Fluence Data Processing Addendum

Version 1.0

This Data Processing Addendum ("DPA") forms part of the Fluence Terms of Use published on the Fluence websites (fluence.ai, fluence.network and fluence.cloud, including their subdomains) (the "Terms") and any order, service description or other agreement under which Fluence provides Services to Customer (together with the Terms, the "Agreement"). It is entered into between **Fluence DAO**, an association organised under the laws of Switzerland (Verein, Art. 60 et seq. Swiss Civil Code), contactable at hello@fluence.network ("Fluence"), and the legal entity that has created a Fluence account and uses the Services under the Agreement ("Customer"). Fluence and Customer are each a "Party" and together the "Parties".

This DPA applies whenever Fluence processes Personal Data on behalf of Customer in the course of providing the Services and that processing is subject to Applicable Data Protection Law. It reflects the Parties' agreement on the terms required by Article 28(3) of the GDPR, Article 9 of the Swiss FADP and the equivalent provisions of the UK GDPR, and supplements the "Data Protection", "Confidentiality" and "Proprietary Rights" sections of the Terms.

This DPA becomes binding on the earliest of: (a) Customer accepting it through the Fluence Console; (b) Customer returning a copy signed by its authorised representative to hello@fluence.network; or (c) Customer continuing to use the Services after Fluence has made this DPA available to it. Where Customer signs, Customer is identified by the legal name, registered address and account email stated in its signature and in its Fluence account, and that information forms part of this DPA without any further amendment.

1. Definitions

1.1 Capitalised terms not defined in this DPA have the meaning given in the Terms. In this DPA:

"Applicable Data Protection Law" means all laws and regulations applicable to the processing of Personal Data under the Agreement, including (a) Regulation (EU) 2016/679 (the "GDPR"); (b) the GDPR as it forms part of the law of the United Kingdom by virtue of the European Union (Withdrawal) Act 2018 and the Data Protection Act 2018 (together the "UK GDPR"); (c) the Swiss Federal Act on Data Protection of 25 September 2020 and its ordinance (the "FADP"); and (d) any national law implementing or supplementing the foregoing, in each case as amended or replaced from time to time.

"Controller", **"Processor"**, **"Data Subject"**, **"Personal Data"**, **"Personal Data Breach"**, **"processing"** and **"Supervisory Authority"** have the meanings given in the GDPR, and the equivalent terms in the UK GDPR and FADP are read accordingly.

"Compute Provider" means an independent data-centre operator or other supplier of CPU, GPU, storage or networking capacity that Customer deploys to through the Services, as described in the Terms.

"Compute Services" means the on-demand and reserved CPU and GPU virtual machines, dedicated servers, clusters, storage and networking that Customer provisions through the Fluence Console or API.

"Console" means the Fluence web console, available through fluence.ai, fluence.network and fluence.cloud and their subdomains, and the Fluence API.

"Customer Content" means the Works and Output as defined in the Terms, being all data, content, code, prompts, files, workloads, configurations and other materials that Customer or its end users submit to, store in or process through the Services, and the results generated for Customer by the Services.

"Customer Personal Data" means Personal Data contained in Customer Content that Fluence processes on behalf of Customer under the Agreement. It excludes Account Data.

"Account Data" means Personal Data relating to Customer's representatives and users that Fluence processes as a Controller for its own purposes of account administration, billing, security, support and marketing, as described in the Fluence Privacy Policy. Account Data is not governed by this DPA.

"Model Provider" means a third party that supplies artificial-intelligence models or inference capacity used by the AI Model API Service.

"Standard Contractual Clauses" or **"SCCs"** means the standard contractual clauses for the transfer of personal data to third countries annexed to Commission Implementing Decision (EU) 2021/914 of 4 June 2021.

"Swiss Addendum" means the amendments to the SCCs set out in clause 12.5, which implement the requirements of the Swiss Federal Data Protection and Information Commissioner ("FDPIC") for transfers subject to the FADP.

"UK Addendum" means the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses issued by the UK Information Commissioner under section 119A of the Data Protection Act 2018, version B1.0, in force from 21 March 2022.

"Sub-processor" means any Processor engaged by Fluence, or by a Sub-processor, to process Customer Personal Data. Compute Providers and Model Providers that process Customer Personal Data are Sub-processors.

"Services" has the meaning given in the Terms and includes the Compute Services and the AI Model API Service.

"Third Country" means a country outside the European Economic Area, the United Kingdom or Switzerland (as relevant to the Customer Personal Data concerned) that is not the subject of a valid adequacy decision under Article 45 GDPR, Article 45 UK GDPR or Article 16(1) FADP respectively.

2. Scope, roles of the Parties and precedence

2.1 **Roles.** For Customer Personal Data, Customer is the Controller (or, where Customer processes Personal Data on behalf of its own clients, a Processor acting on the documented instructions of those clients) and Fluence is a Processor. Where Customer is itself a Processor, Customer warrants that its instructions to Fluence, including the engagement of Fluence and of the Sub-processors in Annex 3, have been authorised by the relevant Controller, and Fluence is a Sub-processor to that Controller.

2.2 **Account Data.** Fluence is an independent Controller of Account Data and processes it in accordance with the Fluence Privacy Policy published on the Fluence websites (fluence.ai, fluence.network and fluence.cloud, including their subdomains). Nothing in this DPA makes Fluence a Processor of Account Data.

2.3 **Nature of the Services.** The Services provide infrastructure and API access on which Customer runs its own workloads. Fluence does not access the content of Customer's virtual machines, storage volumes or network traffic in the ordinary operation of the Compute Services. Administrative personnel of Fluence and of Compute Providers hold privileged platform access that technically permits access to the console of a virtual machine; such access is restricted to authorised personnel bound by confidentiality under clause 4 and is used only to provide support requested by Customer, to respond to security incidents, to maintain the platform or as required by law. Fluence's processing of Customer Personal Data is therefore limited to the operations described in Annex 1: hosting, storage, transmission, computation and deletion carried out automatically by the Services, and the limited access described in this clause.

