Data Processing Addendum

THIS DATA PROCESSING ADDENDUM ("**DPA**") IS ENTERED INTO PURSUANT TO THE AGREEMENT (HEREINAFTER DEFINED) UNDER WHICH EIGHTFOLD AI INC., A DELAWARE CORPORATION WITH OFFICES AT 2625 AUGUSTINE DRIVE, SUITE 601, SANTA CLARA, CA 95054 ("**EIGHTFOLD**") PROVIDES, AND YOU (THE "**CUSTOMER**") OBTAIN THE USE OF THE SERVICES. BY AGREEING TO THIS DPA, BY EITHER (1) CLICKING A BOX INDICATING ACCEPTANCE, OF SUCH DPA OR (2) EXECUTING A SALES ORDER THAT REFERENCES SUCH DPA, CUSTOMER REPRESENTS THAT CUSTOMER HAS FULL POWER, CAPACITY, AND AUTHORITY TO ACCEPT THE TERMS HEREIN. IF CUSTOMER IS ACCEPTING THE TERMS OF THIS DPA ON BEHALF OF AN EMPLOYER OR ANOTHER ENTITY, CUSTOMER REPRESENTS THAT CUSTOMER HAS FULL LEGAL AUTHORITY TO BIND SUCH EMPLOYER OR SUCH OTHER ENTITY TO THIS DPA. THIS DPA IS EFFECTIVE WHEN CUSTOMER CLICKS A BOX INDICATING ACCEPTANCE OR BEGINS USING THE SERVICES, WHICHEVER IS EARLIER ("**EFFECTIVE DATE**").

This DPA forms a part of and is incorporated into the Agreement (defined below). Capitalized terms used but not defined in this DPA shall have their meanings set forth in the Agreement.

1. Definitions

(a) "**Affiliate**" of a party means any entity that is controlled by a party to this Agreement, so long as the control exists. "Control" means direct or indirect control of more than 50% of the shares or other equity interests of the subject entity entitled to vote in the election of directors (or, in the case of an entity that is not a corporation, for the election or appointment of the corresponding managing authority). As to Customer, any reference to "Affiliate" herein is strictly limited to those Affiliates of Customer that qualify as a Controller with respect to the Controller Data and are permitted to use the Services pursuant to the Agreement, but have not signed their own Sales Order and are not a "Customer" as defined under the Agreement.

(b) "**Agreement**" means the subscription agreement between the parties, together with those connected statements of work, purchase orders, contracts, and/or agreements, pursuant to which Eightfold has agreed to provide the Services to Customer, and which may require Eightfold to Process Controller Data.

(c) "**Annex**" means, except as context otherwise requires, the referenced annex to this DPA, the terms and conditions of which are incorporated into this DPA by reference, as applicable.

(d) "**Controller**" means the entity that determines the purposes and means of the Processing of Personal Data.

(e) "**Controller Data**" means any and all Personal Data that Eightfold Processes on behalf of Customer or any Customer Affiliate in the course of providing the Services.

(f) "**Data Protection Laws**" means all laws and regulations applicable to the Processing of Controller Data by Eightfold under the Agreement, including, where applicable, but not limited to: (a) Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of Personal Data and on the free movement of such data (General Data Protection Regulation) ("**GDPR**"); (b) GDPR as it forms parts of the United Kingdom domestic law by virtue of Section 3 of the European Union (Withdrawal) Act 2018 ("**UK GDPR**"); (c) the California Consumer Privacy Act, as amended (including, without limitation, by the California Privacy Rights Act) ("**CCPA**"); and (d) other U.S. state privacy laws; in each case, as may be amended, superseded, repealed, consolidated, or replaced.

(g) "**Data Subject**" means an identified or identifiable natural person about whom Controller Data may be Processed under this DPA.

(h) "**Personal Data**" means information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular individual. This definition includes "personal data," "personal information," or "personally identifiable information," as defined by any applicable Data Protection Laws. Personal Data does not include information or data that has been Processed in such a manner that no longer identifies, relates to, describes, or is capable of being associated or linked with a particular Data Subject.

(i) "**Process**", "**Processes**", or "**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.

(j) "**Processor**" means an entity that Processes Controller Data on behalf of the Controller.

(k) "**Security Incident**" means any unauthorized or unlawful breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or unauthorized access to Controller Data that is Processed by Eightfold on behalf of Customer in providing the Services.

(l) "**Services**" shall have the definition of the term in the Agreement.

(m) "**Subprocessor**" means any Processor engaged by Eightfold to assist in Processing Controller Data with respect to providing the Services.

2. Scope and Applicability. Notwithstanding anything to the contrary, this DPA applies solely to the Processing of Controller Data and not to the Processing of any other Personal Data. With respect to any Controller Data, as between Eightfold and Customer, Customer is the Controller and Eightfold is the Processor. Eightfold may Process Controller Data on behalf of Customer solely in accordance with the terms of the Agreement, this DPA, and Customer's lawful instructions.

3. Purpose. The "**Business Purpose**" for Eightfold's Processing of Controller Data on Customer's behalf is identified in **Annex A**. The duration of Processing, the nature and purpose of the Processing, the types of Controller Data, and the categories of Data Subjects whose Personal Data is Processed under this DPA are further specified in **Annex A**.

4. Customer Representations and Warranties. Customer hereby represents and warrants that it: (a) will maintain appropriate notice and consent mechanisms, consistent with applicable Data Protection Laws, for the collection, use, and disclosure of Controller Data, including with respect to the use of cookies and similar tracking technologies deployed via Customer's sites and mobile applications; (b) has any and all consents, authorizations, rights, and authority necessary to transfer or disclose, and permit Eightfold to Process, any and all Controller Data in connection with the Agreement; and (c) has and will have sole responsibility for the accuracy, quality, and legality of any and all Controller Data provided to Eightfold for Processing by Eightfold. Customer will promptly notify Eightfold if it is unable to comply with any of its obligations hereunder.

5. Subprocessors. Customer acknowledges and expressly agrees that Eightfold may retain its Affiliates or certain third parties as Subprocessors to Process Controller Data in order to provide the Services. Customer hereby authorizes Eightfold to engage the Subprocessors referenced in **Annex C**. Customer shall have notification rights and rights to object to such Subprocessors in accordance with **Annex C**. Prior to a Subprocessor's Processing of Controller Data, Eightfold shall: (a) enter into an agreement with the Subprocessor that imposes data protection terms on the Subprocessor regarding the Processing of Controller Data to the standard required by Data Protection Laws and (b) remain liable for its compliance with the obligations subcontracted to the Subprocessor.

