Data Processing Addendum

Version 1.0 - Effective on 2024-07-01

This Data Processing Addendum and its Annexes (the "DPA") reflects the agreement between Flare and Customer with respect to the Processing of Personal Data by Flare on behalf of Customer for the provision of the Services under the Terms of Service ("TOS") between you and Flare.

This DPA is supplemental to, and forms an integral part of, the TOS and enter into force at Effective Date and continues to full force for as long as Flare is Processing Personal Data on behalf of Customer pursuant to the TOS. In the event of any conflict, inconsistency, or ambiguity between the provisions of this DPA and the remaining of the TOS, 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

The terms not otherwise defined here are defined in the TOS.

- **"Data Protection Laws**" means any laws, treaties, and regulations applicable to the processing of Personal Data by either party pursuant to the TOS, including, the EU's *General Data Protection Regulation*, the UK's the *Data Protection Act 2018*, Canada's the *Personal Information Protection and Electronic Documents Act***,** Quebec's *Act Respecting the Protection of Personal Information in the Private Sector* and any state or provincial privacy laws.
- **"Data Subject"** means an identified or identifiable natural person whose Personal Data is processed by Flare on behalf of Customer.
- **"Data Subject Request"** means the exercise by a Data Subject of his or her rights granted under Data Protection Laws regarding his or her Personal Data.
- "**Privacy Breach**" means the processing of Personal Data in violation of this DPA or Data Protection Laws, including a loss of Personal Data, or access, use or communication of Personal Data not authorized by law.

2. Customer Responsibilities

2.1. Customer is solely responsible for: (1) the accuracy, quality, and legality of Personal Data and the means by which you acquired Personal Data; (2) complying with all applicable Data Protection Laws for the collection and use of the Personal Data; (3) communication a revocation of consent or authorization by Data Subjects to Flare; (4) ensuring you have the right to transfer, or provide access to, the Personal Data to us as set forth in the TOS; and (5) ensuring that your instructions to us regarding the Processing of Personal Data comply with applicable laws, including Data Protection Laws.

2.2. Customer shall indemnify and hold Flare harmless from any damages, losses, liabilities, costs, and expenses (including reasonable attorneys' fees) incurred by Flare as a result of any claim, demand, or action arising out of or related to Flare's compliance with Customer's instructions regarding the Processing of Personal Data under this DPA. Customer's indemnification obligations will apply to the extent that such damages, losses, liabilities, costs, and expenses are not directly caused by Flare 's breach of its obligations under this DPA.

3. Processing Instructions

`

3.1. Flare will process the Personal Data to provide the Services, and in accordance with Customer's instructions (including the TOS). You may also provide us with additional instructions during the Subscription Term that are consistent with the TOS. Flare will not process Personal Data for marketing purposes or otherwise commercialize the Personal Data.

3.2. 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.

3.3. If Flare is required to 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. If the TOS must be amended to Data Protection Laws, Flare will make such modifications as required pursuant to Data Protection Laws and inform Customer in writing. Notwithstanding anything to the contrary, this modification will be deemed effective within 30 days of being notified to Customer, unless Customer provides written motives for rejecting the changes, in which case, the parties will negotiate in good faith.

3.4. 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.

4. Cross-Border Transfer

4.1. Customer authorizes Flare and its Subprocessors to make cross-border transfers of Personal Data in accordance with this DPA so long as Data Protection Laws for such transfers are respected.

4.2. If required under Data Protection Laws, 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; (b) enter contracts with recipients to ensure that the transfer is subject to adequate protections, except to the extent the transfer is required under applicable laws. Flare will comply with additional safeguards required under Data Protection Laws. Upon request, if applicable, Flare will provide Customer with a list of transfers affecting the Personal Data, if those transfers are not to Subprocessors. Customer is responsible for conducting any risk assessment applicable to its own transfer of the Personal Data to Flare.

4.3. If the Processing of Personal Data includes transfer from the EEA, Switzerland and the United Kingdom to another jurisdiction that has not been subject to an adequacy decision, or another transfer mechanisms recognized under Data Protection Laws, the applicable Standard Contractual Clauses (including if applicable, the UK Addendum) will apply.