2.4 **Details of processing.** The subject matter, duration, nature and purpose of the processing, the types of Personal Data and the categories of Data Subjects are set out in Annex 1, which forms part of this DPA.

2.5 **Precedence.** This DPA supplements the Agreement. In the event of any conflict between this DPA and the Agreement with respect to the processing of Customer Personal Data, this DPA prevails. In the event of any conflict between this DPA and the SCCs (where they apply under clause 12), the SCCs prevail. Nothing in this DPA reduces either Party's obligations under Applicable Data Protection Law.

2.6 **Term.** This DPA applies for as long as Fluence processes Customer Personal Data under the Agreement and until Fluence has completed deletion or return of Customer Personal Data in accordance with clause 10.

3. Processing on documented instructions

3.1 Fluence shall process Customer Personal Data only on documented instructions from Customer, including with regard to transfers to a Third Country, unless required to do so by European Union, Member State, United Kingdom or Swiss law to which Fluence is subject. In that case Fluence shall inform Customer of the legal requirement before processing, unless that law prohibits such information on important grounds of public interest.

3.2 Customer's documented instructions consist of: (a) the Agreement and this DPA; (b) the configuration choices Customer makes through the Console, including the Compute Providers, regions, models, storage and retention settings Customer selects; (c) Customer's use of the Services' features and APIs in accordance with the documentation; and (d) any further written instruction sent to hello@fluence.network that is consistent with the Agreement. Fluence may charge reasonable fees for carrying out instructions that fall outside the ordinary functionality of the Services.

3.3 Fluence shall immediately inform Customer if, in Fluence's opinion, an instruction infringes Applicable Data Protection Law. Fluence may suspend performance of that instruction until Customer confirms or withdraws it. Fluence is not obliged to conduct a legal review of Customer's instructions.

3.4 Fluence shall not (a) use Customer Personal Data for its own purposes; (b) sell or share Customer Personal Data; (c) use Customer Content or Customer Personal Data to train, fine-tune or otherwise improve any artificial-intelligence model, whether its own or a Model Provider's, unless Customer has expressly enabled a feature whose documented purpose is model training; or (d) combine Customer Personal Data with Personal Data from other customers, except for aggregated and anonymised security, performance and billing metrics that do not identify any Data Subject.

3.5 Fluence shall ensure that Compute Providers and Model Providers involved in delivering the Services to Customer are bound, through Fluence's contracts with them, to process Customer Content only as necessary to provide the requested resources or return the requested results and to delete temporary copies as described in the Terms.

4. Confidentiality of personnel

4.1 Fluence shall ensure that every person it authorises to process Customer Personal Data, including employees, contractors and personnel of the entities that contribute to the operation of the Fluence network, has committed to confidentiality in writing or is under an appropriate statutory obligation of confidentiality, and processes Customer Personal Data only on Fluence's instructions.

4.2 Fluence shall limit access to Customer Personal Data to personnel who need it to perform the Services, provide support requested by Customer, maintain security or comply with law, and shall provide those personnel with appropriate data-protection training.

4.3 The confidentiality obligations in this clause survive termination of this DPA and of the engagement of the relevant personnel.

5. Security of processing

5.1 Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing, as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Fluence shall implement and maintain the technical and organisational measures set out in Annex 2 so as to ensure a level of security appropriate to the risk, including as appropriate the measures listed in Article 32(1) GDPR.

5.2 Fluence may update Annex 2 from time to time provided that no update materially reduces the overall level of security of the Services during the term of the Agreement. Fluence shall make the current version of Annex 2 available on request.

5.3 **Shared responsibility.** Security is a shared responsibility. Fluence is responsible for the security of the Console, the Fluence API, the provisioning and billing systems and the contractual arrangements with Compute Providers. Customer is responsible for the security of everything it deploys and runs on the Compute Services, including operating systems, applications, encryption of data at rest and in transit within its workloads, access credentials, security-group and firewall rules, and backups, and for the lawful configuration of the AI Model API Service, including the selection of models, retention settings and any zero-data-retention option. Fluence does not snapshot or back up Customer's volumes. Standard volumes are stored as a single copy on a local NVMe device of the host; a replicated volume type is available for Customer to select where offered. Customer volumes are not encrypted at rest by the platform; Customer may apply encryption within its workloads. Customer is solely responsible for maintaining copies of Customer Content outside the resource that holds it.

5.4 Fluence shall ensure that Compute Providers made available through the Console operate from data centres that hold at least one of ISO/IEC 27001 certification, SOC 2 Type II attestation or an equivalent independently audited security standard, and shall make the relevant certification information for the Compute Provider selected by Customer available on request.

6. Sub-processors

6.1 **General authorisation.** Customer gives Fluence general written authorisation to engage Sub-processors to process Customer Personal Data. The Sub-processors engaged at the effective date of this DPA are listed in Annex 3 and are approved by Customer.

6.2 **Customer-selected Sub-processors.** Where Customer selects a specific Compute Provider, region or Model Provider in the Console, that selection constitutes Customer's specific instruction and authorisation to engage that Sub-processor for the relevant resource or request. Fluence shall identify the Compute Provider and the data-centre location for each resource in the Console before deployment, and shall identify the Model Provider for each model in the AI Model API Service documentation.

6.3 **Notice of changes.** Fluence shall inform Customer of any intended addition or replacement of a Sub-processor that is not a Customer-selected Sub-processor at least 30 days before that Sub-processor begins processing Customer Personal Data, by email to the address associated with Customer's account or by notice in the Console. For Customer-selected Sub-processors, publication of the new Compute Provider or Model Provider in the Console or documentation before Customer selects it constitutes notice.

