider or subprocessors to process Personal Data on its behalf, Flare will (a) conduct a reasonable due diligence of such subprocessors, and (b) enter into an agreement containing terms substantially similar to those contained herein regarding the protection of Personal Data.
3.3. **Changes:** Prior to making changes to its list of subprocessors, Flare will inform Customer in writing at least 30 days before such modification is effective. Customer will have 15 days to inform Flare if it has any objection by providing a written description of such reasonable objections. The parties will attempt to resolve the disagreement in good faith. If the parties cannot agree within 30 days, either party can terminate the Agreement without penalty, and Flare will reimburse to Customer any fees paid in advance for services not rendered at the date of termination.

4. RESTRICTED TRANSFERS

4.1. **Restrictions**: Prior to transferring Personal Data outside any other jurisdiction than the jurisdiction in which the Personal Data is collected, Flare will (a) conduct a reasonable assessment of the risks associated with the transfer of Personal Data; (b) enter contracts with recipients to ensure that the transfer is subject to adequate protections as required by Data Protection Laws, except to the extent the transfer is required under applicable laws. Flare will comply with additional safeguards required under Data Protection Laws. If required by Data Protection Laws, Flare will enter appropriate standard contractual clauses for Restricted Transfers.
4.2. **Third Parties:** If Customer instructs Flare to transmit Personal Data to a third party (e.g., an integration partner), Customer is responsible for ensuring that the transfer to the third party is lawful, and that all appropriate safeguards are in place. Flare makes no prior verification of third parties, Including any security or privacy measures.

5. PERSONAL DATA BREACH

5.1. **Notification:** In the event of a Personal Data Breach, Flare will inform Customer without undue delays of being aware of the Personal Data Breach, but no later than within 48 hours of becoming aware of the Personal Data Breach. The notification will include:
- A description of the nature of the Personal Data Breach, including the categories and approximate number of Data Subjects affected, and the categories and approximate number of Personal Information records concerned.
- The name and contact details of the Data Protection Officer or another contact point where more information can be obtained.
- A description of the likely consequences of the Personal Data Breach.
- A description of the measures taken or proposed to be taken by Flare to address the Personal Data Breach, including measures to mitigate its possible adverse effects.

5.2. **Follow Ups:** If such information is not available at the time of the initial disclosure, Flare will follow up promptly with as such information becomes available. Flare will also inform Customer of remediation actions taken or to be taken regarding the Personal Data Breach.
5.3. **Cooperation:** Flare will cooperate with Customer regarding a Personal Data Breach, including to take reasonable measures to assist in the investigation, mitigation and remediation of the Personal

`

Data Breach in accordance with Data Protection Laws. Flare will also provide reasonable assistance to Customer in case a notification to the authorities, concerned individuals, or third parties is required.

6. DELETION AND RETENTION

6.1. **Deletion:** Flare will securely delete Personal Data that is no longer required. Customer Data is deleted in accordance with the Agreement.

`

SCHEDULE B: INDEPENDENT PROCESSING

This Schedule B outlines the terms and conditions under which Flare and Customer act as independent controllers with respect to the processing of Personal Data, i.e., data that is not processed on behalf of the other party, including, without limitation, the transmission of Public Data through the Flare Platform, or the sharing of business contact information with resellers.

1. PROCESSING

1.1. **Independent Controllers:** To the extent applicable under Data Protection Laws, each party acknowledges that they act as independent controllers with regards to Personal Data which are not processed by processor on behalf of Customer. Neither party is a joint controller with the other in respect of such data.
1.2. **Flare:** Flare is an independent controller regarding the Public Data and Intelligence Data it makes available through the Flare Platform, including, through API Calls.
1.3. **Customer:** Customer is provided with the licence to use the Public Data and Intelligence Data as described in the Principal Agreement, and for the permitted purposes.

2. OBLIGATIONS OF THE PARTIES

2.1. **Compliance**: Notwithstanding anything to the contrary, each party shall, in connection with the processing of Personal Data as independent controllers: (a) comply with Data Protection Laws; (b) ensure that there is a lawful basis for their respective processing; (c) indemnify and hold harmless the other party from any third-party claims, losses and damages resulting from their breach of this Schedule B, or Data Protection Laws.
2.2. **Transparency:** Each party shall provide transparent information to data subjects regarding the processing of their personal data, as required by Data Protection Laws.
2.3. **Data Subjects Requests:** Each party is individually responsible for responding to Data Subject Requests concerning the Personal Data it controls. The parties shall provide reasonable assistance to each other as necessary to enable the exercise of Data Subjects Requests.
2.4. **Personal Data Breach:** Each party is individually responsible for its compliance with requirements under Data Protection Laws in case of a Personal Data Breach.

-

3. RESTRICTED TRANSFERS

3.1. **European Union.** In case of a Restricted Transfer from the European Union, the controller-to-controller standard contractual clauses adopted by the European Commission are applicable to the Restricted Transfer, and shall be deemed part of, and integrated therein. The information detailed under Attachment 1 will find application.
3.2. **United Kingdom.** In case of a Restricted Transfer from the United Kingdom, the UK Addendum will find application as set forth under Attachment 2.

`

ATTACHMENT 1—RESTRICTED TRANSFER TO THE EUROPEAN UNION

This Attachment 1 to the DPA contains the annexes applicable to the controller-to-controller standard contractual clauses in case of a Restricted Transfer from the European Union.

ANNEX 1. A LIST OF PARTIES

The signatures and dates are available in the Agreement.