5. Privacy Breach

5.1. Flare will inform Customer without undue delays of any Privacy Breach, including by providing the information necessary for Customer to assess the risks relating to such Privacy Breach. Flare will further inform Customer of any suggested remediation measures to prevent the recurrences of such Privacy Breach. Flare's 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 Data records concerned.
- The name and contact details of the person who can be contacted for more information.
- 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. If such information is not available at the time of the initial disclosure, Flare will follow up promptly as such information becomes available. We will also inform you of remediation actions taken or to be taken regarding the Privacy Breach. Except if required under Data Protection Laws Flare will not inform any third party of any Privacy Breach without Customer's written consent. The parties will collaborate in good faith as necessary to notify concerned individuals and authorities of such Privacy Breach.

6. Data Subject Rights

6.1. Each party agrees to collaborate with the other party to respond to Data Subject Requests in accordance with Data Protection Laws. Flare will assist Customer, to the extent possible, in fulfilling its obligations to respond to requests from Data Subjects exercising their rights under Data Protection Laws. Flare will promptly notify Customer if it receives a request from a Data Subject to exercise their rights under Data Protection Laws.

6.2. Flare will implement and maintain necessary technical and organizational measures to ensure the facilitation of Data Subject Requests as stipulated under Data Protection Laws. Such measures should be designed to anticipate and promptly respond to requests from Data Subjects exercising their rights, in a manner that is appropriate and in line with the obligations under Data Protection Laws. Flare will implement technical and organization measures to ensure that Data Subjects can obtain a copy of the Personal Data Processed by Flare in the form of a written and intelligible transcript, and unless doing so raises serious practical difficulties as intended under Data Protection Laws, computerized Personal Data collected directly from individuals (excluding those that are created or inferred using Personal Data) must, at the Data Subjects' request, be communicated to the Data Subject, or to any person or body authorized by law to collect such Personal Data, in a structured, commonly used technology format.

7. Collaborations

7.1. If Customer is required to 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.

7.2. The Parties will collaborate in good faith to comply with Data Protection Laws, including by (a) notifying the other Party the breach of this DPA and amending the DPA as necessary to ensure compliance with Data Protection Laws.

7.3. Once per calendar year, upon a prior written notice of 30 days to Flare, Customer may audit Flare's compliance with the terms and conditions of this DPA. This audit will include written requests for information and questionnaire review, including access to Flare's recent SOC II Type 2 attestation, or similar independent third-party independent report. The foregoing information is Flare's Confidential Information. This audit must be performed by individuals subject to an appropriate confidentiality obligation, and during business hours. If Customer's audit demonstrates non-compliance, the parties will enter a commercially reasonable remediation plan. Flare will provide regular updates to Customer on the completion of the remediation plan, until completion. Notwithstanding the foregoing, Customer may conduct an additional audit in the same calendar year to follow up on the completion of the remediation plan.

8. Subprocessors

8.1. Prior to allowing a Subprocessor to process Personal Data, 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. Unless Flare makes other means of disclosures available to Customer, as modified from time to time,

8.2. 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 TOS without penalty, and Flare will reimburse to Customer any Fees paid in advance for Services not rendered at the date of termination.

8.3. Our Services may provide access to, connect, or otherwise interact with third-party services, including those accessed through API connections ("Third Parties"). Third Parties are not our Subprocessors. Customer acknowledges and agrees that it is solely responsible for all data transfers, international transfers obligations, and any other verifications related to such third-party services. Flare hereby excludes all liability for any damages, losses, or claims arising from or in connection with the use of such Third Parties. This exclusion of liability also extends to any cookies or add-ons installed on white-labeled Services provided to Customer.

9. Information Security

9.1. Flare will maintain appropriate technical and organizational measures to protect Personal Data from Personal Data Breaches, as described in Flare Security Addendum. We may modify or update the Security Addendum at our discretion, provided that such modification or update does not result in a material degradation in the protection of Personal Data.