6.4 **Right to object.** Customer may object to a new Sub-processor on reasonable, documented data-protection grounds by writing to hello@fluence.network within the 30-day notice period. The Parties shall then discuss the objection in good faith. If Fluence cannot reasonably accommodate the objection, for example by offering a configuration that avoids the new Sub-processor, Customer may terminate the affected Services on written notice without penalty, and Fluence shall refund any prepaid credits attributable to the terminated Services for the period after termination. If Customer does not object within the notice period, the new Sub-processor is deemed approved.

6.5 **Flow-down.** Fluence shall impose on each Sub-processor, by way of a written contract, data-protection obligations that provide at least the same level of protection for Customer Personal Data as this DPA, in particular sufficient guarantees to implement appropriate technical and organisational measures, confidentiality of personnel, assistance with Data Subject requests and Personal Data Breach notification. Fluence shall carry out appropriate due diligence on each Sub-processor before engagement.

6.6 **Liability.** Where a Sub-processor fails to fulfil its data-protection obligations, Fluence remains fully liable to Customer for the performance of that Sub-processor's obligations, subject to clause 14.

6.7 **Compute Providers.** Fluence does not own or operate the data centres from which the Compute Services are delivered. Fluence shall nevertheless ensure that each Compute Provider made available to Customer has accepted contractual terms with Fluence that require it to: process Customer Content only to provide the resources Customer has provisioned; not access the content of Customer's virtual machines except for support requested by Customer, incident response notified to Fluence, platform maintenance or as required by law; not record the serial console output of Customer's virtual machines; retain operational, error and troubleshooting logs for no longer than 31 days and apply masking to Personal Data in those logs where technically feasible; retain Customer data only for the period necessary to provide the resources; and notify Fluence promptly of any Personal Data Breach or security incident.

7. Assistance with Data Subject rights

7.1 Taking into account the nature of the processing, Fluence shall assist Customer by appropriate technical and organisational measures, insofar as this is possible, in fulfilling Customer's obligation to respond to requests from Data Subjects exercising their rights under Chapter III GDPR (access, rectification, erasure, restriction, portability and objection) and the equivalent rights under the UK GDPR and FADP.

7.2 Because Customer controls its own workloads, Customer will normally be able to respond to Data Subject requests using its own applications running on the Compute Services, which give Customer direct access to the data concerned, and the deletion functions of the Console. Where Customer cannot do so, Fluence shall provide reasonable additional assistance within 10 business days of a written request to hello@fluence.network, and may charge reasonable fees for assistance that requires work beyond the ordinary functionality of the Services.

7.3 If Fluence receives a request from a Data Subject that relates to Customer Personal Data, Fluence shall not respond to it other than to acknowledge receipt and refer the Data Subject to Customer, shall notify Customer within 5 business days by email to the address associated with Customer's account, and shall provide Customer with the information it reasonably needs to respond, unless prohibited by law.

8. Personal Data Breach notification

8.1 Fluence shall notify Customer without undue delay, and in any event within 48 hours, after becoming aware of a Personal Data Breach affecting Customer Personal Data. Notification shall be made by email to the address associated with Customer's account and, where Customer has designated a security contact in the Console, to that contact as well.

8.2 The notification shall, to the extent the information is available to Fluence at the time, (a) describe the nature of the Personal Data Breach, including where possible the categories and approximate number of Data Subjects and of Personal Data records concerned; (b) state the name and contact details of the Fluence contact from whom more information can be obtained; (c) describe the likely consequences of the Personal Data Breach; and (d) describe the measures taken or proposed to address the Personal Data Breach and to mitigate its possible adverse effects. Where it is not possible to provide all of this information at the same time, Fluence shall provide it in phases without undue further delay.

8.3 Fluence shall take reasonable steps to contain, investigate and remediate the Personal Data Breach, shall cooperate with Customer and provide the information Customer reasonably needs to meet its own notification obligations under Articles 33 and 34 GDPR, and shall keep Customer informed of material developments.

8.4 Fluence's notification of or response to a Personal Data Breach is not an acknowledgement of fault or liability. Fluence shall not notify a Supervisory Authority or Data Subjects of a Personal Data Breach affecting Customer Personal Data on Customer's behalf unless Customer instructs it to do so in writing or Fluence is required to do so by law.

8.5 Unsuccessful security incidents, such as blocked intrusion attempts, port scans, denial-of-service attacks that do not result in unauthorised access, or log-in failures, are not Personal Data Breaches and do not require notification under this clause.

9. Data protection impact assessments and prior consultation

9.1 Taking into account the nature of the processing and the information available to Fluence, Fluence shall provide Customer with reasonable assistance in ensuring compliance with Customer's obligations under Articles 32 to 36 GDPR and the corresponding provisions of the UK GDPR and FADP, including by providing the information in Annexes 1 to 3, the security documentation described in clause 11 and answers to reasonable written security and privacy questionnaires.

9.2 Where Customer is required to carry out a data protection impact assessment or to consult a Supervisory Authority in relation to processing performed by the Services, Fluence shall provide the additional information reasonably necessary that is not already available to Customer within 15 business days of a written request. Fluence may charge reasonable fees for assistance that goes beyond providing existing documentation.

10. Deletion and return of Customer Personal Data

10.1 **During the term.** Customer may at any time retrieve, modify or delete Customer Content held in the Compute Services through the Console, the API or the resources themselves. When Customer deletes a virtual machine, storage volume or other resource, the resource and its volume are removed from the platform immediately and the underlying storage capacity is released. Released capacity is not accessible to Customer or any other customer, and the storage layer provides newly allocated volumes with zeroed blocks so that data previously written by another volume cannot be read. Physical media are sanitised or destroyed by the Compute Provider when decommissioned.