6. International Data Transfers. Eightfold may transfer Controller Data to, and Process Controller Data in, the United States and anywhere else in the world where Eightfold or its Subprocessors maintain data processing operations, and Customer hereby consents to the transfer of Controller Data to Eightfold and Subprocessor data processing operations located in the United States or anywhere else in the world where Eightfold or its Subprocessors maintain data processing operations, provided that any transfers by Eightfold to countries without an adequacy decision will be subject to a transfer impact assessment and/or any other legally-required transfer mechanism, which will be available to Customer for review upon request. The foregoing includes, without limitation, the express consent of Customer to the transfer of Controller Data outside of the European Economic Area and/or its member states (the "**EEA**"), Switzerland, and/or the United Kingdom (including Gibraltar, the "**UK**"). The parties agree that the data export solution identified in this DPA shall not apply if and to the extent that Eightfold adopts another alternative data export solution for the lawful transfer of Controller Data (as recognized under the applicable Data Protection Law) ("**Alternative Transfer Mechanism"**), in which event, the Alternative Transfer Mechanism shall apply instead (but only to the extent such Alternative Transfer Mechanism extends to the territories to which Controller Data is transferred).

7. Additional Terms. In addition to the terms of this DPA, if and to the extent Eightfold Processes or transfers (directly or via onward transfer) any Controller Data:

(a) That is Personal Data of Data Subjects residing in the EEA, the UK, or Switzerland that is transferred to the U.S., Eightfold shall comply with the EU-U.S. Data Privacy Framework (the "EU-U.S. DPF"), the UK Extension to the EU-U.S. DPF (the "**Data Bridge**"), and the Swiss-U.S. Data Privacy Framework (the "**Swiss-U.S. DPF**") as set forth by the U.S. Department of Commerce. Eightfold has certified to the U.S. Department of Commerce that it adheres (i) to the

EU-U.S. Data Privacy Framework Principles (the "**EU-U.S. DPF Principles**") with regard to the processing of Personal Data received from the EEA in reliance on the EU-U.S. DPF and from the UK in reliance on the Data Bridge, and (ii) to the Swiss-U.S. Data Privacy Framework Principles (the "**Swiss-U.S. DPF Principles**") with regard to the processing of Personal Data received from Switzerland in reliance on the Swiss-U.S. DPF. If there is any conflict between the terms in this DPA and the EU-U.S. DPF Principles and/or the Swiss-U.S. DPF Principles, the applicable principles shall govern. In the event Eightfold is no longer certified under the EU-U.S. DPF, the Data Bridge, or the Swiss-U.S. DPF, or any of the same are invalidated, then the terms set forth in Sections 7(b), 7(c), and 7(d), respectively, shall apply to the impacted transfers of Personal Data to the U.S.

(b) That is Personal Data of Data Subjects residing in the EEA, then, subject to Section 7(a), Module Two (*Controller to Processor*) of the Standard Contractual Clauses approved by the European Commission in Commission Decision 2021/914 dated 4 June 2021 (as amended and updated from time to time) ("**EU SCCs**") hereby apply to any transfers of such Controller Data outside of the European Economic Area and/or its member states, and are deemed incorporated into this DPA by reference, take precedence over the rest of this DPA to the extent of any conflict, and are completed as follows:

i. The optional docking clause in Clause 7 does not apply;

ii. In Clause 9, Option 2 (general written authorization) applies, and the minimum time period for prior notice of Subprocessor changes shall be as set forth in **Annex C**;

iii. In Clause 11, the optional language does not apply;

iv. In Clause 17 (Option 1), the EU SCCs will be governed by law of Ireland;

v. In Clause 18(b), disputes will be resolved before the courts of Ireland;

vi. **Annex A** contains the information required in Annex I of the EU SCCs;

vii. **Annex B** contains the information required in Annex II of the EU SCCs; and

viii. **Annex C** contains the information required in Annex III of the EU SCCs.

(c) That is Personal Data of Data Subjects residing in the UK, then, subject to Section 7(a), the EU SCCs, as amended by, and together with, the terms of **Annex D** apply;

(d) That is Personal Data of Data Subjects residing in Switzerland, then, subject to Section 7(a), the EU SCCs, as amended by, and together with the terms of **Annex E** apply;

(e) That is Personal Data subject to the CCPA, then the terms of **Annex F** apply; and/or

(f) That is Personal Data subject to any other U.S. state privacy law, then the parties agree that the details of the instructions for Processing, the nature and purpose of Processing, the type of Controller Data subject to Processing, and the duration of Processing are set forth in **Annex A**.

8. Confidentiality. Eightfold shall ensure that any person who is authorized by Eightfold to Process Controller Data shall be under an appropriate obligation of confidentiality (whether a contractual or statutory duty), with respect to such Controller Data.

9. Security. Eightfold shall implement and maintain throughout the term of the DPA, in accordance with industry practice, appropriate technical and organizational measures as set forth in **Annex B**. Customer acknowledges that these technical and organizational measures are subject to technical progress and development and that Eightfold may update or modify these technical and organizational measures from time to time, provided that such updates and modifications do not result in the material degradation of the overall security of the Services purchased by Customer.

10. Security Incident. In the event that Eightfold becomes aware of a Security Incident, Eightfold will notify Customer without undue delay and shall provide timely information relating to the Security Incident as it becomes known or as is reasonably requested by Customer, unless otherwise prohibited by law or otherwise instructed by a law enforcement or supervisory authority. Following such notification, Eightfold will take reasonable steps to mitigate the effects of the Security Incident and provide reasonable assistance and cooperation regarding any notifications that Customer is legally required to send to affected Data Subjects and regulators.