Data Exporter	
Name:	Flare Systems, Inc.
Address:	1751 rue Richardson, Unit 3, 108, Montreal, QC, H3K 1G6
Contact Details:	privacy@flare.io
Activities relevant to the data transferred under the DPA:	Threat intelligence management platform allowing data importers to obtain public data about monitored assets, like leaked credentials.
Role:	Controller

Data Importer	
Name:	As indicated in the Principal Agreement
Address:	As indicated in the Principal Agreement
Contact Details:	As indicated in the Principal Agreement
Activities relevant to the data transferred under the DPA:	For the purposes authorized in the Principal Agreement—Receipt and further processing of the Personal Data for its own purposes.
Role:	Controller

ANNEX 1.B. DESCRIPTION OF TRANSFER

1. Categories of Data Subjects whose Personal Data is Transferred

- The data importer's employees and other business contacts.

2. Categories of Personal Data Transferred

- Business contact information, such as employee name, contact information, emails
- API Calls Data (e.g., credentials)
- Public Data
- Intelligence Data (if any Personal Data)

3. Sensitive Data transferred and applied restrictions or safeguards

- The data importer configures the data that are exported, including, Public Data, Intelligence Data, based on identifiers.

4. Nature of the processing

As described in the Agreement

5. Nature of the Processing

The transfer is made for the following purposes:

`

- Make available Intelligence Data through API Calls, or otherwise through the Flare Platform
- If pursuant to the Partner Terms, to develop customers and opportunities together, including, to resell the Flare Platform as part of your commercial offering.

6. The Period for which the Personal Data will be Retained, or, if that is not Possible, the Criteria Used to Determine that Period.

The data importer retains the personal data as long as is necessary based on the Intended Purposes. To determine the appropriate retention period for Personal Data, the data importer considers the amount, nature and sensitivity of the Personal Data, the potential risk of harm from unauthorized use or disclosure of the personal data, the purposes for which the personal data is processed and whether such purposes can be achieved through other means, and the applicable legal, regulatory, tax, accounting or other requirements.

7. **For transfers to (Sub-) Processors, also Specify Subject Matter, Nature and Duration of the Processing**

No subprocessor is involved in the Restricted Transfer. Customer is obtaining the Personal Data directly from the Flare API, or directly from Flare.

ANNEX 1.C. SUPERVISORY AUTHORITY

The Competent Supervisory Authority **in accordance with Clause 13(a) of the EU Transfer Clauses:**

Commission nationale informatique et libertés, France.

ANNEX 2—TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

The measures adopted by the Data Exporter are in the Security Addendum. The data importer agrees to deploy commercially reasonable efforts to develop, implement and maintain security measures that are substantially similar to those described in the Security Addendum in relation to the Personal Data. The data transfer occurs through the Flare API, and is encrypted.

`

SCHEDULE D

UK Addendum to
EU Standard Contractual Clauses

This Appendix C contains the Standard Data Protection Clauses issued under S119A (1) of the UK Data Protection Act 2018 and applies to Transfers of Personal Data from the UK which is not subject to an adequacy status. This Appendix C is an addendum to Appendix B—EU Standard Contractual Clauses are therefore included in this Appendix C.

Part 1: Tables

Table 1: Parties (Information below is provided in Annex A of the DPA)

Start date	The effective date of the Principal Agreement.	
The Parties	**Exporter** (who sends the Restricted Transfer)	**Importer** (who receives the Restricted Transfer)
Parties' details	**Full legal name**: Flare Systems, Inc. **Trading name** (if different): **Main address** (if a company registered address): 1751 Rue Richardson, Unit 3.108, Montréal, Quebec, H3K 1G6, Canada **Official registration number** (if any) (company number or similar identifier): As specified in the Principal Agreement. 1178044542	**Full legal name**: As specified in the Principal Agreement. **Trading name** (if different): **Main address** (if a company registered address): As specified in the Principal Agreement. **Official registration number** (if any) (company number or similar identifier): As specified in the Principal Agreement.
Key Contact	**Full Name** (optional): As specified in the Principal Agreement. **Job Title**: As specified in the Agreement. **Contact details including email**: privacy@flare.io.	**Full Name** (optional): As specified in the Principal Agreement. **Job Title**: As specified in the Principal Agreement. **Contact details including email**: As specified in the Principal Agreement.
Signatures	Signature of the Principal Agreement constitutes signature of this Addendum.	Signature of the Principal Agreement constitutes signature of this Addendum.

Table 2: Selected SCCs, Modules and Selected Clauses

Addendum EU SCCs	**The version of the Approved EU SCCs which this Addendum is appended to, detailed below, including the Appendix Information:** **Date**: The execution date of the Principal Agreement. **Reference**: Module 1 of the SCC: Controller-to-Controller. **Other identifier**: N/A

`

Table 3: Appendix Information

"Appendix Information" means the information which must be provided for the selected modules as set out in the Appendix of the Approved EU SCCs (other than the Parties), and which for this Addendum is set out in:
Annex 1(A): List of Parties: Annex I(A)
Annex 1(B): Description of Transfer: Annex I(B)
Annex II: Technical and organizational measures including technical and organizational measures to ensure the security of the data: Annex II
Annex III: List of Sub processors (Modules 2 and 3 only): N/A

Table 4: Ending this Addendum when the Approved Addendum Changes

Ending this Addendum when the Approved Addendum changes	Which Parties may end this Addendum as set out in Section 19: ☑ Importer ☑ Exporter ☐ Neither Party

Part 2: Mandatory Clauses

Mandatory Clauses of the Approved Addendum, being the template Addendum B.1.0. issued by the Information Commission Office (ICO) and laid before the UK Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18 of those mandatory clauses.

`