10.2 **AI Model API Service.** Request and response content submitted to the AI Model API Service is processed in transient memory to fulfil the request and is not stored by Fluence beyond the time needed to return the result, except where Customer enables a feature whose documented purpose is to store content (such as file storage or caching). Where Customer selects the zero-data-retention option, Fluence shall route requests only to Model Providers that have committed to Fluence not to retain request or response content.

10.3 **On termination.** Customer is responsible for exporting Customer Content from its resources before deleting them and before the Agreement ends. Export is performed by network transfer from within Customer's resources to a destination of Customer's choice, at no egress charge; Fluence does not provide disk-image or snapshot export. Where Fluence terminates the Agreement or a Service other than for Customer's material breach, Fluence shall give Customer at least 30 days' notice during which Customer's resources remain accessible for export. Upon termination or expiry, and at the latest 60 days after termination, Fluence shall delete all Customer Personal Data and shall ensure that Sub-processors do the same, and shall confirm deletion in writing on Customer's request. Copies of Customer Personal Data in Fluence's platform backups, which contain Console and account records and not the content of Customer's volumes, are deleted in accordance with the backup rotation cycle and in any event within 90 days after termination, and are not restored or accessed except as required by law.

10.4 **Legal retention.** Fluence may retain Customer Personal Data after termination only to the extent and for the period required by European Union, Member State, United Kingdom or Swiss law, in which case Fluence shall protect it in accordance with this DPA, process it

only for the purpose of complying with that law and delete it when the retention requirement ends. Account Data, billing records and security logs retained by Fluence as Controller are not affected by this clause.

11. Audits and information

11.1 Fluence shall make available to Customer all information reasonably necessary to demonstrate compliance with the obligations laid down in Article 28 GDPR and this DPA, and shall allow for and contribute to audits, including inspections, conducted by Customer or an auditor mandated by Customer, in accordance with this clause.

11.2 Fluence shall first satisfy audit requests by providing, within 20 business days of a written request: (a) this DPA and its current Annexes; (b) the most recent independent certification or attestation reports (such as ISO/IEC 27001 certificates or SOC 2 Type II reports) of the Compute Providers selected by Customer, to the extent Fluence is permitted to share them; (c) a summary of Fluence's own security programme; and (d) written answers to Customer's reasonable security and data-protection questionnaire.

11.3 Where the information provided under clause 11.2 is not sufficient to demonstrate compliance, or where a Supervisory Authority requires it or a Personal Data Breach affecting Customer Personal Data has occurred, Customer may carry out an on-site or remote audit of Fluence's processing of Customer Personal Data, subject to the following conditions: (a) no more than once in any 12-month period, unless required by a Supervisory Authority or following a Personal Data Breach; (b) at least 30 days' written notice, specifying the scope and proposed dates; (c) during normal business hours and without unreasonable disruption to Fluence's operations; (d) the auditor is not a competitor of Fluence and is bound by written confidentiality obligations; (e) the audit is limited to systems, processes and documentation relevant to Customer Personal Data and does not extend to data of other customers; and (f) each Party bears its own costs, except that Customer shall reimburse Fluence's reasonable costs of assisting with any audit beyond the first business day.

11.4 Audits of Compute Providers' data centres are conducted through the certification and attestation reports referred to in clause 11.2(b). Where a Compute Provider permits on-site inspections by its customers' auditors, Fluence shall use reasonable efforts to arrange such an inspection for Customer on the terms set by that Compute Provider.

11.5 Customer shall provide Fluence with a copy of any audit report and shall treat it as Fluence's Confidential Information. Fluence shall remediate any material non-compliance identified by an audit within a reasonable time agreed between the Parties.

11.6 Fluence shall maintain a record of the categories of processing activities carried out on behalf of Customer as required by Article 30(2) GDPR and shall make it available to a Supervisory Authority on request.

12. International transfers

12.1 **Transfers to Fluence.** Fluence is established in Switzerland. Switzerland is the subject of European Commission Decision 2000/518/EC, confirmed by the Commission's review of 15 January 2024, and of UK adequacy regulations, so Customer's disclosure of Customer Personal Data to Fluence does not require a further transfer mechanism under Chapter V GDPR or the UK GDPR. Should Switzerland cease to benefit from an adequacy decision, the SCCs set out in clause 12.4 shall automatically apply between Customer (as data exporter) and Fluence (as data importer) with effect from the date the adequacy decision ceases to apply.

12.2 **Processing locations.** Customer Personal Data in the Compute Services is processed in the data-centre location that Customer selects for each resource in the Console. Fluence shall not move Customer Content stored in a resource to another country without Customer's instruction. Platform-level processing (provisioning, billing, support and security telemetry) is carried out in the European Union (Germany and Ireland) and in the United States by the Sub-processors listed in Annex 3. Requests to the AI Model API Service are processed in the locations of the Model Provider serving the selected model, which Fluence identifies in the service documentation.

12.3 **Onward transfers to Sub-processors.** Fluence shall transfer Customer Personal Data to a Sub-processor in a Third Country only where (a) the Sub-processor is covered by a valid adequacy decision or certification recognised under Article 45 GDPR, Article 45 UK GDPR or Article 16 FADP, such as the EU-U.S. Data Privacy Framework and its UK and Swiss extensions for the time being valid; or (b) Fluence has entered into the SCCs (Module Three: processor to processor) with that Sub-processor, together with the Swiss Addendum and, for UK Customer Personal Data, the UK Addendum, and has carried out and documented a transfer impact assessment; or (c) another transfer mechanism permitted by Applicable Data Protection Law applies. Fluence shall provide Customer with a copy of the relevant safeguards on request, redacted for commercially sensitive information.