11. Security Reports and Audit Obligations. Eightfold shall provide written responses (on a confidential basis) to all

reasonable requests for information made by Customer that Customer (acting reasonably) considers necessary to confirm Eightfold's compliance with this DPA as well as applicable Data Protection Laws. Eightfold may satisfy audit obligations by providing Customer with attestations, certifications, and summaries of audit reports conducted by accredited third party auditors. If such attestations, certifications, and summaries do not reasonably address Customer's concerns, Customer may elect to audit technical and organizational measures taken by Eightfold and shall document the results. Audits by Customer will be reasonable in scope for the relevant subject matter and subject to the following terms: (a) the audit will be at Customer's expense; (b) the audit will be pre-scheduled in writing with Eightfold and will be performed not more than once a year (except as required by applicable law or mutually agreed upon for exigent circumstances); and (c) the auditor will execute a non disclosure and non-competition undertaking on terms acceptable to Eightfold.

12. Customer Security Responsibilities. Notwithstanding anything herein to the contrary, Customer agrees that except as provided by this DPA, Customer is responsible for its secure use of the Services, including securing its account authentication credentials, protecting the security of Controller Data when in transit to and from the Services and taking any appropriate steps to securely encrypt or backup any Controller Data uploaded to the Services. Eightfold's liability for a Security Incident toward Customer and any third party is subject to the following conditions: (a) the Security Incident is caused by a violation of Eightfold's or its Subprocessor's obligations set forth in this DPA (including violation of Data Protection Laws) and (b) it excludes liability caused by acts or omissions of Customer, or any person acting on behalf of or jointly with Customer.

13. Information and Assistance. To the extent required by an applicable Data Protection Law, Eightfold will cooperate with Customer in compiling necessary records of Processing activities for Customer as well as in necessary data protection impact assessments of Customer or subsequent consultation with a data protection supervisory authority or regulator. Eightfold may charge a reasonable fee for any such assistance, as permitted by applicable law.

14. Data Subject Requests. To the extent that Customer is unable to independently access the relevant Controller Data within the Services, Eightfold shall (to the extent permitted by law, at Customer's expense) taking into account the nature of the Processing, provide reasonable cooperation to assist Customer by appropriate technical and organizational measures, in so far as is possible, to respond to any requests from individuals or applicable data protection authorities relating to the Processing of Controller Data under the Agreement. In the event that any such request is made directly to Eightfold, Eightfold shall not respond to such communication directly without Customer's prior authorization, unless legally compelled to do so.

15. Subpoenas and Court Orders. If a law enforcement agency sends Eightfold a demand for Controller Data (for example, through a subpoena or court order), Eightfold shall give Customer reasonable notice of the demand to allow Customer to seek a protective order or other appropriate remedy unless Eightfold is legally prohibited from doing so.

16. Return or Disposal of Data. Upon termination or expiration of the Agreement for any reason, Eightfold will return or destroy Controller Data (including copies) in its possession or control at Customer's request and choice in accordance with the Agreement, provided this requirement shall not apply to the extent Eightfold is required by applicable law to retain some or all of the Controller Data.

17. Customer Affiliates. Customer shall cause its Affiliates to be bound by the obligations under this DPA and, to the extent applicable, the Agreement. For the avoidance of doubt, a Customer Affiliate is not and does not become a party to the Agreement. All access to and use of the Services by any Customer Affiliates must comply with the terms and conditions of this DPA and any violation of the terms and conditions of this DPA by a Customer Affiliate shall be deemed a violation by Customer. The Customer entity that is the contracting party to the Agreement ("**Contracting Party**") shall remain responsible for coordinating all communication with Eightfold under this DPA and be entitled to make and receive any communication in relation to this DPA on behalf of its Affiliates. To the extent any applicable Data Protection Law requires that a Customer Affiliate be entitled to exercise the rights and seek remedies under this DPA, the parties agree that (a) the Contracting Party is the sole entity entitled to exercise any such right or seek any such remedy on behalf of its Affiliates, and (b) the Contracting Party shall exercise any such rights under this DPA in a combined manner for itself and all of its Affiliates together, not individually.

18. 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, whether in contract, tort, or under any other theory of liability, is subject to the limitations and exclusions of liability in the Agreement, and any reference in provisions to the liability of a party means the aggregate liability of that party and all of its Affiliates under the Agreement and the DPA together. For the avoidance of doubt, to the extent permitted by law, Eightfold and its Affiliates' total liability for all claims from Customer and all of its Controller Affiliates arising out of or related to the Agreement and the DPA shall apply in the aggregate for all claims under both the Agreement and the DPA.

19. Miscellaneous. To the extent applicable, the parties agree that by entering into and executing this DPA, the EU SCCs and

all Annexes constitute legally binding contracts between the parties and are hereby deemed to be signed by the parties. If there is any conflict between this DPA and the Agreement, this DPA shall prevail to the extent of that conflict. Unless otherwise provided for in this DPA or required by applicable Data Protection Law, (a) this DPA shall be governed by and construed in accordance with governing law and jurisdiction provisions in the Agreement, and (b) any disputes between the parties arising under this DPA are to be handled as set out in the Agreement.

ANNEX A - DETAILS OF PROCESSING

1. **List of Parties:**

***For the purposes of the EU SCCs (as applicable), this information constitutes the details of "Annex 1.A".*

Data exporter: Customer

Address (if not set forth in the Agreement): As set forth in the order form/Agreement.

Contact person's name and position: As set forth in the order form/Agreement.

Contact person's contact details (including email): As set forth in the order form/Agreement.

Activities relevant to the data transferred under the SCCs (as applicable): See DPA and Agreement

Signature and date: As set forth in the order form/Agreement.

Role: Controller

Data importer: Eightfold

Address: 2625 Augustine Drive, Suite 601, Santa Clara, CA 95054

Contact person's name and position: Lillian Pang, DPO

Contact person's contact details (including email): % privacy@eightfold.ai

Activities relevant to the data transferred under the SCCs (as applicable): See DPA and Agreement

Signature and date: As set forth in the order form/Agreement.

Role: Processor

2. **Details of Processing:**

***For the purposes of the EU SCCs (as applicable), this information constitutes the details of "Annex 1.B".*

(a) Categories of Data Subjects. The Data Subjects whose Personal Data may be Processed and/or transferred as Controller Data includes:

Authorized Users: Any employees, contractors, or other third parties who are authorized under the Agreement to use the Services.

Customer Job Candidates: Any natural person who is a job candidate to Customer's job positions and whose job profile Customer uses the Services to Process in accordance with the Agreement.