9.2. Customer is solely responsible for independently determining whether data security provisions of the Services adequately meet the Customer's obligations under applicable law. You are also responsible for your secure use of the Services, including protecting the security of Personal Data in transit to and from the Services (including to securely backup or encrypt any such Personal Data).

10. General Terms

10.1. If any individual provisions of this DPA are determined to be invalid or unenforceable, the validity and enforceability of the other provisions of this DPA will not be affected.

10.2. This DPA constitutes the entire agreement between the Parties with respect to the subject matter hereof and replaces all prior agreements, written or oral, with respect to such subject matter.

10.3. Flare reserves the right to amend or update this DPA from time to time. Any changes will be effective immediately upon the posting of the revised DPA on our website or other accessible online platform. As such, we encourage the Customer to periodically review this DPA online for the latest information on our data processing practices. In case of significant changes that materially alter our data processing practices, we may also notify the Customer by email or via a notice on our website prior to the changes taking effect.

10.4. The nature and purpose of the data processing under this DPA may change due to enhancements in our Services, changes in Data Protection Laws, or other relevant reasons. In such cases, Flare will provide the Customer with reasonable notice of any significant changes in the way we process Personal Data under this DPA. The Customer's continued use of the Services after any such changes have been notified and taken effect will constitute the Customer's agreement to the changes in the data processing.

`

Annex A
Details of Processing

List of Parties

1. Data exporter:

Name: Customer, as defined in the Order Form (on behalf of itself and Affiliates)

Address: Customer's address, as set out in the Order Form

Contact person's name, position and contact details: Customer's contact details, as set out in the Order Form

Activities relevant to the data transferred under the DPA: Processing of Personal Data in connection with Customer's use of the Services under the TOS

Role (controller/processor): Controller

2. Data importer:

Name: Flare as defined in the TOS

Address: As set out in the TOS

Contact person's name, position and contact details: Flare's contact details, as set out in the Order Form

Activities relevant to the data transferred under the DPA: Processing of Personal Data in connection with Customer's use of the Services under the TOS.

Role (controller/processor): Controller

Description of Transfer

1. Categories of Data Subjects whose Personal Data is Transferred

You may submit Personal Data in the course of using the Services, the extent of which is determined and controlled by you in your sole discretion, and which may include, but is not limited to Personal Data relating to the following categories of Data Subjects: End Users, as well as other concerned individuals whose Personal Data are monitored based on Customer's instructions.

2. Categories of Personal Data Transferred

You may submit Personal Data to the Services, the extent of which is determined and controlled by you in your sole discretion, and which may include but is not limited to the following categories of Personal Data: End users, as well as other individuals who are monitored by Customer (e.g., using an Identifier).

3. Sensitive Data transferred and applied restrictions or safeguards

The categories of sensitive data transferred may include genetic, biometric and health data, as well as personal data revealing racial and ethnic origin, political opinions, religious or ideological convictions or trade union membership. Access is restricted and protected in accordance with applicable law. No Sensitive Personal Data should be transferred.

4. Frequency of the transfer

`

Continuous

5. Nature of the Processing

Personal Data will be Processed in accordance with the TOS (including this DPA) and may be subject to the following Processing activities:

- Flare provides and maintains an online web application allowing End Users to obtain Intelligence Data by processing Public Data. Threat intelligence can be obtained by assigning Identifiers and monitoring Public Data relating to these Identifiers through the Monitoring Services. Certain functionalities, such as the Retrieval Function, allow End User to extract Public Data. Flare also provides Technical Support regarding the Flare Platform to End Users who access the web application through accounts hosted by Flare, in the Flare Platform.

- Storage and other Processing necessary to provide, maintain and improve the Services provided to Customers.

- Disclosure in accordance with the TOS (including this DPA) or as compelled by applicable laws.

6. Purpose of the transfer and further Processing

We will Process Personal Data as necessary to provide the Services pursuant to the TOS and as further instructed by you in your use of the Services.

7. Duration of Processing

The Processing of Personal Data is for the duration of the Subscription Term.

`

Annex B: Flare Security Measures

A description of the technical and organisational security measures implemented by Flare are available in Flare's Security Addendum.

`