12.4 **Incorporation of the SCCs.** Where the SCCs apply between the Parties under clause 12.1, they are incorporated into this DPA as follows: Module Two (controller to processor) applies where Customer is a Controller and Module Three (processor to processor) applies where Customer is a Processor; Clause 7 (docking clause) applies; in Clause 9, Option 2 (general written authorisation) applies with the notice period in clause 6.3 of this DPA; in Clause 11, the optional language is not used; in Clause 13, the competent

Supervisory Authority is the authority of the EU Member State in which Customer is established or, where Customer is not established in the European Union, the Irish Data Protection Commission; in Clause 17, Option 1 applies and the SCCs are governed by the law of Ireland; in Clause 18, disputes shall be resolved before the courts of Ireland; Annex I to the SCCs is completed by Annex 1 of this DPA and the Parties' details in the preamble; Annex II to the SCCs is completed by Annex 2 of this DPA; and Annex III to the SCCs is completed by Annex 3 of this DPA.

12.5 **Swiss Addendum.** Where Customer Personal Data is subject to the FADP and the SCCs apply, the SCCs are amended as follows, in accordance with the guidance of the FDPIC of 27 August 2021: references to the GDPR are read as references to the FADP insofar as the transfer is subject to the FADP; the FDPIC is the competent supervisory authority for transfers subject to the FADP, in parallel with the authority identified under Clause 13; the term "Member State" shall not be interpreted so as to exclude Data Subjects in Switzerland from exercising their rights under Clause 18(c) in Switzerland; and references to Member State law or courts include Swiss law and Swiss courts insofar as the transfer is subject exclusively to the FADP.

12.6 **UK Addendum.** Where Customer Personal Data is subject to the UK GDPR and the SCCs apply, the UK Addendum is incorporated and completed as follows: Table 1 is completed with the Parties' details in the preamble of this DPA; Table 2 refers to the SCCs as incorporated and completed by clause 12.4; Table 3 refers to Annexes 1, 2 and 3 of this DPA; and in Table 4, both the Importer and the Exporter may end the UK Addendum as set out in section 19 of the UK Addendum.

12.7 **Government access requests.** If Fluence or a Sub-processor receives a legally binding request from a public authority in any country for access to Customer Personal Data, Fluence shall, unless legally prohibited, promptly notify Customer, challenge the request where there are reasonable grounds to consider it unlawful under the law of the requesting country or Applicable Data Protection Law, disclose only the minimum Personal Data required, and document each request and its response.

13. Customer obligations

13.1 Customer is responsible for the lawfulness of the Customer Personal Data it processes through the Services, including having a valid legal basis, providing the notices required by Applicable Data Protection Law to Data Subjects and, where required, obtaining their consent.

13.2 Customer shall ensure that its instructions to Fluence comply with Applicable Data Protection Law and shall not instruct Fluence to process Personal Data in a manner that would cause Fluence to breach Applicable Data Protection Law.

13.3 Customer shall configure and use the Services in a manner appropriate to the sensitivity of the Customer Personal Data it processes, including by selecting data-centre locations, encrypting data within its workloads, managing access credentials and API keys, maintaining backups and, for the AI Model API Service, selecting models and retention settings that are suitable for the data concerned.

13.4 Customer shall carry out its own assessment before processing special categories of Personal Data (Article 9 GDPR), Personal Data relating to criminal convictions and offences (Article 10 GDPR) or data of comparable sensitivity under the FADP through the Services, and shall apply encryption under Customer's exclusive control to such data where it is stored in the Compute Services. Customer shall not submit such data to the AI Model API Service except to models for which Customer has verified, from the Model Provider information published by Fluence, that the Model Provider's commitments are adequate for that data.

13.5 Customer shall promptly notify Fluence at hello@fluence.network if it becomes aware of any Personal Data Breach affecting Customer Personal Data that originated in Customer's own systems or workloads and that may affect the security of the Services.

13.6 Customer shall keep the contact email address and, where offered, the security contact in its Fluence account accurate and current, since Fluence relies on them for the notices required by this DPA.

14. Liability

14.1 Each Party's liability arising out of or related to this DPA, whether in contract, tort or under any other theory of liability, is subject to the exclusions and limitations of liability set out in the Agreement, and the limitations in the Agreement apply to the aggregate liability of each Party under the Agreement and this DPA together.

14.2 Nothing in this DPA or the Agreement excludes or limits either Party's liability towards Data Subjects under Article 82 GDPR, Article 82 UK GDPR or the corresponding provisions of the FADP, or any liability that cannot be excluded or limited under applicable law.

14.3 Where the SCCs apply between the Parties, nothing in this clause limits the liability of either Party under the SCCs, including Clause 12 of the SCCs, to the extent such limitation would be inconsistent with the SCCs.

15. Term, termination and survival

15.1 This DPA takes effect in accordance with the preamble and remains in force for as long as Fluence processes Customer Personal Data on behalf of Customer.

15.2 This DPA terminates automatically when Fluence has deleted or returned all Customer Personal Data in accordance with clause 10. It cannot be terminated independently of the Agreement while Fluence continues to process Customer Personal Data.

15.3 Either Party may terminate the affected Services in accordance with clause 6.4 (objection to a Sub-processor) and Customer may terminate the affected Services if Fluence materially breaches this DPA and fails to remedy the breach within 30 days of written notice.

15.4 Clauses 4 (confidentiality), 10 (deletion and return), 11.5 (audit reports), 12.7 (government access requests), 14 (liability) and 16 (general provisions) survive termination of this DPA.