(b) Categories of Personal Data: The categories of Personal Data that may be Processed and/or transferred as Controller Data includes:

Authorized Users: Identification and contact data (name, address, title, contact details, username); employment details (employer, job title, geographic location, area of responsibility); IT related data (computer ID, user ID, password, IP address, log files).

Customer Job Candidates: Customer's job candidate data (including resumes with professional and educational background, email, address, phone number) and any other Customer Job Candidate data that Customer configures

the Services to Process, if any, subject to the limits of the data the Services are intended to and technically able to lawfully Process.

(c) Special categories of data (if appropriate): Eightfold and/or its Subprocessors do not intentionally Process any special categories of Personal Data unless instructed by Customer as part of Processing job candidates' information in connection with the Services under the Agreement.

(d) Frequency of the Transfer: Continuous during the term of the Agreement.

(e) Nature of the Processing: The Controller Data transferred will be Processed in accordance with this DPA and the Agreement and may be subject to the following Processing activities:

- storage and other Processing necessary to provide, maintain and improve the Services provided to Customer
- to provide customer and technical support to Customer; and
- disclosures in accordance with the Agreement, as compelled by law.

(f) Purposes of Transfer and Processing: For the purposes of: (i) providing the Services under the Agreement, (ii) to perform any steps necessary for the performance of its obligations under the Agreement, (iii) as initiated by any Authorized User in its use of the Services, and (iv) to comply with other reasonable and lawful instructions provided by Customer.

(g) Period for which Personal Data will be retained, or the applicable criteria to determine that period: In accordance with the terms of this DPA and the Agreement.

(h) Transfers to Subprocessors: See details of **Annex C**. The subject matter of the Processing by such Subprocessors is described in **Annex C** and above. The Processing is for the purposes described above and in **Annex C**, and for the duration of the Agreement, consistent and coterminous with the duration of Processing expected of and by Eightfold under the Agreement, subject to the retention period criteria described above.

(i) Competent Supervisory Authority (if applicable):

***For the purposes of the EU SCCs (as applicable), this information constitutes the details of "Annex 1.C".*

Data Protection Commission of Ireland

ANNEX B - TECHNICAL AND ORGANIZATIONAL MEASURES INCLUDING TECHNICAL AND ORGANIZATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

Below is a description of the technical and organizational measures Eightfold implements for data protection and security. Eightfold regularly checks that these measures continue to provide an appropriate level of security. These Technical and Organizational Measures ("Security Terms") are incorporated into and form part of your applicable agreement with Eightfold with respect to your use of Eightfold Services (the "Agreement"). Defined terms used in these Security Measures that are undefined shall have the same meanings as set forth in the Agreement.

Eightfold delivers a software-as-a-service solution through a unified, multi-tenant platform, providing consistency and reliability for all customers. The Service is delivered from a unified, continuously updated codebase, ensuring all users have access to the latest features and security enhancements. This one-to-many model enables Eightfold to maintain rigorous, standardized security and privacy protocols across its customer base. These Security Terms reflect this approach, offering uniform terms to all Customers. Eightfold reserves the right to modify these Security Terms to maintain compliance with applicable laws and industry standards or to enhance security measures, with notice of material changes provided to Customers. Given the nature of the Service, individual negotiations or customizations of these Security Terms are not operationally practicable. All references to "systems" in these Security Terms are to systems used to deliver, maintain, and secure the Services provided to customers. Eightfold has implemented technical and administrative safeguards to protect Customer Data.

Eightfold AI Information Security Program For Customer Data

Eightfold maintains a comprehensive information security program designed to protect the confidentiality, integrity, and availability of Eightfold systems and Customer Data.

Eightfold's security measures are continuously improved, reviewed, updated, and validated by independent third-party auditors to ensure ongoing effectiveness and compliance. These security measures are officially documented and published in Eightfold's Security Policy. Eightfold has appointed a designated management official responsible for leading the information security program, ensuring its effective implementation and alignment with organizational objectives.

Identity and Access

Eightfold maintains formal, documented policies and procedures governing access to information systems that contain Customer Data, ensuring access is restricted to authorized personnel only.

- **Separation of Duties:** Eightfold enforces the separation of duties between privileged and non-privileged users. Access to sensitive or customer data is strictly regulated based on role and operational need.
- **Multi-Factor Authentication:** All privileged users are required to use MFA for production system access.
- **System Access:** Direct system access is minimized. Changes are made through configuration management processes. When direct access is required, MFA and secure VPN connections are used to access systems remotely.
- **Access Rights Management:**
    - Eightfold immediately revokes access rights upon personnel termination.
    - Eightfold maintains appropriate password complexity requirements.
    - Privileged accounts inactive for ninety (90) days are automatically disabled.
- **Least Privilege:** Access is granted based on least privilege and need-to-know principles.
- **User Identity Lifecycle:** Eightfold tracks user identities throughout their lifecycle and performs regular access reviews. User identities are unique and traceable directly to individual personnel.
- **Identity Verification:** Eightfold mandates and enforces identity verification before granting access to any system within the security authorization boundary.
- **Authentication Credential Management:** Eightfold's internal policies govern the secure issuance, handling, and

revocation of authentication credentials.

Security Awareness

- **Mandatory Training:** Upon hire and at least once per year, all Eightfold employees are required to undergo required security awareness training which includes specific security topics such as phishing, insider threat, and data handling..
- **Supplemental Training:** Eightfold conducts additional training sessions in response to emerging security threats, significant policy changes, or new technologies. Role-based training is provided in alignment with internal requirements.
- **Effectiveness Evaluation:** Eightfold evaluates training effectiveness through scored assessments to measure understanding and retention of security protocols.
- **Policy Updates:** Eightfold regularly updates personnel on information security policies, including changes to topic-specific policies and procedures relevant to job functions.
- **Training Updates:** Eightfold consistently updates training materials to reflect security developments and regulatory requirements. Eightfold continually reviews and enhances training programs based on feedback and evolving security landscapes.
- **Acceptable Use Policies:** Eightfold maintains comprehensive acceptable use policies and rules of behavior for all individuals requiring system access. These policies outline responsibilities, expected behaviors, and compliance requirements regarding information and system usage, security, and privacy.