16. General provisions

16.1 **Governing law and disputes.** This DPA is governed by the laws of the State of Texas and applicable federal law of the United States of America, without regard to conflict-of-law principles, consistent with the Agreement, and disputes under it are resolved in accordance with the dispute-resolution provisions of the Agreement, except that (a) mandatory provisions of Applicable Data Protection Law prevail; (b) the SCCs, where they apply, are governed by the law of Ireland and disputes under them are resolved before the courts of Ireland as set out in clause 12.4; and (c) Data Subjects may bring claims as permitted by Applicable Data Protection Law and the SCCs irrespective of the dispute-resolution provisions of the Agreement.

16.2 **Changes in law.** If a change in Applicable Data Protection Law, a decision of a Supervisory Authority or court, or the issue of new standard contractual clauses by the European Commission, the UK Information Commissioner or the FDPIC requires this DPA to be amended, the Parties shall negotiate the necessary amendments in good faith. Fluence may make such amendments by publishing an updated version of this DPA in the Console with at least 30 days' notice, provided the amendments do not materially reduce the protection afforded to Customer Personal Data.

16.3 **Notices.** Notices from Customer to Fluence under this DPA shall be sent by email to hello@fluence.network with the subject line "DPA notice" and Customer's account email. Notices from Fluence to Customer shall be sent to the email address associated with Customer's account or posted in the Console. Notices are deemed received on the business day after they are sent.

16.4 **Severability.** If any provision of this DPA is held invalid or unenforceable, the remaining provisions remain in full force and the invalid provision is replaced by a valid provision that comes closest to the intention of the Parties and the requirements of

Applicable Data Protection Law.

16.5 **Entire agreement.** This DPA, together with the Agreement and, where applicable, the SCCs, constitutes the entire agreement between the Parties regarding the processing of Customer Personal Data and supersedes any earlier data-processing terms between them. Standard data-processing terms issued by Customer apply only if Fluence has expressly accepted them in writing.

16.6 **Counterparts and electronic acceptance.** Where this DPA is signed, it may be signed in counterparts and by electronic signature, each of which is an original. Acceptance through the Console has the same effect as a signature.

16.7 **Execution.** Fluence DAO executes this DPA by publishing it in the Console and making it available to Customer. Customer executes it by one of the methods set out in the preamble. The date of execution is the date of Customer's acceptance, signature or first use of the Services after this DPA was made available, whichever occurs first.

Annex 1 — Description of processing

This Annex completes Article 28(3) GDPR and, where the SCCs apply, Annex I to the SCCs.

A. Parties

Role	Party	Details
Data exporter / Controller (or Processor)	Customer	The legal entity holding the Fluence account, identified by the legal name, address and contact email recorded in that account. Activities: operation of Customer's own applications, services and workloads on the Compute Services and use of the AI Model API Service. Signature and date: by acceptance in the Console or signature as set out in the preamble.
Data importer / Processor	Fluence DAO, a Swiss association	Contact: hello@fluence.network. Activities: provision of the Fluence Console, API, Compute Services and AI Model API Service as described in the Terms. Signature and date: by publication of this DPA in the Console.

B. Description of the processing

Item	Description
Subject matter	Provision of cloud infrastructure (CPU and GPU virtual machines, dedicated servers, clusters, block and object storage, networking) sourced from Compute Providers, and of API access to third-party AI models, on which Customer processes its own data.
Duration	The term of the Agreement, plus the export and deletion periods in clause 10 of this DPA.
Nature of the processing	Hosting, storage, transmission, computation and deletion. The processing is automated and is determined by the workloads Customer deploys and the requests Customer sends. Fluence does not snapshot or back up Customer's volumes. Fluence personnel access Customer Personal Data only for support requested by Customer, incident response, platform maintenance or as required by law.
Purpose of the processing	To provide the Services ordered by Customer, in accordance with Customer's configuration and instructions.
Categories of Data Subjects	Determined by Customer. Typically: Customer's employees, contractors and agents; Customer's end users, customers and prospects; users of applications Customer hosts on the Services; and any other individuals whose Personal Data is contained in Customer Content.
Categories of Personal Data	Determined by Customer. Typically: identification and contact data; account and authentication data of Customer's own users; usage, log and device data generated by Customer's applications; content, files, prompts and documents submitted by Customer or its users; transaction and commercial data; and any other Personal Data Customer chooses to process on the Services.

Item	Description
Special categories of Personal Data	None unless Customer chooses to process them. If Customer does so, the restrictions and safeguards in clause 13.4 apply: encryption under Customer's exclusive control for data at rest in the Compute Services, and verification of Model Provider commitments before submission to the AI Model API Service.
Frequency of the transfer	Continuous, for as long as Customer's resources are deployed or Customer sends requests to the AI Model API Service.
Retention period	For Compute Services: until Customer deletes the resource or the Agreement ends, then as set out in clause 10. For the AI Model API Service: transient processing only, except for features Customer enables that store content.
Transfers to Sub-processors	Compute Providers in the data-centre locations selected by Customer; Model Providers serving the models selected by Customer; and the platform Sub-processors listed in Annex 3, each for the purpose and duration stated there.

C. Competent Supervisory Authority

The Supervisory Authority of the EU Member State in which Customer is established. Where Customer is not established in the European Union, the Irish Data Protection Commission. For processing subject to the UK GDPR, the UK Information Commissioner. For processing subject to the FADP, the Swiss Federal Data Protection and Information Commissioner.

Annex 2 — Technical and organisational measures

This Annex describes the measures Fluence implements under Article 32 GDPR and, where the SCCs apply, Annex II to the SCCs. Measures marked "Platform" apply to the Console, Fluence API, provisioning, billing and support systems operated by Fluence. Measures marked "Data centre" are required of every Compute Provider under its contract with Fluence. Measures inside Customer's workloads are Customer's responsibility under clause 5.3.