System Monitoring

- **Scope:** Eightfold implements logging and monitoring across all activities within the security authorization boundary, including automated alerting for specified events.
- **Log Generation:** Eightfold generates detailed logs of activities, exceptions, faults, and security-relevant events. These logs are aggregated into a central source appropriate to the operational environment.
- **Log Security:** Eightfold security logs are immutable and stored in a manner that protects against loss, destruction, falsification, and unauthorized access. Log data is safeguarded using quantum-resistant AES-256-GCM encryption to ensure data confidentiality and integrity.
- **Log Retention:** Eightfold audit logs are stored for at least one (1) year.
- **Continuous Monitoring:** Eightfold continuously monitors networks, systems, and applications for anomalous behavior that may indicate potential security incidents.

Security Assessments

- **Certifications:** Eightfold maintains ISO 27001, ISO 27701, and SOC 2 assessments which are reassessed annually.
- **Qualified Assessors:** All assessments are conducted by qualified assessors with relevant technical training and knowledge. Assessors must be affiliated with recognized bodies (e.g., AICPA, FedRAMP 3PAO) or hold appropriate certifications.
- **Penetration Testing:** Eightfold contracts with a 3PAO to provide penetration at least annually and internal penetration tests are performed at least quarterly.
- **Continuous Improvement:** Eightfold adapts and enhances security protocols and measures in response to assessment findings or to address identified vulnerabilities.
- **Documentation:** All assessment results are thoroughly documented including detailing findings, remedial actions, and compliance progress.
- **Availability of Reports:** Certifications and report summaries are made available to Customers upon request through a Trust Portal and subject to the confidentiality obligations set forth in the Agreement.
- **Communication:** Eightfold shall promptly communicate to Customer significant changes in its security posture that materially and adversely impact Customer.

Configuration Management

- **Change Management:** Eightfold maintains established requirements for implementing changes to system configurations. All changes within the security authorization boundary require documented approvals from authorized personnel.
- **Development Process:** The Eightfold Secure Development Lifecycle (SDLC) establishes guidelines for planning, delivery, and support of our application security capabilities.
- **Pre-Implementation Review:** Eightfold performs comprehensive reviews of relevant changes prior to implementation. This includes code scanning to ensure compliance with security requirements and to prevent the introduction of vulnerabilities.
- **System Inventory:** Eightfold maintains a detailed inventory of relevant system components. This inventory is regularly reviewed and updated to ensure accuracy and reflect current configurations.
- **Security Baselines:** Eightfold establishes, continuously monitors, and periodically reviews security baseline configurations. Eightfold makes adjustments in response to new security threats or changes in operational requirements.
- **Documentation:** Eightfold maintains comprehensive documentation of relevant configuration management processes and changes, providing a clear audit trail and facilitating compliance with relevant standards and regulations.
- **Testing:** Eightfold conducts thorough testing of all configuration changes in a non-production environment before deployment to production systems to minimize potential disruptions to the Service.
- **Rollback Procedures:** Eightfold maintains documented rollback procedures for relevant configuration changes to achieve rapid restoration of system stability in the event of unforeseen issues.

Contingency Planning

- **Information System Contingency Plan:** Eightfold maintains an Information System Contingency Plan (ISCP) designed to ensure readiness and effective response to operational disruptions, including natural disasters, cyber incidents, and system failures. Eightfold's Recovery Time Objective (RTO) is three (3) business days to functional operation and five (5) business days to return to regular operation. The Recovery Point Objective (RPO) is one (1) hour.
- **Annual Testing:** Eightfold performs annual testing of the ISCP in coordination with its Incident Response Plan (IRP). Upon Customer request, Eightfold provides a summary of annual functional test results.
- **Confidentiality:** Eightfold treats details of the ISCP and IRP as security-restricted information and implements appropriate controls to protect this sensitive data.
- **Resource Monitoring:** Eightfold continuously monitors resources to align with current and projected capacity requirements, protecting against system overloads and maintaining optimal performance.
- **Backup Policy:** Eightfold conducts regular backups in accordance with its comprehensive backup policy. This policy specifies frequency, scope, and methods to ensure data integrity and availability.
- **Backup Testing:** Eightfold regularly tests backup copies to verify their effectiveness in restoring data and systems, ensuring reliable data recovery in the event of an incident.
- **Redundancy:** Eightfold assesses information processing facilities' redundancy measures to meet availability requirements as specified in the Service Level Agreement (SLA).
- **Continuous Improvement:** Eightfold regularly reviews and updates its contingency planning and business continuity measures to address evolving threats and technological advancements.
- **Communication Protocol:** In the event of a significant disruption, Eightfold maintains a clear communication protocol to inform Customers of the situation and recovery progress.
- **Third-Party Coordination:** Where applicable, Eightfold coordinates with third-party service providers for comprehensive contingency planning across the entire Service delivery chain.

Incident Response

- **Incident Response:** Eightfold maintains an established incident response plan designed to address Security Incidents immediately upon detection. The incident response plan is architected based on NIST SP 800-61. Eightfold's Incident Response Team is trained and equipped to respond quickly to mitigate potential damage.
- **Customer Notification:** In the event of a Security Incident, Eightfold notifies customers without undue delay, with a goal of 24 hours and no later than 72 hours from incident confirmation.
- **Notification Content:** Details may be restricted during an ongoing Security Incident to minimize additional risk to

Eightfold systems and Customer Data and are also subject to the availability of information at the time of notification. Eightfold's incident notifications to customers include:

- A description of the incident
- The type of data involved
- The implications of the incident
- Actions taken to secure the data
- Steps customers can take for further protection

- **Regulatory Compliance:** Eightfold communicates relevant Security Incident information to appropriate authorities as required by applicable laws and regulations. Unless laws and regulations prohibit Eightfold from doing so, Eightfold shall notify Customer prior to such communication to authorities and will use commercially reasonable efforts to coordinate first with Customer.
- **Incident Documentation:** Eightfold maintains detailed documentation of Security Incidents and corresponding responses. This documentation supports compliance efforts, aids in the continuous improvement of incident response processes.
- **Post-Incident Review:** Following the resolution of each Security Incident, Eightfold conducts a review to identify root causes and evaluate the effectiveness of the incident response. Eightfold creates an after-action report (AAR) based on this review. Eightfold treats AAR details as security-restricted information and implements appropriate controls. Upon request, Eightfold provides the affected customers with a summary of the AAR.
- **Regular Testing:** Eightfold conducts an annual functional Incident Response Plan (IRP) test in conjunction with the Information System Contingency Plan (ISCP). Eightfold also performs regular tabletop exercises and provides ongoing training to all incident response team members.
- **Continuous Improvement:** Eightfold regularly reviews and updates its Incident Response Plan to incorporate lessons learned from incidents, tests, and industry best practices.