Area	Measure	Scope
Physical access control	Data centres are access-controlled 24/7 with badge or biometric entry, visitor logging, CCTV and perimeter security, and hold ISO/IEC 27001, SOC 2 Type II or an equivalent independently audited certification.	Data centre
Logical access control	Access to production systems requires named accounts, multi-factor authentication and role-based permissions granted on a least-privilege, need-to-know basis; privileged access is time-limited and logged; access rights are reviewed at least quarterly and revoked within one business day of role change or departure.	Platform
Customer authentication	Console and API access is protected by password policy, optional multi-factor authentication, and scoped API keys that Customer can rotate and revoke at any time; sessions expire after inactivity; brute-force and credential-stuffing protection is applied.	Platform
Tenant isolation	Virtual machines run on hypervisors with hardware-enforced isolation; dedicated servers are single-tenant; storage volumes are logically isolated per customer and released storage is not readable by subsequently allocated volumes. Each customer workspace is an isolated namespace and each VPC is isolated from other VPCs with no routes between them; Customer controls inbound and outbound traffic with security groups, address-spoofing protection is always enforced and egress to private address ranges is blocked. Until Customer configures security groups, traffic to and from its resources is not restricted.	Data centre

Area	Measure	Scope
Encryption in transit	All connections to the Console and API, and all traffic between Fluence systems and Compute Providers or Model Providers, use TLS 1.2 or higher with modern cipher suites.	Platform
Encryption at rest	Platform databases, backups and credential stores run on infrastructure of the platform Sub-processors listed in Annex 3 (DigitalOcean, AWS) that encrypts data at rest by default with provider-managed keys (AES-256). Customer volumes are not encrypted at rest by the platform; Customer may encrypt data within its workloads using keys under its exclusive control.	Platform
Secrets management	API keys, tokens and Provider credentials are stored hashed or encrypted, never in source code; infrastructure secrets are protected with AWS Key Management Service; credentials are rotated immediately on suspected compromise.	Platform
Logging and monitoring	Authentication events, administrative actions, API calls, provisioning operations and security-relevant events are logged with timestamps and actor identity, access-restricted, retained for at least 30 days and monitored for anomalies with alerting to on-call engineers.	Platform
Vulnerability management	Systems are patched according to risk, with critical vulnerabilities remediated within 14 days of a fix becoming available; dependencies are scanned automatically.	Platform

Area	Measure	Scope
Secure development	Code changes are peer-reviewed, tested in non-production environments that contain no Customer Personal Data, and deployed through automated pipelines with access controls and audit trails.	Platform
Availability and resilience	Platform services run redundantly across multiple nodes within a single cloud region (DigitalOcean, Frankfurt, Germany) with automated failover between nodes; there is no automated failover to another region. Platform databases are backed up at least daily, with continuous transaction-log archiving, to separate object storage in the same region, encrypted at rest by the storage provider. Compute Providers operate redundant power (UPS and generators), cooling and network uplinks. Standard customer volumes are stored as a single copy on a local NVMe device; a replicated volume type is available where offered. Fluence does not snapshot or back up Customer volumes; Customer is responsible for backups of its own workloads.	Platform and Data centre
Incident response	A documented incident-response procedure defines detection, triage, containment, eradication, recovery and lessons-learned steps, with defined roles and 24/7 on-call coverage; Compute Providers and Model Providers are contractually required to notify Fluence of incidents promptly; Customer notification follows clause 8.	Platform

Area	Measure	Scope
Data minimisation and retention	Fluence collects only the Account Data and telemetry needed to operate, secure and bill the Services; AI Model API request and response bodies are not stored in routine telemetry; retention periods are defined per data category and enforced by automated deletion.	Platform
Deletion and media sanitisation	Customer-initiated deletion removes the resource and releases its storage immediately; newly allocated volumes receive zeroed blocks so that data previously written by another volume cannot be read; decommissioned media are sanitised or destroyed by the Compute Provider in line with NIST SP 800-88; termination deletion follows clause 10.	Data centre
Personnel security	Personnel with access to production systems sign confidentiality undertakings, receive security and data-protection training on joining and at least annually, and are subject to background verification where permitted by local law.	Platform
Sub-processor management	Each Sub-processor is assessed for security and data-protection compliance before engagement and at least annually thereafter; contracts impose the obligations in clause 6.5; the list in Annex 3 is kept current.	Platform

Area	Measure	Scope
Data portability	Customer can export its data at any time by network transfer from within its resources to any destination of its choice (for example over SSH, rsync or object-storage clients), with no egress fees, in whatever structured, commonly used and machine-readable format Customer's applications produce. Disk-image and snapshot export is not provided.	Platform
Accountability and review	Fluence maintains records of processing activities under Article 30(2) GDPR, a risk register and this Annex, and reviews the effectiveness of these measures at least annually and after any significant incident or change.	Platform

Assistance to Customer. Fluence supports Customer's compliance through the Console deletion functions, region and Model Provider selection, the zero-data-retention option for the AI Model API Service, published Sub-processor and location information, and the documentation and assistance described in clauses 7, 9 and 11.

Annex 3 — Authorised Sub-processors

This Annex lists the Sub-processors authorised at the effective date of this DPA and completes, where the SCCs apply, Annex III to the SCCs. Fluence maintains the current list, including the legal name, country and role of each named entity, in the Console and provides it on request to hello@fluence.network. Changes are notified under clause 6.3.

A. Customer-selected Sub-processors

Sub-processor	Role and data processed	Location	Transfer safeguard
Compute Providers (independent data-centre operators offered in the Console)	Supply the physical servers, hypervisors, storage and network on which Customer's virtual machines, dedicated servers and clusters run; process all Customer Content stored or executed on the resources Customer deploys with them. The specific Compute Provider and data centre are shown in the Console for each resource before deployment and in the resource details afterwards.	The data-centre location Customer selects, which includes locations in the European Union and in other countries offered in the Console.	For locations in the EEA, the UK or Switzerland: none required. For locations in a Third Country: SCCs (Module Three) with Swiss Addendum and, for UK data, UK Addendum, or another mechanism under clause 12.3.