Maintenance:

- **Maintenance Activities:** Maintenance activities, including updates and patches, fall under Eightfold's configuration and change management processes.
- **Critical Security Patches:** Eightfold prioritizes and implements critical security patches to protect against known vulnerabilities. All patches undergo the same rigorous testing and approval processes as other maintenance activities.
- **Maintenance Schedule:** Eightfold operates under a continuous deployment model, frequently updating systems to maintain optimal health and security. Customers are provided with access to release notes.
- **Documentation:** Eightfold maintains detailed documentation of all maintenance activities, including the nature of the maintenance, date and time of implementation, and any impact on system performance or security.
- **Compatibility Testing:** Prior to implementing any major system updates, Eightfold performs compatibility testing for continued functionality of relevant system components and integrations.

Media Protection

- **Data Storage Restrictions:** Eightfold stores Customer Data exclusively within the defined security authorization boundary or other authorized systems. Storage of Customer Data on external media or unauthorized locations is prohibited.
- **Secure Hosting Infrastructure:** Eightfold hosts its systems within high-security provider data centers. This infrastructure ensures high availability, data redundancy, and advanced security measures to protect Customer Data.
- **External Media:** Eightfold prohibits the use of external media for storing or transferring Customer Data and there are technical measures in place to prevent exfiltrating customer data to any unauthorized location.
- **Data Deletion:** Eightfold promptly deletes Customer Data when no longer required in accordance with Customer requirements and applicable laws and regulations.
- **Secure Deletion Processes:** Eightfold implements data deletion processes that include thorough sanitization techniques to ensure deleted data cannot be recovered or reconstructed. These techniques adhere to the National Institute of Standards and Technology (NIST) Special Publication 800-88, Guidelines for Media Sanitization.

Physical and Environmental Protection:

- **Physical Access Control:** Eightfold controls access to its offices through electronic badge systems and monitors premises using closed-circuit television (CCTV) surveillance.
- **Data Center Management:** Eightfold's production systems and data reside within data centers managed by Infrastructure as a Service (IaaS) providers. Physical data center controls are inherited from these providers and are regularly reviewed as part of Eightfold's supplier security process.
- **Security Perimeters:** Eightfold establishes security perimeters around sensitive areas to protect information and associated assets. These perimeters are protected by mechanisms including physical barriers, electronic detection systems, and access control systems, with specific implementations varying by location.
- **Environmental Threat Protection:** Eightfold incorporates protection against physical and environmental threats, including natural disasters, fire, and flooding, into the design and implementation of its facilities to ensure minimal impact to the Service.
- **Visitor Management:** Eightfold maintains a visitor management system to track and monitor all visitors to its facilities, ensuring that visitors are properly authorized, logged, and escorted as necessary.
- **Regular Audits:** Eightfold conducts regular audits of its physical security measures to ensure their continued effectiveness and compliance with relevant standards and regulations.

Personnel Security:

- **Pre-Employment Screening:** Eightfold initiates comprehensive background checks on all employees as part of onboarding. These checks include, at minimum, criminal history verification and Office of Foreign Assets Control (OFAC) screening to assess candidate integrity and reliability.
- **Regulatory Compliance:** Eightfold ensures all background checks and screenings comply with relevant legal and regulatory requirements, including data protection and privacy laws, to protect individuals' rights and uphold ethical standards.
- **Secure Record Maintenance:** Eightfold maintains comprehensive, secure records of all background checks and verifications, ensuring transparency and accountability in the screening process. These records are accessible only to authorized personnel and are protected against unauthorized access and disclosure.
- **Confidentiality:** Eightfold treats all information obtained through background checks as confidential and uses it solely for employment-related purposes.
- **Third-Party Verification:** Eightfold engages reputable third-party providers to conduct background checks, promoting impartiality and thoroughness in the screening process.
- **Contractor Screening:** Eightfold extends appropriate background check requirements to suppliers, contractors, and temporary workers with access to sensitive information or systems.

Risk Assessment:

- **Risk Management Framework:** Eightfold assesses security risks using the National Institute of Standards and Technology (NIST) Risk Management Framework (RMF).
- **Threat Intelligence Program:** Eightfold maintains a threat intelligence program to continuously monitor and analyze emerging threats. This program provides actionable intelligence to inform risk management decisions and enhance Eightfold's ability to anticipate and respond to potential security incidents.
- **Vulnerability Detection:** Eightfold performs regular and comprehensive vulnerability scanning across its entire infrastructure and application stack. Vulnerability scans are run continuously when supported and at least weekly. This includes but is not limited to:
    - **Network Vulnerability Scanning:** Eightfold conducts regular systems scans to identify potential vulnerabilities.
    - **Web Application Scanning:** Eightfold performs regular automated and manual scans of all web applications to detect security weaknesses.
    - **Container Scanning:** Eightfold implements continuous scanning of container images and registries to identify vulnerabilities in containerized applications and their dependencies.
    - **Database Scanning:** Eightfold conducts regular scans of all database systems to identify misconfigurations, outdated software versions, and potential vulnerabilities.

    - **Code Scanning:** Eightfold performs static and dynamic code analysis on all application code to identify potential security flaws during the development process.
- **Vulnerability Evaluation:** Eightfold evaluates identified vulnerabilities to determine the potential impact on the organization, including the likelihood of exploitation and the severity of consequences. This evaluation informs the prioritization of remediation efforts. Vulnerabilities are scored using the Common Vulnerability Scoring System (CVSS).
- **Risk Mitigation:** Eightfold develops and implements appropriate measures to mitigate identified risks based on comprehensive risk assessments and vulnerability evaluations. To protect the integrity of the Eightfold platform and customer data, internal vulnerability information is strictly confidential and not shared externally. Eightfold adheres to the following vulnerability target resolution timeframes, based on severity, fix availability, and date of discovery:
    - **Critical Vulnerabilities:** Immediate action upon discovery, with mitigation or remediation within 48 hours.
    - **High Vulnerabilities:** Mitigation or remediation within 30 days of discovery.
    - **Medium Vulnerabilities:** Mitigation or remediation within 90 days of discovery.
    - **Low Vulnerabilities:** Mitigation or remediation within 180 days of discovery.