Sub-processor	Role and data processed	Location	Transfer safeguard
Model Providers (suppliers of the models offered through the AI Model API Service)	Receive the request content and technical metadata needed to generate a response and return it; the Model Provider serving each model, its location and its retention and training commitments are published in the AI Model API Service documentation. Where Customer selects the zero-data-retention option, only Model Providers that have committed to Fluence not to retain request or response content are used.	The locations stated in the AI Model API Service documentation for the selected model, which include the United States and the European Union.	As above for the location concerned; for United States Model Providers, EU-U.S. Data Privacy Framework certification (with UK and Swiss extensions) where held, otherwise SCCs (Module Three) with Swiss Addendum and UK Addendum.

B. Platform Sub-processors

Sub-processor	Role and data processed	Location	Transfer safeguard
DigitalOcean, LLC	Hosts the platform's Kubernetes clusters, persistent volumes, platform database backups (Spaces object storage) and the virtual-machine images used to provision the Compute Services; holds Console and account records including resource metadata, configuration and the Customer Personal Data that Customer enters into the Console (for example resource names, tags and SSH public keys).	European Union (Frankfurt, Germany, region fra1).	Data hosted in the EEA; DigitalOcean's data processing agreement with SCCs covers remote support access from the United States.
Amazon Web Services EMEA SARL	Stores infrastructure-as-code state (Terraform), provides key management (AWS KMS) for infrastructure secrets and runs CI runners; processes platform configuration and secrets, not Customer Content.	European Union (Ireland, region eu-west-1).	Data hosted in the EEA; AWS data processing addendum with SCCs covers remote support access from the United States.

Sub-processor	Role and data processed	Location	Transfer safeguard
Cloudflare, Inc.	DNS, reverse proxy, DDoS protection and edge workers for the Fluence websites, Console and API; processes IP addresses, request metadata and traffic in transit to the Console and API.	Global edge network; headquartered in the United States.	EU-U.S. Data Privacy Framework (with UK and Swiss extensions) and SCCs.
GitHub, Inc.	Source-code hosting and CI pipelines for the platform; processes platform code, build logs and the identities of Fluence engineers; does not hold Customer Content.	United States.	EU-U.S. Data Privacy Framework (with UK and Swiss extensions) and SCCs.
Twilio Inc. (SendGrid)	Delivers account, security, billing and DPA notices to the email addresses in Customer's account; processes recipient email addresses and message content.	United States.	EU-U.S. Data Privacy Framework (with UK and Swiss extensions) and SCCs.
Authentication service provider	Verifies log-in credentials and issues sessions and tokens for Console and API access; processes the credentials and identifiers of Customer's users.	European Union and United States.	EU-U.S. Data Privacy Framework or SCCs (Module Three) with Swiss and UK Addenda.

Sub-processor	Role and data processed	Location	Transfer safeguard
Stripe, Inc. and Stripe Payments Europe, Ltd.	Processes card and bank payments for Customer's account, including payment-method data, billing address and transaction records; Fluence receives only limited payment-method information and transaction status. Stripe acts as an independent Controller for the payment transaction itself and as a Sub-processor for billing records held for Fluence.	United States and European Union (Ireland).	EU-U.S. Data Privacy Framework (with UK and Swiss extensions) and SCCs.
NOWPayments	Processes cryptocurrency payments for Customer's account, including wallet addresses, transaction identifiers and payment status; Fluence receives transaction records and payment status.	European Union (Estonia).	None required within the EEA.

Sub-processor	Role and data processed	Location	Transfer safeguard
HubSpot, Inc. and HubSpot Ireland Limited	Customer-relationship, support-ticketing and account-communication platform; stores the names, email addresses, company details and support conversations of Customer's users, which may contain Customer Personal Data if Customer includes it in a support request.	United States and European Union (Ireland).	EU-U.S. Data Privacy Framework (with UK and Swiss extensions) and SCCs.
PostHog, Inc.	Product-analytics service for the Console; receives usage events, feature interactions, session identifiers, device and browser information and the account identifiers of Customer's users. Does not receive Customer Content.	United States, with EU data hosting in Germany where enabled.	EU-U.S. Data Privacy Framework or SCCs (Module Three) with Swiss and UK Addenda.
Google LLC (Google Analytics)	Web analytics on the Fluence website and Console; receives IP address, browser and device information, cookie identifiers, pages visited and conversion events of Customer's users. Does not receive Customer Content.	United States.	EU-U.S. Data Privacy Framework (with UK and Swiss extensions).

Sub-processor	Role and data processed	Location	Transfer safeguard
X Corp. (X Ads pixel)	Advertising-measurement and retargeting tag on the Fluence website; receives IP address, browser and device information, cookie identifiers and conversion events of Customer's users, subject to the cookie-consent choices made in the browser. Does not receive Customer Content.	United States.	EU-U.S. Data Privacy Framework (with UK and Swiss extensions) or SCCs (Module Three) with Swiss and UK Addenda.
OpenRouter, Inc. and the model providers serving its routed requests	Provides the AI-assisted support and content-protection features described in the Fluence Privacy Policy; receives the support messages, account context or request and response content needed for those features. Content-protection inspection is not applied to requests made with the zero-data-retention option where the provider's retention commitments have not been verified.	United States.	SCCs (Module Three) with Swiss and UK Addenda, with zero-retention routing where selected.

C. Scope of analytics and advertising recipients. Google Analytics, PostHog and the X Ads pixel process usage, device and cookie data about the individuals who use the Fluence website and Console on Customer's behalf. They never receive Customer Content or data from Customer's workloads, and analytics and advertising tags fire only in accordance with the cookie-consent choices made in the browser as described in the Fluence Privacy Policy.