  Eightfold strives to address vulnerabilities as quickly as possible, often ahead of these deadlines. Eightfold maintains the right to adjust these timeframes based on risk analysis, operational impact, and resource availability, always prioritizing the security of the platform and customer data.

- **Confidentiality of Vulnerability Information:** Eightfold prohibits the external sharing of internal vulnerability information to minimize risk to the Eightfold platform and customer data.
- **Documentation and Reporting:** Eightfold documents and reports risk assessment findings and mitigation activities to relevant stakeholders to ensure transparency and facilitate informed decision-making.
- **Continuous Monitoring:** Eightfold continuously monitors its systems and networks to detect new vulnerabilities and emerging threats in a timely manner.
- **Regular Risk Assessments:** Eightfold conducts regular risk assessments, at least annually or upon significant changes to the information system or operating environment.
- **Third-Party Risk Assessment:** Eightfold extends its risk assessment processes to third-party vendors and service providers that may impact the security of Eightfold's systems or customer data.
- **Risk Treatment Plans:** Eightfold develops and maintains risk treatment plans for identified risks that cannot be immediately mitigated, detailing the approach and timeline for risk reduction.
- **Security Metrics:** Eightfold maintains and regularly reviews security metrics to measure the effectiveness of its risk management and vulnerability mitigation processes.

Supplier Security:

- **Security Requirements:** Eightfold maintains stringent security requirements for system and service acquisitions. Each applicable acquisition undergoes a risk assessment to identify potential security risks and ensure alignment with Eightfold's security posture before integration.
- **Contractual Obligations:** Where applicable, Eightfold requires vendors to adhere to specific security requirements in contractual agreements, covering data protection, access controls, incident response, and regulatory compliance.
- **Supplier Monitoring:** Eightfold performs regular monitoring of suppliers to ensure continuous compliance with security requirements, including performance reviews and security audits as necessary.
- **Periodic Evaluation:** Eightfold periodically reviews and evaluates supplier relationships and performance to assess the effectiveness of their security measures and identify areas for improvement.
- **Corrective Actions:** In cases where suppliers do not meet expected security standards, Eightfold implements corrective actions to address deficiencies and mitigate potential risks.
- **Vendor Risk Assessment:** Eightfold subjects each vendor to a risk assessment, evaluating the potential impact of their services on operations and data security.
- **Data Protection Obligations:** Eightfold specifies data protection obligations in contracts, including encryption, access controls, and incident response procedures for sensitive information.
- **Annual Security Assessments:** Eightfold conducts annual security assessments of vendors to evaluate compliance

with security requirements and identify new risks or areas for improvement.

- **Incident Response Requirements:** Eightfold requires subprocessors to maintain incident response plans and report any security incidents or breaches immediately.
- **Communication:** Eightfold maintains communication with vendors to discuss security updates, regulatory changes, and other factors impacting supply chain risk management.
- **Remediation and Termination:** If a vendor fails to meet security and compliance standards, Eightfold works with them to develop and implement a remediation plan. Failure to address identified issues within agreed-upon timelines may result in contract termination.

System and Information Integrity

- **Continuous Monitoring and Protection:** Eightfold equips systems with continuous monitoring capabilities to detect and respond to security events in real-time. This includes collecting and analyzing log data for anomalies and potential threats. Eightfold continuously monitors relevant systems and communications for suspicious activity and potential security incidents.
- **Endpoint Security:** Eightfold protects information stored on, processed by, or accessible via endpoint devices using encryption, access controls, and secure configurations. Eightfold implements extended detection and response (XDR) tools to provide visibility and protection for all endpoint devices. Comprehensive endpoint protection solutions safeguard devices against malware, ransomware, and other security threats.
- **UnifiedEndpoint Management:** For applicable devices, Eightfold has implemented Mobile Device Management (MDM) and eXtended Detection and Response (XDR) controls which enforce security controls including specific security configuration settings including encryption enforcement and forced updates.
- **Data Encryption:** Eightfold encrypts data on endpoint devices, both at rest and in transit, to prevent unauthorized access and ensure data integrity, even if devices are lost or stolen. Eightfold uses industry-standard protocols such as AES-256 and TLS 1.2 for all data in transit and at rest, protecting against interception and unauthorized access.
- **Audit Trails:** Eightfold maintains comprehensive audit trails to record access and modifications to critical data and systems. These logs are regularly reviewed to detect and investigate unauthorized or suspicious activities.
- **Network Security:** Eightfold deploys network firewalls and intrusion detection/prevention systems (IDS/IPS) to monitor and control incoming and outgoing network traffic, providing an additional layer of defense against unauthorized access and cyber threats. Eightfold implements network segmentation to isolate sensitive systems and data, reducing the risk of lateral movement by attackers and enhancing overall security posture.
- **Application Security:** Eightfold implements web application firewalls (WAF) to protect web applications from common threats such as SQL injection, cross-site scripting (XSS), and other application-layer attacks.
- **System Configuration and Maintenance:** Eightfold configures systems according to foundational security practices and in accordance with Eightfold AI Security policy. Eightfold regularly applies updates and patches to address known vulnerabilities and protect against potential exploits.

ANNEX C – LIST OF SUBPROCESSORS

Eightfold may update its list of Subprocessors as Subprocessors are added or deleted, and will maintain an updated list as part of its online privacy policy, linked from its website at https://eightfold.ai/privacy-policy/subprocessor-notice/. Eightfold will update this online list publicly and regularly to keep all of its customers and prospective customers informed. Eightfold will also provide notice of new Subprocessors specific to Customer in a separate written update to Customer. To the extent a new Subprocessor is added in an update, Customer may object in writing to the Processing of Controller Data by the new Subprocessor within fifteen (15) days following the update and such objection shall describe Customer's legitimate reason(s) for objection. If Customer does not object during such time period, the new Subprocessor shall be deemed approved. If Customer objects to the use of a new Subprocessor pursuant to the process provided hereunder, Eightfold shall have the right to cure the objection through one of the following options (at Eightfold's reasonable election) within sixty (60) days following Customer's objection: (a) Eightfold will cease to use the new Subprocessor with regard to Controller Data; (b) Eightfold will take the corrective steps requested by Customer in its objection and proceed to use the Subprocessor to Process Controller Data; or (c) Eightfold may cease to provide or Customer may agree not to use (temporarily or permanently) the particular aspect of a Service that would involve use of the Subprocessor to Process Controller Data.

To the extent Customer has engaged an Eightfold partner in connection with the Agreement, such partner may in some cases be a Subprocessor under the Agreement.

Eightfold partners are participants in Eightfold's partner program, are independent third parties, and are not Affiliates of Eightfold; the use of "partner" in this context does not refer to a legal partnership or any similar arrangement under which Eightfold or the Eightfold partner may bind or act on behalf of one another. More information on Eightfold's partner program is available at https://eightfold.ai/about/partners/.

ANNEX D – UK ADDENDUM

Subject to Section 7 of the DPA, the parties agree as follows:

The terms of this addendum (the "**Addendum**") apply solely to the Processing of Controller Data of Data Subjects who are residents of the UK and not to the Processing of any other Personal Data. This Addendum applies with respect to transfers from the UK to the U.S. solely in the event Eightfold is no longer certified under the Data Bridge or the Data Bridge is invalidated.

Part 1:

1. *Start Date.* The effective date of this Addendum is the effective date of the DPA.
2. *Parties' Details.* The "Customer" as defined in the DPA is the "Exporter." Eightfold AI Inc. is the "Importer." The parties' details are set forth in the signature section of the DPA, the Agreement, and **Annex A**.
3. *Addendum EU SCCs.* For the purposes of this Addendum, the "Addendum EU SCCs" means the EU SCCs identified in Section 7(b) to the DPA, including the Appendix Information (defined below) and with only the modules, clauses, and optional provisions of the EU SCCs brought into effect for the purposes of this Addendum as set forth in Section 7(b) of the DPA.
4. *Appendix Information.* "Appendix Information" or "Table 3" for the purposes of the Mandatory Clauses, means the information which must be provided for the Approved EU SCCs and which for this Addendum is set forth as follows:
    a. "Annex 1A" shall be deemed to mean that information as per **Part 1, Section 2** above.
    b. "Annex 1B" shall be deemed to mean that information in **Annex A**.
    c. "Annex II" shall be deemed to mean that information in **Annex B**.
    d. "Annex III" shall be deemed to mean that information in **Annex C**.
5. *Ending the Addendum when the Approved Addendum Changes.* Neither party may end this Addendum pursuant to the Mandatory Clauses, Section 19.

Part 2:

Mandatory Clauses of the Approved Addendum, being the template Addendum B.1.0 issued by the UK Information Commissioner's Office (ICO) and laid before 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.

ANNEX E – SWITZERLAND

Subject to Section 7 of the DPA, the parties agree as follows:

This Annex applies with respect to transfers from Switzerland to the U.S. solely in the event Eightfold is no longer certified under the Swiss-U.S. DPF or the Swiss-U.S. DPF is invalidated.

1. The terms of this Annex E apply solely to the Processing of Controller Data of Data Subjects who are residents of Switzerland and not to the Processing of any other Personal Data.
2. Transfers from Switzerland are made pursuant to the EU SCCs (as defined by the DPA) with the modifications set forth below.
3. The transfer of Personal Data shall, to the extent legally permitted, be governed by the provisions of the revised Federal Act on Data Protection, version of 25 September 2020 ("**Revised FADP**"); references to provisions of the GDPR in the EU SCCs shall be understood to be referring to the equivalent provisions of the Revised FADP.
4. Clause 13 is modified so that the Federal Data Protection and Information Commissioner is the competent supervisory authority with respect to Personal Data transfers governed by the Revised FADP.
5. For the purposes of the Clauses, the term "Member State" shall not be interpreted in such a way as to exclude Data Subjects in Switzerland from the possibility of suing for their rights in their place of habitual residence in accordance with Clause 18.c.
6. Any capitalized terms not otherwise defined herein shall have their meanings as set forth in the EU SCCs.

ANNEX F – CCPA

The parties agree as follows:

1. Application. This annex applies solely to the Processing of Controller Data that is personal information under the California Consumer Privacy Act, as amended (including, without limitation, by the California Privacy Rights Act) ("**CCPA**"); this Annex F does not apply to the Processing of any other Personal Data.

2. Definitions. All capitalized terms not otherwise defined herein shall have their meanings as set forth in the DPA. For the purposes of this Annex F, "business", "business purpose", "collects", "consumer", "person", "personal information", "processing", "sell", "service provider" and "share" have their respective meanings as set forth in the CCPA.

3. Purpose. Customer is a business, and Eightfold is processing personal information pursuant to the Agreement as a service provider of Customer for the business purposes. The personal information is disclosed by Customer to Eightfold for these limited and specific purposes.

4. CCPA rights and obligations

(a) Eightfold will comply with all applicable obligations under the CCPA, including by providing the same level of privacy protection as required by the CCPA;

(b) Customer may take those reasonable and appropriate steps set forth in the DPA and the Agreement to ensure that Eightfold uses the personal information in a manner consistent with Customer's obligations under the CCPA;

(c) Eightfold will notify Customer if Eightfold makes a determination that Eightfold can no longer meet its obligations under the CCPA;

(d) Customer may, upon notice (including a notice described in clause (c) immediately above), take those reasonable and appropriate steps set forth in the DPA and the Agreement to stop and remediate unauthorized use of personal information;

(e) Eightfold will not sell or share any personal information;

(f) Eightfold will not retain, use, or disclose any personal information for any purpose other than the business purposes, except as permitted by the CCPA;

(g) Eightfold will not retain, use, or disclose personal information outside of the direct business relationship between Eightfold and Customer, except as permitted by the CCPA;

(h) Eightfold will not combine any personal information with personal information that is not in the Controller Data that it receives from, or on behalf of, another person or business, or that Eightfold collects from its own interactions with the consumer outside of the business purposes and the direct business relationship between Eightfold and Customer, except as permitted by the CCPA; the parties acknowledge and agree that any combining contemplated by the Services is being performed by Eightfold for the business purposes and the direct business relationship between Eightfold and Customer;

(i) Customer may monitor Eightfold's compliance with this Annex F in accordance with the audit terms set forth in the DPA; and

(j) Eightfold will notify Customer of any consumer requests pursuant to the terms of the DPA.

This DPA template was updated as of November 20, 2023.